Computer Security and Insecurity

Emmanuel Goff

COMPUTER SECURITY
AND
INSECURITY

COMPUTER SECURITY AND INSECURITY

Emmanuel Goff

BIBLIOTEX
Digital Library

Computer Security and Insecurity
by Emmanuel Goff

Copyright© 2022 BIBLIOTEX

www.bibliotex.com

All rights reserved. No part of this book may be reproduced or used in any manner without the prior written permission of the copyright owner, except for the use brief quotations in a book review.

To request permissions, contact the publisher at info@bibliotex.com

Ebook ISBN: 9781984664280

BIBLIOTEX
Digital Library

Published by:
Bibliotex
Canada
Website: www.bibliotex.com

Contents

1

Network Security Consulting and Network Management Services

Vulnerabilities in a network are exploited by both people inside the network and people outside the network. If your company is connected to the Internet or utilizes internal networking, a security evaluation is crucial to avoid compromises of valuable company resources and company information. We offer both on-site and off-site network testing, as well as evaluations and assessments for secure network architecture. Takniki also develops custom security software and provide educational and training classes on information security topics. When we started business, breaking into computers wasn't even a crime. Since then, both major and small security problems have become a well-known and often looked as thorn in the side of almost every organization. You can contract Takniki to examine or build your existing network architecture and make recommendations to optimize security. Whether you are expanding, upgrading, or simply wanting to make improvements to the overall security of your network, this is a valuable service at any time. In particular, we look at third party connections, expanding and defining security parameters, identifying and securing critical systems.

We at Takniki not only have rich experience in dealing with network security but also have world-class expertise. Whether it is about explaining how to write a password policy to your technical staff or describing to developers why "save %sp, -96, %sp" causes a window overflow trap which can lead to a buffer overflow vulnerability, We're just as comfortable as we are in designing the network architecture.

Every Activity at Takniki is done by hands. While testing your network we don't take help of network security scan software. Our team of security experts examine the network manually for each protocol and security loop hole. While testing, we typically invent entirely new attacks, just like a "real" hacker would. While architecting or designing a new network, we start with a clean sheet design. This unique approach makes us completely different from any other security consulting company.

Types of Network Security Services

Penetration Testing

A realistic assessment of security—creative by design and policy is absolutely invaluable. We have found vulnerabilities and security holes in everything from a Web Server to a Internet Instant Messenger or be it a Point of Sale Payment Terminal. We provide the most realistic and useful security analysis anywhere in any network system.

Network Testing: We test everything from a single computer, servers and firewall to an entire enterprise.

Server Testing: When you are deploying a new server, whether in-house or in a data centre, can result in significant security risks. We provide hard evidence of the risks, and then find a solution which doesn't reduce functionality and provides your the best working security model without compromising over functionality.

Application Review: Many security lapses and vulnerabilities are caused by poorly written software applications. We can analyse source code to find inherent flaws. If source is not available, we can attack the application as an outsider, and suggest alternative mechanisms to ensure the applications meets the security criteria.

Embedded Devices: We examine the devices to make sure that they comply with all security regulations. We also try to work closely with the device manufacturer to ensure its long-term security and necessary firmware updates are available.

Our work focuses is always on:

Functionality: Normally when it comes to security the organization has to compromise over software or network functionality. But we have rarely foudn that to be the case. Despite security being typically viewed as the enemy of functionality, we always find a solution which doesn't reduce functionality and provides you the best working security model without compromising over functionality and information accessibility.

Scalability: We at Takniki clearly understand that nothing is forever. An Network architecture is not a one-shot, rather it's a step by step methodology for implementing all new services, connectivity, and policies. The architecture and systems grow with the customer's needs and this is why all our solutions are typically canvassed with NO LIMITS.

Cost: Despite our aggressive and extensive approach, significant capital expenditures are rarely recommended. In all most all of our suggested solutions time & materials costs are generally minimal.

Secure Architecture makes security easier to maintain, expand and understand. To create a custom EGS Secure Architecture Plan, we analyse your business structure through discussions of corporate security issues and reviews of documentation such as network maps, policies and business processes. We then advise you on the best implementation of the most appropriate solution, which would address policy, technology and administrative elements.

Security in Networks

Networks their design, development, and usage are critical to our style of computing. We interact with networks daily, when we perform banking transactions, make telephone calls, or ride trains and planes. The utility companies use networks to track electricity or water usage and bill for it. When we pay for groceries or gasoline, networks enable our credit or debit card transactions and billing. Life without networks would be considerably less convenient, and many activities would be impossible. Not surprisingly, then, computing networks are attackers' targets of choice. Because of their actual and potential impact, network attacks attract the attention of journalists, managers, auditors, and the general public. For example, when you read the daily newspapers, you are likely to find a story about a network-based attack at least every month. The coverage itself evokes a sense of evil, using terms such as hijacking, distributed denial of service, and our familiar friends viruses, worms, and Trojan horses. Because any large-scale attack is likely to put thousands of computing systems at risk, with potential losses well into the millions of dollars, network attacks make good copy.

The media coverage is more than hype; network attacks are critical problems. Fortunately, your bank, your utility company, and even your Internet service provider take network security very seriously. Because they do, they are vigilant about applying the most current and most effective controls to their systems. Of equal importance, these organizations continually assess their risks and learn about the latest attack types and defence mechanisms so that they can maintain the protection of their networks.

In this chapter we describe what makes a network similar to and different from an application programme or an operating system. In investigating networks, you will learn how the concepts of confidentiality, integrity, and availability apply in networked settings. At the same time, you will see that the basic notions of identification and authentication, access control, accountability, and assurance are the basis for network security, just as they have been in other settings.

Networking is growing and changing perhaps even faster than other computing disciplines. Consequently, this chapter is unlikely to present you with the most current technology, the latest attack, or the newest defence mechanism; you can read about those in daily newspapers and at web sites. But the novelty and change build on what we know today: the fundamental concepts, threats, and controls for networks. By developing an understanding of the basics, you can absorb the most current news quickly and easily. More importantly, your understanding can assist you in building, protecting, and using networks.

Network Concepts

To study network threats and controls, we first must review some of the relevant networking terms and concepts. This review does not attempt to provide the depth of a classic networking reference. Our study of security focused on the individual pieces of a computing system, such as a single application, an operating system, or a database. Networks involve not only the pieces but also importantly the connections among them.

Networks are both fragile and strong. To see why, think about the power, cable television, telephone, or water network that serves your home. If a falling tree branch breaks the power line to your home, you are without electricity until that line is repaired; you are vulnerable to what is called a single point of failure , because one cut to the network destroys electrical functionality for your entire home. Similarly, there may be one telephone trunk line or water main that serves your home and those nearby; a failure can leave your building, street, or neighbourhood without service. But we have ways to keep the entire network from failing. If we trace back through the network from your home to the source of what flows through it, we are likely to see that several main distribution lines support an entire city or campus. That is, there is more than one way to get from the source to your neighbourhood, enabling engineers to redirect the flow along alternative paths. Redundancy makes it uncommon for an entire city to lose service from a single failure. For this reason, we say that such a network has resilience or fault tolerance.

Complex routing algorithms reroute the flow not just around failures but also around overloaded segments. The routing is usually done automatically; the control programme is often supplemented by human supervision or intervention. Many types of networks have very high reliability by design, not by accident. But because there often is less redundancy near a network's endpoints than elsewhere, we say that the network has great strength in the middle and fragility at the perimeter.

From the user's perspective, a network is sometimes designed so that it looks like two endpoints with a single connection in the middle. For example, the municipal water supply may appear to be little more than a reservoir (the source), the pipes (the transmission or communication medium), and your water faucet (the destination). Although this simplistic view is functionally correct, it ignores the complex design, implementation, and management of the "pipes." In a similar way, we describe computer networks in this chapter in ways that focus on the security concepts but present the networks themselves in a simplistic way, to highlight the role of security and prevent the complexity of the networks from distracting our attention. Please keep in mind that our network descriptions are often abstractions of a more complex actuality.

The Network

A network in its simplest form, as two devices connected across some medium by hardware and software that enable the communication. In some cases, one device is a computer (sometimes called a "server") and the other is a simpler device (sometimes called a "client") enabled only with some means of input (such as a keyboard) and some means of output (such as a screen). For example, a powerful computer can be a server, but a handheld personal digital assistant (PDA) or a cell phone might be a network client. In fact, because more consumer devices are becoming network-enabled, network security issues will continue to grow.

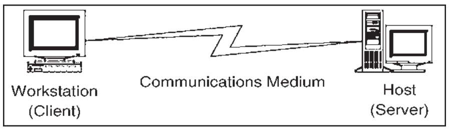


Fig. Simple View of Network.

Although this model defines a basic network, the actual situation is frequently significantly more complicated.

- The simpler client device, employed for user-to-computer communication, is often a PC or workstation, so the client has considerable storage and processing capability.
- A network can be configured as just a single client connected to a single server. But more typically, many clients interact with many servers.
- The network's services are often provided by many computers. As a single user's communication travels back and forth from client to server, it may merely pass through some computers but pause at others for significant interactions.

- The end user is usually unaware of many of the communications and computations taking place in the network on the user's behalf.

The user at one of the lettered client machines may send a message to System 3, unaware that communication is actually passing through the active Systems 1 and 2. In fact, the user may be unaware that System 3 sometimes passes work to System 4.

A single computing system in a network is often called a node, and its processor (computer) is called a host . A connection between two hosts is known as a link . Network computing consists of users, communications media, visible hosts, and systems not generally visible to end users. Systems 1 through 4 are nodes. In our figure the users are at the lettered client machines, perhaps interacting with Server F.

Users communicate with networked systems by interacting directly with terminals, workstations, and computers. A workstation is an end-user computing device, usually designed for a single user at a time. Workstations often have powerful processors and good- sized memory and storage so that they can do sophisticated data manipulation (such as converting coded data to a graphical format and displaying the picture). A system is a collection of processors, perhaps including a mixture of workstations and independent processors, typically with more processing power and more storage capacity than a workstation.

Environment of Use

The biggest difference between a network and a stand-alone device is the environment in which each operates. Although some networks are located in protected spaces (for example, a local area network in a single laboratory or office), at least some portion of most networks is exposed, often to total strangers.

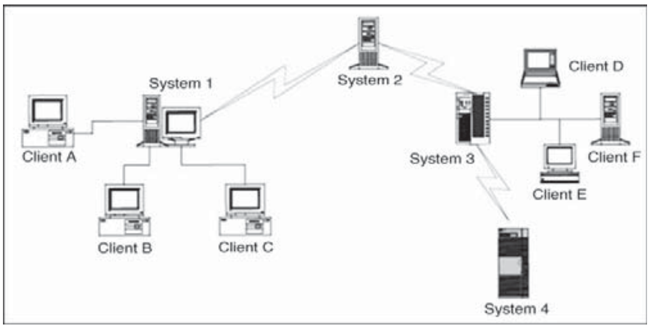


Fig. More Complex but More Typical View of Networks.

The relatively simple network is a good example. Systems 2, 3, and 4 are remote from System 1, and they may be under different ownership or control.

Networks can be described by several typical characteristics:

- *Anonymity.* You may have seen the cartoon image that shows a dog typing at a workstation, and saying to another dog, "On the Internet, nobody knows you're a dog." A network removes most of the clues, such as appearance, voice, or context, by which we recognize acquaintances.
- *Automation.* In some networks, one or both endpoints, as well as all intermediate points, involved in a given communication may be machines with only minimal human supervision.
- *Distance.* Many networks connect endpoints that are physically far apart. Although not all network connections involve distance, the speed of communication is fast enough that humans usually cannot tell whether a remote site is near or far.

- *Opaqueness*. Because the dimension of distance is hidden, users cannot tell whether a remote host is in the room next door or in a different country. In the same way, users cannot distinguish whether they are connected to a node in an office, school, home, or warehouse, or whether the node's computing system is large or small, modest or powerful. In fact, users cannot tell if the current communication involves the same host with which they communicated the last time.
- *Routing diversity*. To maintain or improve reliability and performance, routings between two endpoints are usually dynamic. That is, the same interaction may follow one path through the network the first time and a very different path the second time. In fact, a query may take a different path from the response that follows a few seconds later.

Shape and Size

The way a network is configured, in terms of nodes and connections, is called the network topology. You can think of the topology as the shape of the network.

The topology ranges from very simple, such as two hosts connected by one path, to very complex, such as the Internet.

These two extremes highlight three dimensions of networks that have particular bearing on a network's security.

- *Boundary.* The boundary distinguishes an element of the network from an element outside it. For a simple network, we can easily list all the components and draw an imaginary line around it to separate what is in the network from what is outside. But listing all the hosts connected to the Internet is practically impossible. For example, a line surrounding the Internet would have to surround the entire globe today, and Internet connections also pass through satellites in orbit around the earth. Moreover, as people and organizations choose to be connected or not, the number and type of hosts change almost second by second, with the number generally increasing over time.

- *Ownership.* It is often difficult to know who owns each host in a network. The network administrator's organization may own the network infrastructure, including the cable and network devices. However, certain hosts may be connected to a network for convenience, not necessarily implying ownership.
- *Control.* Finally, if ownership is uncertain, control must be, too. To see how, pick an arbitrary host. Is it part of network A? If yes, is it under the control of network A's administrator? Does that administrator establish access control policies for the network, or determine when its software must be upgraded and to what version? Indeed, does the administrator even know what version of software that host runs?

The truth is that, for many networks, it is difficult and at times impossible to tell which hosts are part of that network, who owns the hosts, and who controls them. Even for networks significantly smaller than the Internet, major corporate, university, or government networks are hard to understand and are not even well known by their system administrators. Although it seems contrary to common sense, many corporations today have no accurate picture of how their networks are configured. To understand why, consider a network of automated teller machines for a multinational bank. The bank may have agreements with other banks to enable customers to withdraw money anywhere in the world. The multinational bank may understand its own bank's network, but it may have no conception of how the connecting banks' networks are configured; no "big picture" shows how the combined networks look or operate. Similarly, a given host may be part of more than one network. In such a situation, suppose a host has two network interfaces. Whose rules does that host (and that host's administrator) have to follow?

Depicting, configuring, and administering networks are not easy tasks.

Mode of Communication

A computer network implements communication between two endpoints. Data are communicated either in digital format (in which data items are expressed as discrete binary values) or analog (in which data items are expressed as points in a continuous range, using a medium like sound or electrical voltage). Computers typically store and process digital data, but some telephone and similar cable communications are in analog form (because telephones were originally designed to transmit voice). When the transmission medium expects to transfer analog data, the digital signals must be converted to analog for transmission and then back to digital for computation at the receiving end. Some mostly analog networks may even have some digital segments, so the analog signals are digitized more than once. These conversions are performed by a modem, which converts a digital data stream to tones and back again.

Media

Communication is enabled by several kinds of media. We can choose among several types, such as along copper wires or optical fibre or through the air, as with cellular phones. Let us look at each type in turn.

Cable

Because much of our computer communication has historically been done over telephone lines, the most common network communication medium today is wire. Inside our homes and offices, we use a pair of insulated copper wires, called a twisted pair or unshielded twisted pair (UTP). Copper has good transmission properties at a relatively low cost. The bandwidth of UTP is limited to under 10 megabits per second (Mbps), so engineers cannot transmit a large number of communications simultaneously on a single line. Moreover, the signal strength degrades as it travels through the copper wire, and it cannot travel long distances without a boost.

Thus, for many networks, line lengths are limited to approximately 300 feet. Single twisted pair service is most often used locally, within a building or up to a local communications drop (that is, the point where the home or office service is connected to the larger network, such as the commercial telephone system). Although regular copper wire can transmit signals, the twisting reduces crossover (interference and signal transfer) between adjacent wires.

However, as speeds or capacities change, the basic ranking of two technologies tends to remain the same. Another choice for network communication is coaxial (coax) cable, the kind used for cable television. Coax cable is constructed with a single wire surrounded by an insulation jacket. The jacket is itself surrounded by a braided or spiral-wound wire. The inner wire carries the signal, and the outer braid acts as a ground. The most widely used computer communication coax cable is Ethernet, carrying up to 100 Mbps over distances of up to 1500 feet.

Coax cable also suffers from degradation of signal quality over distance. Repeaters (for digital signals) or amplifiers (for analog signals) can be spaced periodically along the cable to pick up the signal, amplify it, remove spurious signals called "noise," and retransmit it.

Optical Fibre

A newer form of cable is made of very thin strands of glass. Instead of carrying electrical energy, these fibres carry pulses of light. The bandwidth of optical fibre is up to 1000 Mbps, and the signal degrades less over fibre than over wire or coax; the fibre is good for a run of approximately 2.5 miles. Optical fibre involves less interference, less crossover between adjacent media, lower cost, and less weight than copper.

Thus, optical fibre is generally a much better transmission medium than copper. Consequently, as copper ages, it is being replaced by optical fibre in most communication systems. In particular, most long distance communication lines are now fibre.

Wireless

Radio signals can also carry communications. Similar to pagers, wireless microphones, garage door openers, and portable telephones, wireless radio can be used in networks, following a protocol developed for short-range telecommunications, designated the 802.11 family of standards. The wireless medium is used for short distances; it is especially useful for networks in which the nodes are physically close together, such as in an office building or at home. Many 802.11 devices are becoming available for home and office wireless networks.

Microwave

Microwave is a form of radio transmission especially well suited for outdoor communication. Microwave has a channel capacity similar to coax cable; that is, it carries similar amounts of data. Its principal advantage is that the signal is strong from point of transmission to point of receipt. Therefore, microwave signals do not need to be regenerated with repeaters, as do signals on cable.

However, a microwave signal travels in a straight line, presenting a problem because the earth curves. Microwave signals travel by line of sight: The transmitter and receiver must be in a straight line with one another, with no intervening obstacles, such as mountains. A straight microwave signal transmitted between towers of reasonable height can travel a distance of only about 30 miles because of the earth's curvature. Thus, microwave signals are "bounced" from receiver to receiver, spaced less than 30 miles apart, to cover a longer distance.

Infrared

Infrared communication carries signals for short distances (up to 9 miles) and also requires a clear line of sight. Because it does not require cabling, it is convenient for portable objects, such as laptop computers and connections to peripherals.

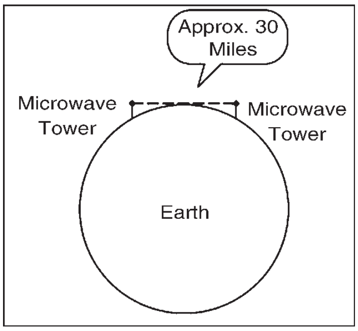


Fig. Microwave Transmission.

An infrared signal is difficult to intercept because it is a point-to-point signal. However, it is subject to "in the middle" attacks in which the interceptor functions like a repeater, receiving the signal, extracting any desired data, and retransmitting to the original destination the original signal or a modified version. Because of line-of-sight requirements and limited distance, infrared is typically used in a protected space, such as an office, in which in-the-middle attacks would be difficult to conceal.

Satellite

Many communications, such as international telephone calls, must travel around the earth. In the early days of telephone technology, telephone companies ran huge cables along the ocean's bottom, enabling calls to travel from one continent to another. Today, we have other alternatives. The communication companies place satellites in orbits that are synchronized with the rotation of the earth (called geosynchronous orbits), so the satellite appears to hover in a fixed position 22,300 miles above the earth. Although the satellite can be expensive to launch, once in space it is essentially maintenance free. Furthermore, the quality of a satellite communication link is often better than an earthbound wire cable.

Satellites act as nave transponders : Whatever they receive they broadcast out again. Thus, satellites are really sophisticated receivers, in that their sole function is to receive and repeat signals. From the user's point of view, the signal essentially "bounces" off the satellite and back to earth. For example, a signal from North America travels 22,300 miles into the sky and the same distance back to a point in Europe.

We can project a signal to a satellite with reasonable accuracy, but the satellite is not expected to have the same level of accuracy when it sends the signal back to earth. To reduce complexity and eliminate beam focusing, satellites typically spread their transmissions over a very wide area. A rather narrow angle of dispersion from the satellite's transmitter produces a fairly broad pattern (called the footprint) on the surface of the earth because of the 22,300-mile distance from the satellite to earth. Thus, a typical satellite transmission can be received over a path several hundred miles wide; some cover the width of the entire continental United States in a single transmission. For some applications, such as satellite television, a broad footprint is desirable. But for secure communications, the smaller the footprint, the less the risk of interception.

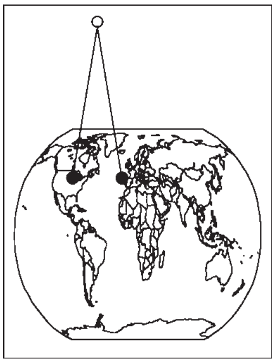


Fig. Satellite Communication.

Protocols

When we use a network, the communication media are usually transparent to us. That is, most of us do not know whether our communication is carried over copper wire, optical fibre, satellite, microwave, or some combination. In fact, the communication medium may change from one transmission to the next.

This ambiguity is actually a positive feature of a network: its independence. That is, the communication is separated from the actual medium of communication. Independence is possible because we have defined protocols that allow a user to view the network at a high, abstract level of communication (viewing it in terms of user and data); the details of how the communication is accomplished are hidden within software and hardware at both ends. The software and hardware enable us to implement a network according to a protocol stack, a layered architecture for communications. Each layer in the stack is much like a language for communicating information relevant at that layer. Two popular protocol stacks are used frequently for implementing networks: the Open Systems Interconnection

(OSI) and the Transmission Control Protocol and Internet Protocol (TCP/IP) architecture. We examine each one in turn.

ISO/OSI Reference Model

The International Standards Organization (ISO)/ Open Systems Interconnection model consists of layers by which a network communication occurs.

How communication works across the different layers. We can think of the layers as creating an assembly line, in which each layer adds its own service to the communication. In concert, the layers represent the different activities that must be performed for actual transmission of a message. Separately, each layer serves a purpose; equivalent layers perform similar functions for the sender and receiver. For example, the sender's layer four affixes a header to a message, designating the sender, the receiver, and relevant sequence information. On the receiving end, layer four reads the header to verify that the message is for the intended recipient, and then removes this header.

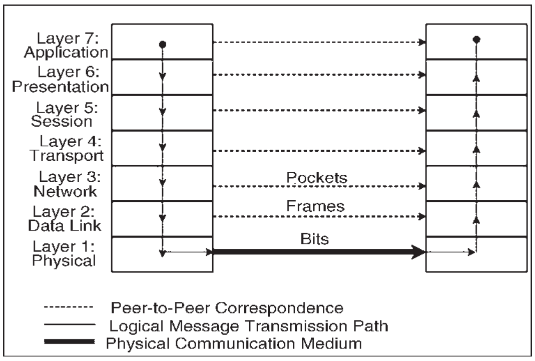
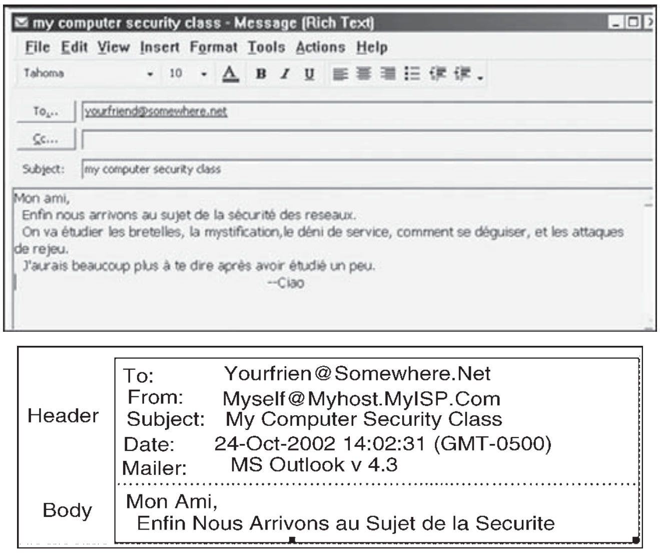


Fig. ISO/ OSI Network Model.

Each layer passes data in three directions: above with a layer communicating more abstractly, parallel or across to the same layer in another host, and below with a layer handling less abstract (that is, more fundamental) data items. The communications above and below are actual interactions, while the parallel one is a virtual communication path. Parallel layers are called "peers."

Let us look at a simple example of protocol transmission. Suppose that, to send e-mail to a friend, you run an application such as Eudora, Outlook, or Unix mail. You type a message, using the application's editor, and the application formats the message into two parts: a header that shows to whom the message is intended (as well as other things, such as sender and time sent), and a body that contains the text of your message. The application reformats your message into a standard format so that even if you and your friend use different mail applications, you can still exchange e-mail. This transformation is shown in Figure below.


my computer security class - Message (Rich Text)
File Edit View Insert Format Tools Actions Help
Tahoma
10
B I U
Header
Body

To... yourfriend@somewhere.net

Cc...

Subject: my computer security class

Mon ami,
Enfin nous arrivons au sujet de la sécurité des reseaux.
On va étudier les bretelles, la mystification,le déni de service, comment se déguiser, et les attaques de rejeu.
J'aurais beaucoup plus à te dire après avoir étudié un peu.
--Ciao

To: Yourfrien@Somewhere.Net
From: Myself@Myhost.MyISP.Com
Subject: My Computer Security Class
Date: 24-Oct-2002 14:02:31 (GMT-0500)
Mailer: MS Outlook v 4.3

Mon Ami,
Enfin Nous Arrivons au Sujet de la Securite

Fig. Transformation.

However, the message is not transmitted exactly as you typed it, as raw text. Raw text is a very inefficient coding, because an alphabet uses relatively few of the 255 possible characters for an 8-bit byte. Instead, the presentation layer is likely to change the raw text into something else. It may do compression, character conversions, and even some cryptography. An e-mail message is a one-way transfer (from sender to receiver), so it is not initiating a session in which data fly back and forth between the two endpoints. Because the notion of a communication session is not directly relevant in this scenario, we ignore the session layer for now. Occasionally, spurious signals intrude in a communication channel, as when static rustles a telephone line or interference intrudes on a radio or television signal. To address this, the transport layer adds error detection and correction coding to filter out these spurious signals.

Addressing

Suppose your message is addressed to yourfriend@ somewhere.net. This notation means that “somewhere.net” is the name of a destination host (or more accurately, a destination network). At the network layer, a hardware device called a router actually sends the message from your network to a router on the network somewhere.net. The network layer adds two headers to show your computer’s address as the source and somewhere.net’s address as the destination. Logically, your message is prepared to move from your machine to your router to your friend’s router to your friend’s computer. (In fact, between the two routers there may be many other routers in a path through the networks from you to your friend.) Together, the network layer structured with destination address, source address, and data is called a packet. The basic network layer protocol transformation is shown in Figure below.

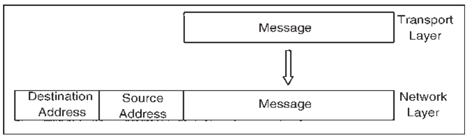


Fig. Network Layer Transformation.

The message must travel from your computer to your router. Every computer connected to a network has a network interface card (NIC) with a unique physical address, called a MAC address (for Media Access Control). At the data link level, two more headers are added, one for your computer's NIC address (the source MAC) and one for your router's NIC address. A data link layer structure with destination MAC, source MAC, and data is called a frame. Every NIC selects from the network those frames with its own address as a destination address. The data link layer adds the structure necessary for data to get from your computer to another computer (a router is just a dedicated computer) on your network.

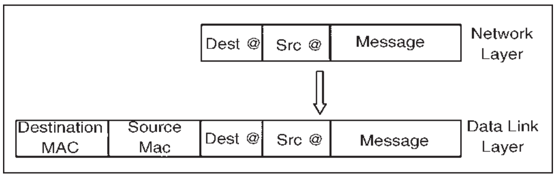


Fig. Data Link Layer Transformation.

Finally, the message is ready to be sent out as a string of bits. We noted earlier that analog transmissions communicate bits by using voltage or tone changes, and digital transmissions communicate them as discrete pulses. The physics and electronics of how bits are actually sent are handled at the physical layer.

On the receiving (destination) side, this process is exercised in reverse: Analog or digital signals are converted to digital data. The NIC card receives frames destined for it. The recipient network layer checks that the packet is really addressed to it. Packets may not arrive in the order in which they were sent (because of network delays or differences in paths through the network), so the session layer may have to reorder packets. The presentation layer removes compression and sets the appearance appropriate for the destination computer. Finally, the application layer formats and delivers the data as an e-mail message to your friend.

The layering and coordinating are a lot of work, and each protocol layer does its own part. But the work is worth the effort because the different layers are what enable Outlook running on an IBM PC on an Ethernet network in Washington D.C. to communicate with a user running Eudora on an Apple computer via a dial-up connection in Prague. Moreover, the separation by layers helps the network staff troubleshoot when something goes awry.

Layering

Each layer reformats the transmissions and exchanges information with its peer layer. Let us summarize what each layer contributes. A typical message that has been acted upon by the seven layers in preparation for transmission. Layer 6 breaks the original message data into blocks. At the session layer (5), a session header is added to show the sender, the receiver, and some sequencing information. Layer 4 adds information concerning the logical connection between the sender and receiver.

The network layer (3) adds routing information and divides the message into units called packets, the standard units of communication in a network. The data link layer (2) adds both a header and a trailer to ensure correct sequencing of the message blocks and to detect and correct transmission errors.

The individual bits of the message and the control information are transmitted on the physical medium by level 1. All additions to the message are checked and removed by the corresponding layer on the receiving side.

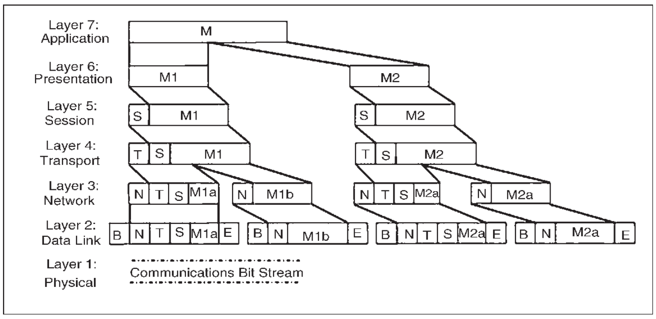


Fig. Message Prepared for Transmission.

The OSI model is one of several transmission models. Different network designers implement network activities in slightly different combinations, although there is always a clear delineation of responsibility. Some designers argue that the OSI model is overly complexit has too many levels and so other models are typically shorter.

TCP/IP

The OSI model is a conceptual one; it shows the different activities required for sending a communication. However, full implementation of a seven-layer transmission carries too much overhead for megabit-per-second communications; the OSI protocol slows things down to unacceptable levels.

For this reason, TCP/IP (Transmission Control Protocol/ Internet Protocol) is the protocol stack used for most wide area network communications. TCP/IP was invented for what became the Internet. TCP/IP is defined by protocols, not layers, but we can think of it in terms of four layers: application, host-to-host (end-to-end) transport, Internet, and physical.

In particular, an application programme deals only with abstract data items meaningful to the application user. Although TCP/IP is often used as a single acronym, it really denotes two different protocols: TCP implements a connected communications session on top of the more basic IP transport protocol. In fact, a third protocol, UDP (user datagram protocol) is also an essential part of the suite.

The transport layer receives variable-length messages from the application layer; the transport layer breaks them down into units of manageable size, transferred in packets. The Internet layer transmits application layer packets in datagrams, passing them to different physical connections based on the data's destination (provided in an address accompanying the data). The physical layer consists of device drivers to perform the actual bit-by-bit data communication. How each layer contributes to the complete interaction.

The TCP protocol must ensure the correct sequencing of packets as well as the integrity (correct transmission) of data within packets. The protocol will put out-of-sequence packets in proper order, call for retransmitting a missing packet, and obtain a fresh copy of a damaged packet. In this way, TCP hands a stream of correct data in proper order to the invoking application. But this service comes at a price. Recording and checking sequence numbers, verifying integrity checks, and requesting and waiting for retransmissions of faulty or missing packets take time and induce overhead. Most applications expect a flawless stream of bits, but some applications can tolerate a less accurate stream of data if speed or efficiency is critical.

A TCP packet is a data structure that includes a sequence number, an acknowledgment number for connecting the packets of a communication session, flags, and source and destination portnumbers. A port is a number designating a particular application running on a computer. For example, if Jose and Walter begin a communication, they establish a unique channel number by which their computers can route their respective packets to each of them. The channel number is called a port. Each service uses a well-known port, such as port 80 for HTTP (web pages), 23 for Telnet (remote terminal connection), 25 for SMTP (e-mail), or 161 for SNMP(network management). More precisely, each of these services has a waiting process that monitors the specified port number and tries to perform its service on any data passed to the port.

The UDP protocol does not provide the error-checking and correcting features of TCP, but it is a much smaller, faster protocol. For instance, a UDP datagram adds 8 bytes for control information, whereas the more complex TCP packet adds at least 24 bytes.

Addressing

Scheme for communication to occur, the bits have to be directed to somewhere. All networks use an addressing scheme so that data can be directed to the expected recipient. Because it is the most common, we use the Internet addressing scheme known as IP addresses in our examples, since it is the addressing handled by the IP protocol.

All network models implement an addressing scheme. An address is a unique identifier for a single point in the network. For obvious reasons, addressing in shared, wide area networks follows established rules, while addressing in local area networks is less constrained.

Starting at the local area network, each node has a unique address, defined in hardware on the network connector device (such as a network interface card) or its software driver. A network administrator may choose network addresses to be easy to work with, such as 1001, 1002, 1003 for nodes on one LAN, and 2001, 2002, and so forth on another.

A host on a TCP/IP wide area network has a 32-bit address, called an IP address. An IP address is expressed as four 8-bit groups in decimal notation, separated by periods, such as 100.24.48.6. People prefer speaking in words or pseudowords, so network addresses are also known by domain names, such as ATT.COM or CAM.AC.UK. Addressing tables convert domain names to IP addresses.

The world's networks are running out of unique addresses. This 32-bit standard address is being increased to 128 bits in a scheme called IPv6. But because 32-bit addresses will remain for some time, we focus on the older version.

A domain name is parsed from right to left. The rightmost portion, such as .COM, .EDU, .NET, .ORG, or .GOV, or one of the two-letter country specific codes, such as .UK, .FR, .JP, or .DE, is called a top-level domain. A small set of organizations called the Internet Registrars controls these top-level domains; the registrars also control the registration of second-level domains, such as ATT in ATT.COM. Essentially, the registrars publish addresses of hosts that maintain tables of the second-level domains contained in the top-level domain. A host connected to the Internet queries one of these tables to find the numeric IP address of ATT in the .COM domain. AT&T, the company owning the ATT Internet site, must maintain its own host to resolve addresses within its own domain, such as MAIL.ATT.COM.

You may find that the first time you try to resolve a fully qualified domain name to its IP address, your system performs a lookup starting at the top; for subsequent attempts, your system maintains a cache of domain name records that lets it resolve addresses locally. Finally, a domain name is translated into a 32-bit, four-octet address, and that address is included in the IP packets destined for that address. (We return to name resolution later in this chapter because it can be used in network attacks.)

Routing Concepts

A host needs to know how to direct a packet from its own IP address. Each host knows to what other hosts it is directly connected, and hosts communicate their connections to their neighbours. For the example network of Figure above, System 1 would inform System 2 that it was one hop away from Clients A, B, and C.

In turn, System 2 would inform its other neighbour, System 3, that it (System 2) was two hops away from Clients A, B, and C. From System 3, System 2 would learn that System 3 was one hop away from Clients D and E, Server F, and System 4, which System 2 would then pass to System 1 as being a distance of two hops. The routing protocols are actually more complex than this description, but the concepts are the same;

hosts advertise to their neighbours to describe to which hosts (addresses) they can route traffic and at what cost (number of hops). Each host routes traffic to a neighbour that offers a path at the cheapest cost.

2

Security and Privacy in Information Technology

Computer networks have been around for several decades and evolved from interconnecting only a few computers in a single room, into integrating hundreds of millions of devices worldwide forming an entity we all know as the Internet. While in the past, computer networks usually consisted of classic hardware devices like terminals, servers and network accessories like storage systems or printers, networks nowadays cover a multitude of device classes, starting from the most powerful super computers going all the way via personal computers, laptops, household appliances to simple sensor nodes. With the demand for mobility, wireless communication means have been developed, allowing the appearance of ultra-portable computing devices such as notebooks, tablet computers and smart phones. Thanks to advanced miniaturization, wireless devices can be even smaller than a coin, allowing to connect virtually everything to a network following the imagination of Kristofer Pister.

He introduced the concept of smart dust in 2000, which is basically a hypothetical system of tiny wireless devices coping with a variety of tasks. Although it might take another ten years to come close to his vision of interconnecting everything, recent developments brought small, powerful mobile devices with outstanding connectivity to the mass market and therefore into our very homes and workplaces.

Establish an Electronic Information, Privacy, and Security Policy

Focus on managing this evolving risk by establishing an electronic privacy and security policy. Many camps already have some type of policy governing employee use of the Internet, e-mail, Facebook, and other social media. This is a good start. If these policies haven't been reviewed in a while, take some time to review these guidelines before summer. Expand on these to include some broader developing risks.

The following are some examples of issues to be addressed in your updated policy. This list is not exhaustive; consider including other risks — especially those which may be unique to your camp.

- Use of electronic communications systems; security and privacy of electronic information; use of passwords; structure for passwords; prohibitions on downloading personally identifiable information to notebook computers or flash drives; guidelines for camper contact outside of camp.

- Use of camp e-mail; no expectation of privacy for employee e-mail communications sent on camp e-mail systems; prohibition of offensive, hostile, discriminatory or intimidating content.
- Internet, Intranet, or Extranet to be used solely to facilitate the conduct of the camp's business.
- Establish guidelines for the use of social media (Facebook, LinkedIn, etc.), blogs, and other internet publications; identify prohibited conduct; emphasize the importance of using good judgment in postings; and clarify that employees have no permission to use the camp's name, etc.
- Consequences of violating the policies — disciplinary action, which may include termination of employment.

Enlist your insurance broker or insurance company loss control representatives in this process. Share your current policies on these topics with them and ask for their suggestions to improve and expand your guidelines. Your electronic privacy and security policy should be shared with every employee.

Require each employee to read the policies and acknowledge with a signature that the employee has received a copy of the policy, read it, and agrees to follow the guidelines set forth in the document. This acknowledgement should include a statement of consequences for failing to follow the company policy, such as disciplinary action up to and including termination of employment. A copy of the signed acknowledgment should be kept permanently with the employee's human resources records.

Security Breaches and Failure to Manage Privacy

California was the first state to pass a data security breach law. Since then, forty-three other states, plus the District of Columbia, Puerto Rico, and the US Virgin Islands, have passed data security laws. The requirements of each state law are different, but the common thread is a requirement to notify the persons whose personally identifiable information was compromised. Personally identifiable information includes name, address, social security number, gender, marital status, contact information, driver's license issue and expiry dates, credit card information, and medical history, among other things. This sounds like the very kind of information maintained in camp databases about their campers, camper families, and employees.

Notification costs have been quoted by various information technology industry experts to be in the $200 – $300 range per compromised data file. Not terrible, you say, but suppose your database had one thousand names, and all were compromised. That's an expense of $200,000 – $300,000 probably not covered by your camp insurance policies. If you store personally identifiable information in your camp databases, you need to be aware of your state's data security breach disclosure law. Other consequences will most likely include civil suits, depending on the extent of any financial damages.

Types of Situations Contributing to Security Breaches

Not all security breaches are major. In fact, some events are so minor you might not notice the event unless someone on your staff or an independent consultant is watching closely. A frequency of small events left unchecked may lead to a larger, more catastrophic event. Security breaches may occur when passwords are stolen because unprotected wireless networks were used.

Passwords should be complex and changed on a regular basis. Security may be compromised by failing to change employee login information when someone leaves. Not all former employees may be disgruntled and vindictive, but it only takes one. Sometimes employees are fooled into clicking on links that compromise their individual work stations and jeopardize network security.

Beware of clicking on a link in any e-mail that is from an unfamiliar source or that you didn't solicit. Don't click on ads that say you've "won," for example; they may download spyware that compromise security. If you allow employees to take notebook computers or flash drives out of the office with customer information stored on the devices, you are at risk of a security breach should the device be lost or stolen. Some smart phones are also capable of storing customer information with e-mail and text applications, posing a similar security and privacy breach risk if they are lost or stolen.

My Information is in the Cloud

There are many internet service providers (ISPs) focused on the camp industry who offer directors the convenience of accessing software and storing customer information offsite on the Cloud. The Cloud in this instance is a metaphor for the Internet. Your camp management information is accessed via the Internet from any computer, anywhere, at any time, usually through a Web browser. The experience is often the same as if the software applications and data were stored locally on the user's computer.

What about security in this situation? There are divergent views on this issue, but generally security is often as good as or better than other traditional network systems because the services are shared. As a result, these ISPs are able to devote greater resources to security than many businesses could afford on their own. If you experience a security breach, don't expect the ISP to be responsible. Most Cloud computing contracts will contain comprehensive limitation of liability provisions, including both a financial cap on liability and an exclusion clause for indirect losses, and in most cases, a separate exclusion clause for data loss and data breaches.

Another common feature of Cloud computing contracts involves tying the financial cap in liability to the amount of fees paid by the Cloud customer under the contract, further limited to a specific time, such as the previous twelve months. This means you are most likely on your own to pay for breach notification costs and deal with any other legal consequences from a security breach. It is recommended that directors read Cloud computing (ISP) agreements carefully and take the time to understand any limitation clauses or other provisions in the contracts that limit the ISP's liability for damages arising out of security breaches or other services.

Defensive Strategy — Protect Your Computer Network

Whether your network is wired or wireless, whether you are Cloud computing or not, and regardless if you operate just one or twenty computers, protect them by using a network router. This electronic device allows a number of computers to share the same internet connection. It also provides security for the computer's access points or ports, as well as filtering communications and blocking unauthorized access. Wireless routers come with default administrator passwords. Unfortunately, these default passwords are not always changed before the wireless router is put into service. This increases the risk of unauthorized access and network security breaches. Be sure your camp computer network administrator is changing the default passwords in your wireless routers and using complicated passwords in their place. Also be sure that any transmitted wireless signal is encrypted.

Other suggestions for protecting your computer network and keeping private information secure include:

- Keep all operating systems up to date.
- Install and run a good antivirus and spyware scanner regularly.
- Use an external hard drive to store all information, including personally identifiable information, and disconnect it from your computer when not in use.
- Consider using Web-accessed e-mail.

As a practical matter, even the most savvy computer users can benefit from having an IT consultant. If you don't have such a person available to you, consider hiring one as part of your first line of defence against security breach risks and cyber thieves. This will be money well spent.

Be Prepared

In the final analysis, an effective strategy for managing the risk of computer network security involves constant vigilance. This vigilance needs to be backed up by a sophisticated information technology structure, as comprehensive as you can afford, with practical guidelines for people to follow. This approach will help to reduce the risks of privacy and security breaches. Once you've done all you can from a risk management perspective, consider buying some cyber liability insurance to protect against lawsuits alleging negligence and notification costs in the event a breach occurs in spite of your efforts.

Network Topologies

In computer networking, *topology* refers to the layout of connected devices. This chapter introduces the standard topologies of networking.

Topology in Network Design

Think of a topology as a network's virtual shape or structure. This shape does not necessarily correspond to the actual physical layout of the devices on the network. For example, the computers on a home LAN may be arranged in a circle in a family room, but it would be highly unlikely to find a ring topology there.

Network topologies are categorized into the following basic types:

- Bus
- Ring
- Star
- Tree
- Mesh.

More complex networks can be built as hybrids of two or more of the above basic topologies.

Bus Topology

Bus networks (not to be confused with the system bus of a computer) use a common backbone to connect all devices. A single cable, the backbone functions as a shared communication medium that devices attach or tap into with an interface connector.

A device wanting to communicate with another device on the network sends a broadcast message onto the wire that all other devices see, but only the intended recipient actually accepts and processes the message. Ethernet bus topologies are relatively easy to install and don't require much cabling compared to the alternatives. 10Base-2 ("ThinNet") and 10Base-5 ("ThickNet") both were popular Ethernet cabling options many years ago for bus topologies.

However, bus networks work best with a limited number of devices. If more than a few dozen computers are added to a network bus, performance problems will likely result. In addition, if the backbone cable fails, the entire network effectively becomes unusable.

Ring Topology

In a ring network, every device has exactly two neighbours for communication purposes. All messages travel through a ring in the same direction (either "clockwise" or "counterclockwise"). A failure in any cable or device breaks the loop and can take down the entire network. To implement a ring network, one typically uses FDDI, SONET, or Token Ring technology. Ring topologies are found in some office buildings or school campuses.

Star Topology

Many home networks use the star topology. A star network features a central connection point called a “hub node” that may be a network hub, switch or router. Devices typically connect to the hub with Unshielded Twisted Pair (UTP) Ethernet. Compared to the bus topology, a star network generally requires more cable, but a failure in any star network cable will only take down one computer’s network access and not the entire LAN. (If the hub fails, however, the entire network also fails.)

Tree Topology

Tree topologies integrate multiple star topologies together onto a bus. In its simplest form, only hub devices connect directly to the tree bus, and each hub functions as the root of a tree of devices. This bus/star hybrid approach supports future expandability of the network much better than a bus (limited in the number of devices due to the broadcast traffic it generates) or a star (limited by the number of hub connection points) alone.

Mesh Topology

Mesh topologies involve the concept of routes. Unlike each of the previous topologies, messages sent on a mesh network can take any of several possible paths from source to destination. (Recall that even in a ring, although two cable paths exist, messages can only travel in one direction.) Some WANs, most notably the Internet, employ mesh routing. A mesh network in which every device connects to every other is called a full mesh. Partial mesh networks also exist in which some devices connect only indirectly to others.

A Brief History of the Internet & Related Networks

In 1973, the U.S. Defense Advanced Research Projects Agency (DARPA) initiated a research programme to investigate techniques and technologies for interlinking packet networks of various kinds. The objective was to develop communication protocols which would allow networked computers to communicate transparently across multiple, linked packet networks. This was called the Internetting project and the system of networks which emerged from the research was known as the “Internet.” The system of protocols which was developed over the course of this research effort became known as the TCP/IP Protocol Suite, after the two initial protocols developed: Transmission Control Protocol (TCP) and Internet Protocol (IP).

In 1986, the U.S. National Science Foundation (NSF) initiated the development of the NSFNET which, today, provides a major backbone communication service for the Internet. With its 45 megabit per second facilities, the NSFNET carries on the order of 12 billion packets per month between the networks it links. The National Aeronautics and Space Administration (NASA) and the U.S. Department of Energy contributed additional backbone facilities in the form of the NSINET and ESNET respectively. In Europe, major international backbones such as NORDUNET and others provide connectivity to over one hundred thousand computers on a large number of networks. Commercial network providers in the U.S. and Europe are beginning to offer Internet backbone and access support on a competitive basis to any interested parties.

"Regional" support for the Internet is provided by various consortium networks and "local" support is provided through each of the research and educational institutions. Within the United States, much of this support has come from the federal and state governments, but a considerable contribution has been made by industry. In Europe and elsewhere, support arises from cooperative international efforts and through national research organizations. During the course of its evolution, particularly after 1989, the Internet system began to integrate support for other protocol suites into its basic networking fabric. The present emphasis in the system is on multiprotocol interworking, and in particular, with the integration of the Open Systems Interconnection (OSI) protocols into the architecture.

Both public domain and commercial implementations of the roughly 100 protocols of TCP/IP protocol suite became available in the 1980's. During the early 1990's, OSI protocol implementations also became available and, by the end of 1991, the Internet has grown to include some 5,000 networks in over three dozen countries, serving over 700,000 host computers used by over 4,000,000 people.

A great deal of support for the Internet community has come from the U.S. Federal Government, since the Internet was originally part of a federally-funded research programme and, subsequently, has become a major part of the U.S. research infrastructure. During the late 1980's, however, the population of Internet users and network constituents expanded internationally and began to include commercial facilities. Indeed, the bulk of the system today is made up of private networking facilities in educational and research institutions, businesses and in government organizations across the globe. The Coordinating Committee for Intercontinental Networks (CCIRN), which was organized by the U.S. Federal Networking Council (FNC) and the European Reseaux Associees pour la Recherche Europeenne (RARE), plays an important role in the coordination of plans for government- sponsored research networking. CCIRN efforts have been a stimulus for the support of international cooperation in the Internet environment.

Internet Technical Evolution

Over its fifteen year history, the Internet has functioned as a collaboration among cooperating parties. Certain key functions have been critical for its operation, not the least of which is the specification of the protocols by which the components of the system operate. These were originally developed in the DARPA research programme, but in the last five or six years, this work has been undertaken on a wider basis with support from Government agencies in many countries, industry and the academic community. The Internet Activities Board (IAB) was created in 1983 to guide the evolution of the TCP/IP Protocol Suite and to provide research advice to the Internet community.

During the course of its existence, the IAB has reorganized several times. It now has two primary components: the Internet Engineering Task Force and the Internet Research Task Force. The former has primary responsibility for further evolution of the TCP/IP protocol suite, its standardization with the concurrence of the IAB, and the integration of other protocols into Internet operation (*e.g.* the Open Systems

Interconnection protocols). The Internet Research Task Force continues to organize and explore advanced concepts in networking under the guidance of the Internet Activities Board and with support from various government agencies.

A secretariat has been created to manage the day-to-day function of the Internet Activities Board and Internet Engineering Task Force. IETF meets three times a year in plenary and its approximately 50 working groups convene at intermediate times by electronic mail, teleconferencing and at face-to-face meetings. The IAB meets quarterly face-to-face or by videoconference and at intervening times by telephone, electronic mail and computer-mediated conferences.

Two other functions are critical to IAB operation: publication of documents describing the Internet and the assignment and recording of various identifiers needed for protocol operation. Throughout the development of the Internet, its protocols and other aspects of its operation have been documented first in a series of documents called Internet Experiment Notes and, later, in a series of documents called Requests for Comment (RFCs). The latter were used initially to document the protocols of the first packet switching network developed by DARPA, the ARPANET, beginning in 1969, and have become the principal archive of information about the Internet. At present, the publication function is provided by an RFC editor.

The recording of identifiers is provided by the Internet Assigned Numbers Authority (IANA) who has delegated one part of this responsibility to an Internet Registry which acts as a central repository for Internet information and which provides central allocation of network and autonomous system identifiers, in some cases to subsidiary registries located in various countries. The Internet Registry (IR) also provides central maintenance of the Domain Name System (DNS) root database which points to subsidiary distributed DNS servers replicated throughout the Internet. The DNS distributed database is used, inter alia, to associate host and network names with their Internet addresses and is critical to the operation of the higher level TCP/IP protocols including electronic mail.

There are a number of Network Information Centers (NICs) located throughout the Internet to serve its users with documentation, guidance, advice and assistance. As the Internet continues to grow internationally, the need for high quality NIC functions increases. Although the initial community of users of the Internet were drawn from the ranks of computer science and engineering, its users now comprise a wide range of disciplines in the sciences, arts, letters, business, military and government administration.

Related Networks

In 1980-81, two other networking projects, BITNET and CSNET, were initiated. BITNET adopted the IBM RSCS protocol suite and featured direct leased line connections between participating sites. Most of the original BITNET connections linked IBM mainframes in university data centres. This rapidly changed as protocol implementations became available for other machines.

From the beginning, BITNET has been multi-disciplinary in nature with users in all academic areas. It has also provided a number of unique services to its users. Today, BITNET and its parallel networks in other parts of the world (*e.g.*, EARN in Europe) have several thousand participating sites. In recent years, BITNET has established a backbone which uses the TCP/IP protocols with RSCS-based applications running above TCP.

CSNET was initially funded by the National Science Foundation (NSF) to provide networking for university, industry and government computer science research groups. CSNET used the Phonenet MMDF protocol for telephone-based electronic mail relaying and, in addition, pioneered the first use of TCP/IP over X.25 using commercial public data networks. The CSNET name server provided an early example of a white pages directory service and this software is still in use at numerous sites. At its peak, CSNET had approximately 200 participating sites and international connections to approximately fifteen countries.

In 1987, BITNET and CSNET merged to form the Corporation for Research and Educational Networking (CREN). In the Fall of 1991, CSNET service was discontinued having fulfilled its important early role in the provision of academic networking service. A key feature of CREN is that its operational costs are fully met through dues paid by its member organizations.

A Brief History of Computer Networking and the Internet

An overview of technology of computer networking and the Internet. You should know enough now to impress your family and friends. However, if you really want to be a big hit at the next cocktail party, you should sprinkle your discourse with tidbits about the fascinating history of the Internet.

1961-1972: Development and Demonstration of Early Packet Switching Principles

The field of computer networking and today's Internet trace their beginnings back to the early 1960s, a time at which the telephone network was the world's dominant communication network. The telephone network uses circuit switching to transmit information from a sender to receiver—an appropriate choice given that voice is transmitted at a constant rate between sender and receiver. Given the increasing importance (and great expense) of computers in the early 1960's and the advent of timeshared computers, it was perhaps natural (at least with perfect hindsight!) to consider the question of how to hook computers together so that they could be shared among geographically distributed users. The traffic generated by such users was likely to be "bursty"—intervals of activity, *e.g.*, the sending of a command to a remote computer, followed by periods of inactivity, while waiting for a reply or while contemplating the received response.

Three research groups around the world, all unaware of the others' work, began inventing the notion of packet switching as an efficient and robust alternative to circuit switching. The first published work on packet-switching techniques was the work by Leonard Kleinrock, at that time a graduate student at MIT. Using queuing theory, Kleinrock's work elegantly demonstrated the effectiveness of the packet-switching approach for bursty traffic sources. At the same time, Paul Baran at the Rand Institute had begun investigating the use of packet switching for secure voice over military networks, while at the National Physical

Laboratory in England, Donald Davies and Roger Scantlebury were also developing their ideas on packet switching.

The work at MIT, Rand, and NPL laid the foundations for today's Internet. But the Internet also has a long history of a "Let's build it and demonstrate it" attitude that also dates back to the early 1960's. J.C.R. Licklider and Lawrence Roberts, both colleagues of Kleinrock's at MIT, both went on to lead the computer science programme at the Advanced Projects Research Agency (ARPA) in the United States. Roberts published an overall plan for the so-called ARPAnet, the first packet-switched computer network and a direct ancestor of today's public Internet.

The early packet switches were known as Interface Message Processors (IMP's) and the contract to build these switches was awarded to BBN. On Labor Day in 1969, the first IMP was installed at UCLA, with three additional IMP being installed shortly thereafter at the Stanford Research Institute, UC Santa Barbara, and the University of Utah. The fledgling precursor to the Internet was four nodes large by the end of 1969. Kleinrock recalls the very first use of the network to perform a remote login from UCLA to SRI crashing the system.

By 1972, ARPAnet had grown to approximately 15 nodes, and was given its first public demonstration by Robert Kahn at the 1972 International Conference on Computer Communications. The first host-to-host protocol between ARPAnet end systems known as the Network Control Protocol (NCP) was completed [RFC 001]. With an end-to-end protocol available, applications could now be written. The first e-mail programme was written by Ray Tomlinson at BBN in 1972.

1972-1980: Internetworking, and New and Proprietary Networks

The initial ARPAnet was a single, closed network. In order to communicate with an ARPAnet host, one had to actually be attached to another ARPAnet IMP.

In the early to mid 1970's, additional packet-switching networks besides ARPAnet came into being; ALOHAnet, a satellite network linking together universities on the Hawaiian islands; Telenet, a BBN commercial packet-switching network based on ARPAnet technology; Tymnet; and Transpac, a French packet-switching network. The number of networks was beginning to grow. In 1973, Robert Metcalfe's PhD thesis laid out the principle of Ethernet, which would later lead to a huge growth in so-called Local Area Networks (LANs) that operated over a small distance based on the Ethernet protocol.

Once again, with perfect hindsight one might now see that the time was ripe for developing an encompassing architecture for connecting networks together. Pioneering work on interconnecting networks (once again under the sponsorship of DARPA), in essence creating a *network of networks*, was done by Vinton Cerf and Robert Kahn; the term "internetting" was coined to describe this work. The architectural principles that Kahn' articulated for creating a so-called "open network architecture" are the foundation on which today's Internet is built:

- Minimalism, autonomy: a network should be able to operate on its own, with no internal changes required for it to be internetworked with other networks;

- Best effort service: internetworked networks would provide best effort, end-to-end service. If reliable communication was required, this could accomplished by retransmitting lost messages from the sending host;
- Stateless routers: the routers in the internetworked networks would not maintain any per-flow state about any ongoing connection
- Decentralized control: there would be no global control over the internetworked networks.

These principles continue to serve as the architectural foundation for today's Internet, even 25 years later - a testament to insight of the early Internet designers. These architectural principles were embodied in the TCP protocol. The early versions of TCP, however, were quite different from today's TCP. The early versions of TCP combined a reliable in-sequence delivery of data via end system retransmission (still part of today's TCP) with forwarding functions (which today are performed by IP). Early experimentation with TCP, combined with the recognition of the importance of an unreliable, non-flow-controlled end-end transport service for application such as packetized voice, led to the separation of IP out of TCP and the development of the UDP protocol. The three key Internet protocols that we see today—TCP, UDP and IP—were conceptually in place by the end of the 1970's.

In addition to the DARPA Internet-related research, many other important networking activities were underway. In Hawaii, Norman Abramson was developing ALOHAnet, a packet-based radio network that allowed multiple remote sites on the Hawaiian islands to communicate with each other. The ALOHA protocol was the first so-called multiple access protocol, allowing geographically distributed users to share a single broadcast communication medium (a radio frequency).

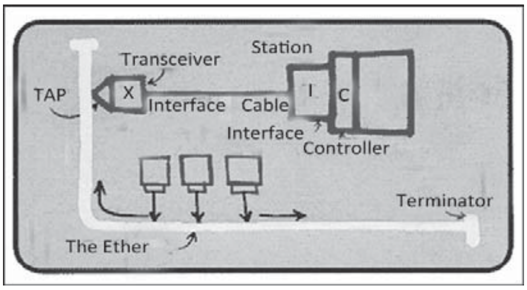


Fig. A 1976 drawing by R. Metcalfe of the Ethernet concept (from Charles Spurgeon's Ethernet Web Site)

Abramson's work on multiple access protocols was built upon by Robert Metcalfe in the development of the Ethernet protocol for wire-based shared broadcast networks. Interestingly, Metcalfe's Ethernet protocol was motivated by the need to connect multiple PCs, printers, and shared disks together. Twenty-five years ago, well before the PC revolution and the explosion of networks, Metcalfe and his colleagues were laying the foundation for today's PC LANs. Ethernet technology represented an important step for internetworking as well. Each Ethernet local area network was itself a network, and as the number of LANs proliferated, the need to internetwork these LANs together became all the more important. An excellent source for information on Ethernet is Spurgeon's Ethernet Web Site, which includes Metcalfe's drawing of his Ethernet concept.

In addition to the DARPA internetworking efforts and the Aloha/Ethernet multiple access networks, a number of companies were developing their own proprietary network architectures. Digital Equipment Corporation (Digital) released the first version of the DECnet in 1975, allowing two PDP-11 minicomputers to communicate with each other. DECnet has continued to evolve since then, with significant portions of the OSI protocol suite being based on ideas pioneered in DECnet. Other important players during the 1970's were Xerox (with the XNS architecture) and IBM (with the SNA architecture). Each of these early networking efforts would contribute to the knowledge base that would drive networking in the 80's and 90's. It is also worth noting here that in the 1980's (and even before), researchers were also developing a "competitor" technology to the Internet architecture. These efforts have contributed to the development of the ATM (Asynchronous Transfer Mode) architecture, a connection-oriented approach based on the use of fixed size packets, known as cells. We will examine portions of the ATM architecture throughout this book.

1980-1990: A Proliferation of Networks

By the end of the 1970's approximately 200 hosts were connected to the ARPAnet. By the end of the 1980's the number of host connected to the public Internet, a confederation of networks looking much like today's Internet would reach 100,000. The 1980's would be a time of tremendous growth. Much of the growth in the early 1980's resulted from several distinct efforts to create computer networks linking universities together. BITnet (Because It's There NETwork) provided e-mail and file transfers among several universities in the Northeast. CSNET (Computer Science NETwork) was formed to link together university researchers without access to ARPAnet. In 1986, NSFNET was created to provide access to NSF-sponsored supercomputing centres. Starting with an initial backbone speed of 56Kbps, NSFNET's backbone would be running at 1.5 Mbps by the end of the decade, and would be serving as a primary backbone linking together regional networks.

In the ARPAnet community, many of the final pieces of today's Internet architecture were falling into place. January 1, 1983 saw the official deployment of TCP/IP as the new standard host protocol for Arpanet (replacing the NCP protocol). The transition from NCP to TCP/IP was a "flag day" type event—all host were required to transfer over to TCP/IP as of that day. In the late 1980's, important extensions were made to TCP to implement host-based congestion control. The Domain Name System, used to map between a human-readable Internet name (*e.g.*, gaia.cs.umass.edu) and its 32-bit IP address, was also developed.

Paralleling this development of the ARPAnet (which was for the most part a US effort), in the early 1980s the French launched the Minitel project, an ambitious plan to bring data networking into everyone's home.

Sponsored by the French government, the Minitel system consisted of a public packet-switched network (based on the X.25 protocol suite, which uses virtual circuits), Minitel servers, and inexpensive terminals with built-in low speed modems. The Minitel became a huge success in 1984 when the French government gave away a free Minitel terminal to each French household that wanted one.

Minitel sites included free sites—such as a telephone directory site—as well as private sites, which collected a usage-based fee from each user. At its peak in the mid 1990s, it offered more than 20,000 different services, ranging from home banking to specialized research databases. It was used by over 20% of France's population, generated more than $1 billion each year, and created 10,000 jobs. The Minitel was in a large fraction of French homes ten years before most Americans had ever heard of the Internet. It still enjoys widespread use in France, but is increasingly facing stiff competition from the Internet.

The 1990s: Commercialization and the Web

The 1990's were issued in with two events that symbolized the continued evolution and the soon-to-arrive commercialization of the Internet. First, ARPAnet, the progenitor of the Internet ceased to exist. MILNET and the Defense Data Network had grown in the 1980's to carry most of the US Department of Defense related traffic and NSFNET had begun to serve as a backbone network connecting regional networks in the United States and national networks overseas. Also, in 1990, The World (http://gaia.cs.umass.edu/kurose/introduction/www.world.std.com) became the first public dialup Internet Service Provider (ISP). In 1991, NSFNET lifted its restrictions on use of NSFNET for commercial purposes. NSFNET itself would be decommissioned in 1995, with Internet backbone traffic being carried by commercial Internet Service Providers.

The main event of the 1990's however, was to be the release of the World Wide Web, which brought the Internet into the homes and businesses of millions and millions of people, worldwide. The Web also served as a platform for enabling and deploying hundreds of new applications, including on-line stock trading and banking, streamed multimedia services, and information retrieval services.

The WWW was invented at CERN by Tim Berners-Lee in 1989-1991, based on ideas originating in earlier work on hypertext from the 1940's by Bush and since the 1960's by Ted Nelson. Berners-Lee and his associates developed initial versions of HTML, HTTP, a Web server and a browser—the four key components of the WWW. The original CERN browsers only provided a line-mode interface. Around the end of 1992 there were about 200 Web servers in operation, this collection of servers being the tip of the iceberg for what was about to come. At about this time several researchers were developing Web browsers with GUI interfaces, including Marc Andreesen, who developed the popular GUI browser Mosaic for X. He released an alpha version of his browser in 1993, and in 1994 formed Mosaic Communications, which later became Netscape Communications Corporation. By 1995 university students were using Mosaic and Netscape browsers to surf the Web on a daily basis. At about this time the US government began to transfer the control of the Internet backbone to private carriers. Companies—big and small—began to operate Web servers and transact commerce over the Web. In 1996 Microsoft got into the Web business in a big way, and in the late 1990s it was sued for making its browser a central component of its operating system. In 1999 there were over two-million Web servers in operation. And all of this happened in less than ten years!

During the 1990's, networking research and development also made significant advances in the areas of high-speed routers and routing and local area networks. The technical community struggled with the problems of defining and implementing an Internet service model for traffic requiring real-time constraints, such as continuous media applications. The need to secure and manage Internet infrastructure also became of paramount importance as e-commerce applications proliferated and the Internet became a central component of the world's telecommunications infrastructure.

Sharing Computer Network Logs for Security and Privacy

Log data is an essential resource to security teams at any organization large enough to hire full-time IT personnel. While IDSs can operate directly upon streaming network data, matching signatures and producing alerts, it is still necessary for human beings to examine logs to understand these alerts. Logs also form the core source of evidence for computer forensic investigations following security incidents. In addition to these very applied uses, logs are important to security researchers, for instance, those involved with research honeynets.

It is typical in the current security culture for each autonomous organization to use log data only to locally optimize network management and security protection. For example, when an organization notices an Internet attack (*e.g.*, an external reconnaissance scan) a typical reaction is to block the offending IP addresses at the organization's perimeter but not to alert others—even administrators of the offending network— about this activity. Another example of this type of behaviour is reactively scanning for a vulnerability on all the organization's systems after noticing vulnerabilities being exploited, but not alerting others of this activity. Although these examples are not universally true, as some security engineers have trusted channels for sharing security events, such sharing is the exception. There is a culture of pushing attackers away from oneself without any consideration of the poor overall security resulting from this lack of coordination between organizations. It is analogous to local policeman chasing criminals from one jurisdiction to another without crossing jurisdictional boundaries.

In these ways, administrators may miss the bigger picture and are unlikely to notice when they are just a piece of a larger target. Indeed, there are very few cross-sectional views of the Internet, and until recently there have been no mechanisms to enable such wider views. Furthermore, current examples of wide views, such as spam blacklists and worm signatures, are often focused on a specific characteristic even though signatures are gathered from events across the entire Internet. While security professionals are having problems sharing logs, sharing data is in fact quite common among attackers.

They trade zombies, publicly post information on vulnerable systems/networks and coordinate attacks. Recent events at several U.S. supercomputing centres have demonstrated examples of coordinated attacks against organizations that do not have good mechanisms in place for data sharing and log correlation.

These problems highlight why it is no longer satisfactory to focus solely on the local picture; there is a need to look globally across the Internet. And while the data needed exists, tapping into thousands of data sources effectively and sharing critical information—intelligently and to the data owners' satisfaction—is an open problem.

The importance of solving this problem has even caught the government's attention as the Department of Homeland Security has recognized the importance of sharing information and established Information Sharing and Analysis Centers (ISACs) to facilitate the storage and sharing of information about security threats. The importance of log sharing has also gained industry recognition with investments in infrastructure dedicated solely for this purpose across multiple industry sectors.

The National Strategy to Secure Cyberspace (NSSC) explicitly lists sharing as one of its highest priorities—data sharing within the government, within industry sectors and between the government and industry. In fact, of the eight action items reached in the NSSC report, three of them are directly related to log data sharing: Item 2: "Provide for the development of tactical and strategic analysis of cyber attacks and vulnerability assessments"; Item 3: "Encourage the development of a private sector capability to share a synoptic view of the health of cyberspace"; and Item 8: "Improve and enhance public/private information sharing involving cyber-attacks, threats, and vulnerabilities".

However, the reluctance to share logs—which has resulted in fewer entities sharing—is understandable due to the sensitivity of the information contained within logs. Logs may be accidently mishandled by friendly peers, or fall directly/ indirectly into the hands of malicious crackers. Security engineers have enough concerns without worrying about being a contributor to a security compromise of their own organization, or even worse, creating third party liability to a security compromise of another organization.

The first phase of any digital attack is reconnaissance, and logs are like a treasure map for would-be attackers. Access to computer and network logs can provide intruders with special views of a network not visible from the outside, even with scanning tools. Information gleaned from these logs could indicate potential bottlenecks for DoS attacks or could even contain passwords—as often happens when a user accidentally types a password into the username field. Logs can even be used to identify machines infected by worms, which are most likely not well-maintained or monitored. Soft targets such as these can be used to get a foothold into a network.

While some would claim that the difficulties in sharing logs is social, we believe the problems are technical at the heart. To share logs and address these concerns about the sensitivity of the information within them, anonymization techniques must be employed.

However, the field of log anonymization is still immature. There are very few tools, and the ones that exist are deficient in many ways. Further, current anonymization tools are one-size-fits-all, or better put one-size-tries-to-fit-all. Ideally, they would support multiple levels of anonymization that trade-off between security—of the anonymization scheme— and utility—the amount of useful information retained in anonymized logs. Thus far, no log anonymizers—besides a tool we recently developed for NetFlow anonymization — support multiple levels of anonymization, even though there are typically multiple levels of trust between parties who might wish to share logs and those with whom they would share their logs.

We believe a new anonymization framework must be created that supports trade-offs between security and utility by providing multiple levels of anonymization. To achieve this goal two important research problems must be solved. *First*, a metric must be created for the utility of a log that is based on the fields or data types within that log. Utility should be measured by the types of attacks that can be detected with a log or set of logs. *Second*, a metric for the security of an anonymization scheme must be developed. This metric should be based upon the types of attacks that can be used against an anonymization scheme—a log and the anonymization algorithms used on it. The difficulty of the attack and the amount of information that can be obtained by reversing the anonymization will both affect this metric. This new framework should be based upon the data types and fields within logs rather than the specific log types and versions.

The prototype tools we are developing handle several log formats, but more importantly a framework that is extensible to handle almost any log is needed. Additionally, guidelines and standards must be developed to help organizations map trust levels to anonymization levels. In this way, organizations will be able to customize anonymization to fit their needs for the first time.

3

The Scope of National Cyber Security

Where such precision is most required is in *definitions*. Having no legal force itself, the Policy arguably does not require the sort of legal precision one would expect of an act of Parliament, for example. Yet the Policy deals in terms plagued with ambiguity, *cyber security*not the least among them. In forgoing basic definitions, the Policy fails to define its own scope, and as a result it proves remarkably broad and arguably unfocused.

The Policy's preamble comes close to defining *cyber security* in paragraph 5 when it refers to "cyber related incident[s] of national significance" involving "extensive damage to the information infrastructure or key assets…[threatening] lives, economy and national security." Here at least is a picture of cyber security on a national scale, a picture which would be quite familiar to Western policymakers: computer security practices "fundamental to both protecting government secrets and enabling national defence, in addition to protecting the critical infrastructures that permeate and drive the 21st century global economy."

Here the Policy runs afoul of a common pitfall: conflating threats to the state or society writ large (e.g. cyber warfare, cyber espionage, cyber terrorism) with threats to businesses and individuals (e.g. fraud, identity theft). Although both sets of threats may be fairly described as cyber security threats, only the former is worthy of the term *national* cyber security. The latter would be better characterized as cyber *crime*. The distinction is an important one, lest cyber crime be "securitized," or elevated to an issue of national security. National cyber security has already provided the justification for the much decried Central Monitoring System (CMS). Expanding the range of threats subsumed under this rubric may provide a pretext for further surveillance efforts on a national scale.

Apart from mission creep, this vague and overly broad conception of national cyber security risks overwhelming an as yet underdeveloped system with more responsibilities than it may be able to handle.

Where cyber crime might be left up to the police, its inclusion alongside true national-level cyber security threats in the Policy suggests it may be handled by the new "nodal agency" mentioned in section IV. Thus clearer definitions would not only provide the Policy with a more focused scope, but they would also make for a more efficient distribution of already scarce resources.

What It Get Right

Definitions aside, the Policy actually gets a lot of things right — at least as an aspirational document. It certainly covers plenty of ground, mentioning everything from information sharing to procedures for risk assessment / risk management to supply chain security to capacity building. It is a sketch of what could be a very comprehensive national cyber security strategy, but without more specifics, it is unlikely to reach its full potential. Overall, the Policy is much of what one might expect from a first draft, but certain elements stand out as worthy of special consideration.

First and foremost, the Policy should be commended for its commitment to "[safeguarding] privacy of citizen's data" (sic). Privacy is an integral component of cyber security, and in fact other states' cyber security strategies have entire segments devoted specifically to privacy. India's Policy stands to be more specific as to the *scope* of these safeguards, however. Does the Policy aim primarily to safeguard data from criminals? Foreign agents? Could it go so far as to protect user data even from its *own* agents? Indeed this commitment to privacy would appear at odds with the recently unveiled CMS. Rather than merely paying lip service to the concept of online privacy, the government would be well advised to pass legislationprotecting citizens' privacy and to use such legislation as the foundation for a more robust cyber security strategy.

The Policy also does well to advocate "fiscal schemes and incentives to encourage entities to install, strengthen and upgrade information infrastructure with respect to cyber security." Though some have argued that such regulation would impose inordinate costs on private businesses, anyone with a cursory understanding of computer networks and microeconomics could tell you that “externalities in cyber security are so great that even the freest free market would fail”—to quote expert Bruce Schneier. In less academic terms, a network is only as strong as its weakest link. While it is true that many larger enterprises take cyber security quite seriously, small and medium-sized businesses either lack immediate incentives to INVEST in security (e.g. no shareholders to answer to) or more often lack the basic resources to do so. Some form of government transfer for cyber security related investments could thus go a long way toward shoring up the country’s overall security.

The Policy also “[encourages] wider usage of Public Key Infrastructure (PKI) within Government for trusted communication and transactions.” It is surprising, however, that the Policy does not *mandate* the usage of PKI. In general, the document provides relatively few details on what specific security practices operators of Critical Information Infrastructure (CII) can or should implement.

Where It Goes Wrong

One troubling aspect of the Policy is its ambiguous language with respect to acquisition policies and supply chain security in general. The Policy, for example, aims to “[mandate] security practices related to the design, *acquisition*, development, use and operation of information resources” (emphasis added). Indeed, section VI, subsection A, paragraph 8 makes reference to the “procurement of indigenously manufactured ICT products,” presumably to the exclusion of imported goods. Although supply chain security must inevitably factor into overall cyber security concerns, such restrictive acquisition policies could not only deprive critical systems of potentially higher-quality alternatives but—depending on the implementation of these policies—could also sharpen the vulnerabilitiesof these systems.

Not only do these preferential acquisition policies risk mandating lower quality products, but it is unlikely they will be able to keep pace with the rapid pace of innovation in information technology. The United States provides a cautionary tale. The U.S. National Institute of Standards and Technology (NIST), tasked with producing cyber security standards for operators of critical infrastructure, made its first update to a 2005 set of standards earlier this year. Other regulatory agencies, such as the Federal Energy Regulatory Commission (FERC) move at a marginally faster pace yet nevertheless are delayed by bureaucratic processes. FERC has already moved to implement Version 5 of its Critical Infrastructure Protection (CIP) standards, nearly a year before the deadline for Version 4 compliance. The need for new standards thus outpaces the ability of industry to effectively implement them.

Fortunately, U.S. cyber security regulation has so-far been technology-neutral. Operators of Critical Information Infrastructure are required only to ensure certain functionalities and not to procure their hardware and software from any particular supplier. This principle ensures competition and thus security, allowing CII operators to take advantage of the most cutting-edge technologies regardless of name, model, etc. Technology neutrality does of course raise risks, such as those emphasized by the Government of India regarding Huawei and ZTE in 2010. Risk assessment must, however, remain focused on the technology in question and avoid politicization. India's cyber security policy can be technology neutral as long as it follows one additional principle: *trust but verify*. Verification may be facilitated by the use of free and open-source software (FOSS). FOSS provides *security through transparency* as opposed to *security through obscurity* and thus enables more agile responses to security responses. Users can identify and patch bugs themselves, or otherwise take advantage of the broader user community for such fixes. Thus open-source software promotes security in much the same way that competitive markets do: by accepting a wide range of inputs.

Despite the virtues of FOSS, there are plenty of good reasons to run proprietary software, e.g. fitness for purpose, cost, and track record. Proprietary software makes verification somewhat more complicated but not impossible. Source code escrow agreements have recently gained some traction as a verification measure for proprietary software, even with companies like Huawei and ZTE. In 2010, the infamous Chinese telecommunications giantspersuaded the Indian government to lift its earlier ban on their products by concluding just such an agreement. Clearly *trust but verify* is imminently practicable, and thus technology neutrality.

What's Missing

Level of detail aside, what is most conspicuously absent from the new Policy is any framework for institutional cooperation beyond 1) the designation of CERT-In "as a

Nodal Agency for coordination of all efforts for cyber security emergency response and crisis management" and 2) the designation of the "National Critical Information Infrastructure Protection Centre (NCIIPC) to function as the nodal agency for critical information infrastructure protection in the country." The Policy mentions additionally "a National nodal agency to coordinate all matters related to cyber security in the country, with clearly defined roles & responsibilities." Some clarity with regard to roles and responsibilities would certainly be in order. Even among these three agencies—assuming they are all distinct—it is unclear who is to be responsible for what.

More confusing still is the number of other pre-existing entities with cyber security responsibilities, in particular the National Technical Research Organization (NTRO), which in an earlier draft of the Policy was to have authority over the NCIIPC. The Ministry of Defence likewise has bolstered its cyber security and cyber warfare capabilities in recent years. Is it appropriate for these to play a role in securing civilian CII? Finally, the already infamous Central Monitoring System, justified predominantly on the very basis of cyber security, receives no mention at all. For a government that is only now releasing its first cyber security policy, India has developed a fairly robust set of institutions around this issue. It is disappointing that the Policy does not more fully address questions of roles and responsibilities among government entities.

Next Steps

India's inaugural National Cyber Security Policy is by and large a step in the right direction. It covers many of the most pressing issues in national cyber security and lays out a number of ambitious goals, ranging from capacity building to robust public-private partnerships. To realize these goals, the government will need a much more detailed roadmap. Firstly, the extent of the government's proposed privacy safeguards must be clarified and ideally backed by a separate piece of privacy legislation. As Benjamin Franklin once said, "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety." When it comes to cyberspace, the Indian people must demand both liberty and safety.

Secondly, the government should avoid overly preferential acquisition policies and allow risk assessments to be technologically rather than politically driven. Procurement should moreover be technology-neutral. Open source software and source code escrow agreements can facilitate the verification measures that make technology neutrality work.

Finally, to translate this policy into a sound *strategy* will necessarily require that India's various means be directed toward specific ends. The Policy hints at organizational mapping with references to CERT-In and the NCIIPC, but the roles and responsibilities of other government agencies as well as the private sector remain underdetermined. Greater clarity on these points would improve inter-agency and public-private cooperation—and thus, one hopes, security—significantly.

Not only is there a lack of coordination among government cyber security entities, but there is no mention of how the public and private sectors are to cooperate on cyber security information—other than oblique references to “public-private partnerships.” Certainly there is a need for information sharing, which is currently facilitated in part by the sector-level CERTS. More interesting, however, is the question of liability for high-impact cyber attacks. To whom are private CII operators accountable in the event of disruptive cyber attacks on their systems? This legal ambiguity must necessarily be resolved in conjunction with the “fiscal schemes and incentives” also alluded to in the Policy in order to motivate strong cyber security practices among all CII operators and the public more broadly.

National Cyber Security Policy

IT as an engine for economic growth and prosperity

The IT sector has become one of the most significant growth catalysts for the Indian economy. In addition to fuelling India’s economy, this sector is also positively influencing the lives of its people through direct and indirect contribution to the various socio-economic parameters such as employment, standard of living and diversity among others.

The sector has played a significant role in transforming India’s image to that of a global player in providing world-class technology solutions and business services. The government has been a key driver for increased adoption of IT-based products and solutions in the country. It has embarked on various IT-enabled initiatives including in Public services (Government to citizen services, citizen identification, public distribution systems), Healthcare (telemedicine, remote consultation, mobile clinics), Education (e- Learning, virtual classrooms, etc.) and Financial service (mobile banking/payment gateways), etc. In addition, Government sector has enabled increased IT adoption in the country through sectors reforms that encourage IT acceptance and National programmes such as National eGovernance Programmes (NeGP) and the Unique Identification Development Authority of India (UIDAI) programme that create large scale IT infrastructure and promote corporate participation.

Security of cyber space - Need for action

In light of the growth of IT sector in the country, ambitious plans for rapid social transformation & inclusive growth and India's prominent role in the IT global market, providing right kind of focus for secure computing environment and adequate trust & confidence in electronic transactions becomes one of the compelling priorities for the country.

This kind of focus enables creation of suitable cyber security eco system in the country, in tune with globally networked environment and at the same time assures its citizens as well the global community about the seriousness of its intentions and ability to act suitably.

Target audience

The cyber security policy is an evolving task, which need to be regularly updated/refined in line with technological trends and security challenges posed by such technology directions.

This policy caters for the whole spectrum of ICT users and providers including small and home users, medium and large enterprises and Government & non-Government entities. It proviides an over view of what it takes to effectively protect information, information systems & networks and also to provide an insight into the Government's approach and strategy for protection of cyber space in the country. It also outlines some pointers to enable collaborative working of all key players in public & private to safeguard country's information and information systems. This policy, therefore, aims to create a cyber security framework, which will address all the related issues over a long period. The framework will lead to specific actions and programmes to enhance the security posture of country's cyber space.

Securing cyber space – Key policy considerations

The key considerations for securing the cyber space include:

- The security of cyber space is not an optional issue but an imperative need in view of its impact on national security, public safety and economic well-being.
- The issue of cyber security needs to move beyond traditional technological measures such as anti-virus and firewalls. It needs to be dynamic in nature and have necessary depth to detect, stop and prevent attacks.
- Cyber security intelligence forms an integral component of security of cyber space in order to be able to anticipate attacks, adopt suitable counter measures and attribute the attacks for possible counter action.
- Effective correlation of information from multiple sources and real-time monitoring of assets that need

protection and at the same time ensuring that adequate expertise and process are in place to deal with crisis situations.

- There is a need to focus on having a suitable security posture and adopt counter measures on the basis of hierarchy of priority and understanding of the inter dependencies, rather than attempting to defend against all intrusions and attacks.
- Security is all about what people, process and technology and as such there is a clear need for focusing on people and processes while attempting to use the best available technological solutions, which otherwise could prove ineffective.
- Use of adequately trained and qualified manpower along with suitable incentives for effective results in a highly specialized field of cyber security.
- Security needs to be built-in from the conceptual design stage itself when it comes to developing and deploying critical information infrastructure, as opposed to having security as an afterthought.

Cyber space – Nature of threat

Threat landscape

Existing and potential threats in the sphere of cyber security are among the most serious challenges of the 21st century. Threats emanate from a wide variety of sources, and manifest themselves in disruptive activities that target individuals, businesses, national infrastructures, and governments alike. Their effects carry significant risk for public safety, the security of nations and the stability of the globally linked international community as a whole. Malicious use of information technology can easily be concealed. The origin, identity of the perpetrator, or motivation for the disruption can be difficult to ascertain. Often, the perpetrators of these activities can only be inferred from the target, the effect or other circumstantial evidence. Threat actors can operate with substantial impunity from virtually anywhere. The motives for disruption vary widely, from simply demonstrating technical prowess, to the theft of money or information, or as an extension of state conflict. The source of these threats includes non-state actors such as criminals and, potentially, terrorists as well as States themselves. Many malicious tools and methodologies originate in the efforts of criminals and hackers. The growing sophistication and scale of criminal activity increases the potential for harmful actions.

International cooperation

Increasingly, nations are also concerned that the ICT supply chain could be influenced or subverted in ways that would affect normal, secure and reliable use of information technology. Inclusion of malicious hidden functions in information technology can undermine confidence in products and services, erode trust in commerce, and affect national security. As disruptive activities using information technology grow more complex and dangerous, it is obvious that no nation is able to address these threats alone. Confronting the challenges of the 21st century depends on successful cooperation among like-minded partners. Collaboration among nations, and between nations, the private sector and civil society, is important and the effectiveness of measures to improve cyber security requires broad international cooperation.

Securing cyber space – Scope of action

Cyber security and cyber defence

Cyber security is the activity of protecting information and information systems (networks, computers, data bases, data centers and applications) with appropriate procedural and technological security measures. In that sense, the notion of cyber security is quite generic and encompasses all protection activities.

Cyber defence relates to a much more specialized activity linked to particular aspects and organizations. The distinguishing factors between cyber security and cyber defence in a network environment are the nature of the threat, the assets that need to be protected and the mechanisms applied to ensure that protection. Cyber defence relates to defensive actions against activities primarily originating from hostile actors that have political, quasi-political or economic motivation that have an impact on national security, public safety or economic well being of the society.

The cyber defence environment requires deployment of technologies and capabilities for real-time protection and incident response. Generally, cyber defence is driven by intelligence on the threat to achieve the kind of defence that directs, collects, analysis and disseminates the relevant actionable intelligence information to the stakeholders concerned for necessary proactive, preventive and protective measures. The effectiveness of cyber defence lies in the proactive nature of security counter measures as well as in ensuring resilience and continuity of operations, despite the possibilities of successful attacks.

Cyber intelligence and cyber defence

The value of collecting intelligence information about threat sources and possible cyber attacks cannot be underestimated. A well-deployed cyber attack can yield vital information that compromises communication and encryption ciphers.

It tends to project the power of the attacker and demoralize the victim. However, the changing phase of cyber attacks as well as ever- increasing sophistication of attack methods have complicated the efforts of collecting valuable intelligence information for effective proactive, preventive and protective measures. Generally, attacks directed against Govt. and critical information infrastructure can be categorized as either

massive attacks, aimed at disabling the infrastructure rendering it unusable or inaccessible to users; or targeted attacks, aimed at collecting sensitive/strategic information. Massive attacks generally take the form of denial of service attacks against the infrastructure.

The targeted attacks involve a good deal of customization and personalization of attack methods and levels of technological and operational sophistication. Skillful execution of attack and the methodology used to conceal any traces of attack complicates the task of advance intelligence information collection and/or attack detection.

Priorities for action

Assuring security of cyber space requires careful and due attention to creation of well defined systems and processes, use of appropriate technology and more importantly, engaging right kind of people with suitable awareness, ethics and behavior. Considering the transnational character of information technology & the cyber space, the technical & legal challenges in ensuring security of information, information systems & networks as well as related impact on socio-economic life in the country, the priorities for action for creating a secure cyber eco-system include series of enabling processes, direct actions and cooperative & collaborative efforts within the country and beyond, covering:

- Creation of necessary situational awareness regarding threats to ICT infrastructure for determination and implementation of suitable response
- Creation of a conducive legal environment in support of safe and secure cyber space, adequate trust & confidence in electronic transactions, enhancement of law enforcement capabilities that can enable responsible action by stakeholders and effective prosecution
- Protection of IT networks & gateways and critical communication & information infrastructure
- Putting in place 24 x 7 mechanism for cyber security emergency response & resolution and crisis management through effective predictive, preventive, protective, response and recovery actions
- Policy, promotion and enabling actions for compliance

to international security best practices and conformity assessment (product, process, technology & people) and incentives for compliance.

- Indigenous development of suitable security techniques & technology through frontier technology research, solution oriented research, proof of concept, pilot development etc. and deployment of secure IT products/processes
- Creation of a culture of cyber security for responsible user behavior & actions
- Effective cyber crime prevention & prosecution actions
- Proactive preventive & reactive mitigation actions to reach out & neutralize the sources of trouble and support for creation of global security eco system, including public-private partnership arrangements, information sharing, bilateral & multi-lateral agreements with overseas CERTs, security agencies and security vendors etc.
- Protection of data while in process, handling, storage & transit and protection of sensitive personal information to create a necessary environment of trust.

Partnership and collaborative efforts

Government leadership catalyzes activities of strategic importance to the Nation. In cyber security, such leadership can energize a broad collaboration with private-sector partners and stakeholders to generate fundamental technological advances in the security of the Nation's IT infrastructure. First, in support of national and economic security, the Government should identify the most dangerous classes of cyber security threats to the Nation, the most critical IT infrastructure vulnerabilities, and the most difficult cyber security problems. Second, the Government can use these findings to develop and implement a coordinated R&D effort focused on the key research needs that can only be addressed with such leadership. While these needs will evolve over time, this cyber security policy provides a starting point for such an effort. Public- private partnership is a key component of this cyber security policy. These partnerships can usefully confront coordination problems. They can significantly enhance information exchange and cooperation. Public-private engagement will take a variety of forms and will address awareness, training, technological improvements, vulnerability remediation, and recovery operations. These actions will help in leveraging rapid technological developments and capabilities of private sector.

Security threat and vulnerability management

All infrastructure facilities face a certain level of risk associated with various threats. These threats may be result of natural events, accidents or intentional acts to cause harm. Regardless of the nature of the threat, facility owners have a responsibility to limit or manage risks from these threats to the extent possible. This is more so, if the facility is a part of nation's critical information infrastructure. As such focus of these efforts would be:

1) To prevent cyber attacks on critical ICT infrastructure
2) Reduce vulnerability of critical ICT infrastructure to cyber attacks.
3) Enhancing the capability of critical ICT infrastructure to resist cyber attacks

4) Minimize damage and recovery in a reasonable time frame time

The key actions to reduce security threats and related vulnerabilities are:

1) Identification and classification of critical information infrastructure facilities and assets.
2) Roadmaps for organization-wise security policy implementation in line with international security best practices standards and other related guidelines.
3) Process for national level security threat & vulnerability assessments to understand the potential consequences.
4) Use of secure products/services, protocols & communications, trusted networks and digital control systems. Internet Service Providers (ISPs) would be closely associated in providing for secure information flow through their networks and gateways. Appropriate legally binding agreements need to be in place to support law enforcement, information security incident handling and crisis management processes on a 24x7 basis.
5) Identification of national level security organization (CERT-In, DIT) to act as a nodal agency and co-ordinate all matters related to information security in the country, with clearly defined roles & responsibilities.
6) Emergency preparedness and crisis management (Mirror Centers, Hot/warm/cold sites, communication, redundancy, and disaster recovery plans, test & evaluation of plans etc.

7) Periodic as well as random verification of the level of emergency preparedness of critical information infrastructure facilities in resisting cyber attacks and minimize damage & recovery time in case cyber attacks do occur.
8) Development of comprehensive repair and maintenance policy so as to minimize false alarms and increase cyber resource availability to all users efficiently.

Security threat early warning and response a) National cyber alert system:

(i) Rapid identification, information exchange, and remediation can often mitigate the damage caused by malicious cyberspace activity. For these activities to take place effectively at a national level, it requires a central nodal agency (CERT-In, DIT) to perform analysis, issue warnings, and coordinate response efforts. Because no information security plan can be impervious to concerted and intelligent attacks, information systems must be able to operate while under attack and also have the resilience to restore full operations in reasonable time frame. The National Cyber Alert System will involve critical infrastructure organizations, public and private institutions to perform analysis, conduct watch and warning activities, enable information exchange, and facilitate restoration efforts.

(ii) The essential actions under National Cyber Alert System include:

- Identification of focal points in the critical infrastructure

- Establishment of a public-private architecture for responding to national-level cyber incidents
- Tactical and strategic analysis of cyber attacks and vulnerability assessments
- Expanding the Cyber Warning and Information Network to support the role of Government in coordinating crisis management for cyberspace security;
- Cyber security drills and exercises in IT dependent business continuity plans of critical sectors to assess the level of emergency preparedness of critical information infrastructure facilities in resisting cyber attacks and minimize damage & recovery time in case cyber attacks do occur.

Security Risks

As a result of the Internet and e-mail, there has been a sharp increase in security incidents involving the accidental disclosure of classified and other sensitive information. One common problem occurs when individuals download a seemingly unclassified file from a classified system, and then fail to carefully review this file before sending it as an attachment to an e-mail message.

Too often, the seemingly unclassified file actually has some classified material or classification markings that are not readily apparent when the file is viewed on line.

Sending such material by e-mail is a security violation even if the recipient has an appropriate security clearance, as e-mail can easily be monitored by unauthorized persons.

More important, even if the downloaded file really is unclassified, the electronic version of that file may have recoverable traces of classified information. This happens because data is stored in “blocks.” If a file does not take up an entire block, the remainder of that block may have recoverable traces of data from other files. Your system administrator must follow an approved technical procedure for removing these traces before the file is treated as unclassified.

Some organizations have found it necessary to lock their computer drives to prevent any downloading of files from the classified system. If an individual wishes to download and retransmit an unclassified file from a classified system, the file must be downloaded and processed by the system administrator to remove electronic traces of other files before it is retransmitted.

Inappropriate Materials

Sending e-mail is like sending a postcard through the mail. Just as the mailman and others have an opportunity to read a postcard, network eavesdroppers can read your e-mail as it passes through the Internet from computer to computer. E-mail is not like a telephone call, where your privacy rights are protected by law.

The courts have repeatedly sided with employers who monitor their employees’ e-mail or Internet use. In an American Management Association poll, 47% of major companies reported that they store and review their employees’ e-mail. Organizations do this to protect themselves against lawsuits, because the organization can be held liable for abusive, harassing, or otherwise inappropriate messages sent over its computer network. In the same poll, 25% of companies reported that they have fired employees for misuse of the Internet or office e-mail.

In the past couple years, *The New York Times* fired 23 employees for exchanging off-colour e-mail. Xerox fired 40 people for inappropriate Internet use. Dow Chemical fired 24 employees and disciplined another 230 for sending or storing pornographic or violent material by e-mail. Several years ago, Chevron Corp. had to pay $2.2 million to plaintiffs who successfully brought a suit of sexual harassment, in part because an employee sent an e-mail to coworkers listing the reasons why beer is better than women.

Security of Tools

Secrets in the computer require the same protection as secrets on paper. This is because information can be recovered from a computer hard drive even after the file has been deleted or erased by the computer user. It is estimated that about a third of the average hard drive contains information that has been "deleted" but is still recoverable. Computers on which classified information is prepared must be kept in facilities that meet specified physical security requirements for processing classified information. If necessary to prepare classified information on a computer in a non-secure environment, use a removable hard drive or laptop that is secured in an approved safe when not in use. Alternatively, use a typewriter. Check with your security office concerning rules for traveling with a laptop on which classified or other sensitive information has been prepared. Laptop computers are a particular concern owing to their vulnerability to theft.

Computer Passwords

Passwords are used to authenticate an individual's right to have access to certain information. Your password is for your use only. Lending it to someone else is a security violation and may result in disciplinary action against both parties. Never disclose your password to anyone. Memorize it – do not put it in writing. If you leave your terminal unattended for any reason, log off or use a screen lock. Otherwise, someone else could use your computer to access information they are not authorized to have. You will be held responsible if someone else uses your password in connection with a system transaction. Do change your password regularly. Use a password with at least six and preferably eight characters and consisting of a mix of upper and lower case letters, numbers, and special characters such as punctuation marks This mix of various types of characters makes it more difficult for a hacker to use an automated tool called a "password cracker" to discover your password. Cracking passwords is a common means by which hackers gain unauthorized access to protected systems.

Social Engineering

"Social engineering" is hacker-speak for conning legitimate computer users into providing useful information that helps the hacker gain unauthorized access to their computer system. The hacker using social engineering usually poses as a legitimate person in the organization (maintenance technician, security officer, inexperienced computer user, VIP, etc.) and employs a plausible cover story to trick computer users into giving useful information. This is usually done by telephone, but it may also be done by forged e-mail messages or even in-person visits.

Most people have an incorrect impression of computer break-ins. They think they are purely technical, the result of technical flaws in computer systems which the intruders are able to exploit. The truth is, however, that social engineering often plays a big part in helping an attacker slip through security barriers. Lack of security awareness or gullibility of computer users often provides an easy stepping stone into the protected system if the attacker has no authorized access to the system at all.

Computer Applications in Business

Computer Applications in Business provides an overview of the integrated software packages most often used in the workplace. By the end of this course, you will have a sound understanding of the basic features and business applications for the word processor, spreadsheet, database, and presentation software in your choice of either Microsoft Works Suite or Microsoft Office Professional packages.

This process of completing this course, you will also learn how to problem solve and use the Help function and online tutorial assistance for your software. Finally, as this is an online course, you will learn about using the Internet and e-mail.

Delivery Method

There is continuous enrolment for this course. Delivery is self-paced, allowing you the flexibility to proceed through the course according to your own schedule.

Prerequisites

None. Students will need access to a PC with full internet access and MS Office Professional (XP preferred) including Access database software or MS Works (the 2002 or newer Works 'Suite' with Word included is preferred). This course is not ideal for those using the MS Office 2007 version.

Exclusions

Students with credit for CMPT 109, 150 or a similar course may not take CMPT 119 for further credit.

Objectives

- Answer questions regarding your computer's hardware, software, and basic operations.
- Set up your computer for World Wide Web connection.
- Use e-mail to send messages and file attachments.
- Participate in on-line discussion groups.
- Describe the types of documents created with a word processing programme.
- List the principal features of a word processing programme.
- Create and format a business letter.
- Create and format a schedule containing a table.
- Design either a textual or a visual message for a public audience.
- Select and use style features to create new documents.
- Use the Help system to answer questions and troubleshoot problems.
- Describe the purposes of a spreadsheet and define its vocabulary.

- Set up and analyse itemized lists of numbers, such as the various types of budgets or financial statements.
- Perform and manipulate the calculations to achieve meaningful information.
- Present the numerical data in the spreadsheet in a graphical format.
- Conduct "what if" simulations of the numerical statements.
- Import spreadsheet reports and charts into word processing and/or database documents.
- Define the purpose of a database programme.
- Describe the components of a database.
- Plan a simple two-table database.
- Use wizards to enter and to search data, and to create a report.
- Enter data in a form.
- Merge data with a document.
- Create mailing labels.
- Analyse data in a database.
- Privacy issues related to databases.
- Plan a presentation.
- Apply good design principles to a presentation.
- Examine examples of a presentation.
- Describe the purpose of presentation software.
- Describe the components of a presentation.
- Create a presentation outline.
- Apply and modify a design template.
- Add clip art and charts to a presentation.
- Run a slide show.

Small, rural high schools are constantly trying to determine what type of computer training should be provided to students to meet the needs of business in the surrounding area. Many students in high schools today are not college bound and attempt to find local employment after graduation. Leaders in the community are also interested in retaining as many young people as possible in the area by helping them find local jobs through adequate high school training.

Changing Face of Business

Reports of shipments of personal computers to small businesses and home offices are growing at a 16% annual rate. The power of the computer, the fax machine and voice mail allow a small company to do almost anything a larger corporation does. New technology has streamlined every part of our business lives.

The challenge for small firms is to apply these technologies appropriately. After investing in a computer, for example, most discover other peripherals they want to incorporate into their office systems. The bottom line is that even small businesses can, and do, utilize computers and related technologies in their day-to-day operations. This means that even a high school graduate who does not plan to further his or her formal education should have some knowledge of computers.

In addition, it is important to bridge the gap between basic theory and computer applications. There is a strong correlation between high anxiety and reduced computer competence. Experience with computers in school tends to reduce anxiety on the job and leads to more productive workers. A good computer course also shows students how the computer can be utilized in many diverse fields.

Identifying Skills

Businesses must be periodically surveyed for information on the type of skills needed by their workers. In today's evolving world of work, required skills change as fast as the available technologies.

In Nebraska, for example, the Manpower company surveyed offices from Lincoln west to the Colorado border by sending a questionnaire on office automation topics to over 2,500 businesses.

The results indicated that word processing was the number one activity, using a spreadsheet was number two, and manipulating a database was number three. Lotus 1-23 was the most widely installed software. WordPerfect was the most popular word processing package, capturing 40% of those responding to their survey. Service companies were the largest number of respondents, with government second and retail/wholesale businesses third.

Previous to its decisions on what type of computers to purchase and which software packages to teach, Auburn High School needed to know similar information. They wanted to provide their students specific experience with the computers and applications being utilized by business and industry in the local geographic area. This would reassure their students that they would be employable after graduation. It would also assist the local communities by keeping young people in the area and not have them travel to find jobs elsewhere. Upon the suggestion of Auburn's computer programming teacher, Claudette Stevens, a comprehensive survey of local area businesses was conducted in southeast Nebraska in two rural counties, Richardson and Nemaha. All of both counties' businesses were identified from the telephone book and local Chamber of Commerces, totalling 627. A random sample of 150 (approximately 25%) of these firms were contacted by telephone. All companies that were contacted agreed to answer the questions on the survey.

Examining the Survey Results

Almost half of the small, rural businesses contacted (46%) are still not using computers. Of those using computers, over 68% said they purchased them mainly for accounting. However, most companies indicated they use computers for a variety of functions. Surveyed companies reported using a total of 38 different software packages. The most common type of programme used was for accounting, the second most common was word processing, and the third most common software produced customer receipts.

The questionnaire also dealt with the amount of knowledge new employees were expected to possess. Only one employer expected to hire a person with a bachelor's degree in computer science, and that job also required a four month period of intense training. A majority of companies expected to hire employees with basic knowledge on how to use the type of computer the firm owned. Some companies wanted potential employees to have an amount of keyboarding skills; other firms wanted general computer ability.

The Future of Cyber Security

The product of human ingenuity and innovation, cyberspace now delivers a range of critical services to more citizens around the world than ever before. Yet, the online world as we know it stands at the threshold of unprecedented change.

Being invited to speak at the EastWest Institute's Worldwide Security Conference in Brussels this week provided an opportunity to examine the needs faced by the global security community as we prepare to meet the needs of the Internet's next billion users. The International Telecommunication Union (ITU) reported that the number of Internet users reached the two billion threshold in March of this year and according to a Boston Consulting Group report, another billion are expected to come online in the next four years, bringing the total number of Internet users worldwide to about three billion by 2015.

Planning to ensure that our online world—cyberspace—is trustworthy, resilient and secure as we move into this uncertain future, policy leaders need to consider the fundamental changes that are occurring in cyberspace, and the policy issues that these changes will likely present and that will need to be addressed. Looking towards the future of three billion users, four factors will fundamentally change the future of cyberspace security: people, devices, data, and cloud services.

The Global Online Population Expands

The emergence of the next billion Internet users will impact security in two ways. Most important will be the impact of the demographic characteristics of these users. Consider that the next billion users will (1) be younger, (2) spend more time online, (3) be more mobile, (4) see the world through social media and apps, and (5) make greater use of natural interfaces. These five factors could hasten the onset of totally digital lifestyles making connectivity seemingly as essential as oxygen. The next billion could also help foster new innovation in the development and application of technology.

Separately, however, this emerging user population also represents a greatly expanded “target rich” environment for cybercriminals that want to exploit their data, social networks, and devices via botnets or other means.

Internet of Things to Immersive Computing

These new users will require new devices. According to The Boston Consulting Group, the number of Internet-connected devices is predicted to exceed 15 billion—twice the world’s population–by 2015, and to soar to 50 billion devices by 2020. “Devices” of course refers to more than smart phones, netbooks and tablets. It also systems such as smart grids, intelligent transportation, healthcare monitoring, smart manufacturing, and environmental sensors.

The advent of powerful wireless devices that both run infrastructure and deliver infrastructure services, including providing access to cloud services, means that cybercriminals and other threat actors need not merely target traditional, and increasingly protected, commercial software and consumer applications to execute attacks with significant consequences. Attackers may well target the embedded software, firmware and hardware in these devices to attack the infrastructure or seize control of the devices and turn them into sensors that can report status, collect personally identifiable information, or conduct other espionage.

Data: Rapid increases in Understanding

The striking growth in the number of users and devices will also produce an exponential growth in the amount of data that is being generated, stored, analysed and transformed into innovation and knowledge. Analysing large data sets—so-called big data—will become a key basis of competition, underpinning new waves of productivity growth, innovation, and consumer surplus, according to research by MGI and McKinsey's Business Technology Office. However, such data sets also represent attractive targets for organized cyber criminals and other threat actors. From a security standpoint, safeguarding these huge data sets, protecting privacy and integrity, will require concerted global effort requiring collaboration among governments, the private sector, and users.

Cloud Computing: The Information Society Enabler

With an exponentially growing community of increasingly mobile users, cloud computing will commensurately grow in importance. It will fundamentally change how businesses operate, how every manner of services are delivered, and even how lives are lived. On the positive side, the security best practices implemented by an effective cloud provider may rival or surpass the measures that cloud customers might themselves be able to provide, resulting in enhanced security. Yet there are global issues that will need to be addressed in terms of transparency and jurisdiction to enable cloud services that are both secure and scalable to service the needs of this expanded user community across multiple countries.

Reducing the Cyber-attack Surface

Reducing the cyber-attack surface can be achieved by industry and government working in partnership to make the ICT infrastructure less susceptible to attack and compromise. One important way to achieve this is through concerted action to address risks in the supply chain for information and communications technology products and services.

Vendors and service providers need to build and maintain world-class approaches to secure software and hardware development methodologies. Microsoft began this journey over 10 years ago and has openly shared its Security Development Lifecycle. The nonprofit alliance SAFECode provides a platform for companies to share, both within the software development community and more broadly, information on secure software development techniques that have proven to be effective as well as those that have not. Industry needs to do more.

For their part, governments need to understand the nature of ICT supply chain risk more clearly and work collaboratively with one another and with vendors to develop a common risk management framework rooted in core principles that both address supply chain integrity concerns and preserve the fruits of global free trade. Such a system should be risk-based, transparent, flexible, and should recognize the realities of reciprocal treatment in the global economic environment.

Improving Internet Health

Improving Internet health requires a global, collaborative approach to protecting people from the potential dangers of the Internet.

Despite the best efforts at education and protection, many consumer computers host malware and may be part of a "botnet," unbeknownst to their legitimate owners.

There is currently no concerted mechanism to shield users from or help them mitigate these risks. Such infected computers do not simply expose their owners' valuable information and data; they place others at risk too. This threat to greater society makes it is essential that the technology ecosystem take collective action to combat it.

Work has been underway in industry circles to build cooperation among various stakeholder groups including ISPs, software vendors, and others; to leverage investments made in key regions of the world; and to create a future roadmap for an Internet health system.

The active discussions of cyber security policy and legislation now underway in many nations afford a ripe opportunity to promote this Internet health model. As part of this discussion, it is important to focus on building a socially acceptable model. While the security benefits may be clear, it is important to achieve those benefits in a way that does not erode privacy or otherwise raise concern.

4

Security and Data Integrity Threats

The range of means by which the security and integrity of computing resources can be threatened is very broad, and encompasses:

- Operator error (for example a user inadvertently deleting the wrong file).
- Hardware or media failure (either as a result of wear-and-tear, old age or accidental damage).
- Theft or sabotage (of hardware and/or data or its media).
- Hackers (who obtain unauthorised online access via the Internet).
- Malware (any form of virus, and including "Trojan" e-mail attachments that users are encouraged to open).
- Power surges and/or outages (which are one of the most common means of hard disk corruption and hardware damage).

- Flood, fire, storm or other natural disasters.
- Fraud or embezzlement.
- Industrial espionage.
- Terrorism.

Physical Security Measures

Given the breadth of the human reliance on computer technology, physical security arrangements to try and ensure that hardware and storage media are not compromised by theft or unauthorised access are more important today than ever before. And yet surprisingly they still often not taken seriously enough. Indeed, the number of high-profile instances of CDs, DVDs, hard disks and laptops going missing from government offices in the United Kingdom over the past year is quite staggering. Not least due to advances in mobile and cloud computing, computing resources are more vulnerable to theft than ever before. Twenty or more years ago, most computer equipment and data lived in a secure IT "glass house" well out of the reach of the casual thief, and with the hardware involved of little or no street value anyway. However, this is obviously no longer the case.

Personal and business data is now stored across a wide range of organisational, cloud vendor and personal locations, more work is conducted at home than since the rise of the modern city, and IT departments therefore have a right to be nervous. At the very least, physical computing security measures—such as external building safeguards and the control of access to areas of a building where computers are located—should be subject to regular formal updating and review. Most large organizations—particularly in the public sector—have a horror story or several to tell of computer equipment that has “walked”. Many such stories suggest that people who walk out of buildings with computer equipment under their arm are rarely challenged (and sometimes even assisted!). Locking-down computer equipment and/or ensuring adequate door and window security at all computer locations should today just be pure common sense.

Physical security also needs to be particularly carefully considered in semi-public locations (such as many open plan offices). For example, it needs to be considered how easy it would be for somebody to gain access to a PC, insert a USB memory stick, and walk away with valuable or sensitive data. Large corporate data centres in which the computer equipment is located in an air conditioned room typically have fire control systems that will hermetically seal the location and put out a fire using an inert gas. In smaller companies and domestically this clearly is not an option. However, whilst computers themselves may be at risk from fire (and indeed the cause of a fire!), back-up media can be protected in a fire safe, and/or via off-site storage. The physical security ofstorage media against the threats of fire, flood and other forms of damage.

Alongside theft, fire and flood, the other most significant threat that can damage computer equipment and/or the data held on it comes from power surges (voltage spikes) or power outages (brown-outs or black-outs). Many hard disk failures in particular are thought to be linked to power surge or outage issues of which users are often unaware. To protect against this very real but often ignored threat to computer equipment and data, a power surge protector and/or uninteruptable power supply (UPS) unit can be employed. Surge protectors are relatively cheap and protect against voltage spikes. They are today often built into multi-socket outlets with an insurance guarantee included for the connected equipment.

For even greater protection, a UPS unit includes a rechargeable battery that will continue to power a computer and key peripherals during a mains power brown-out or black-out. Software is usually also used to permit a controlled shut-down of equipment when a power black-out occurs. UPS units are more expensive than surge protectors, somewhat bulky, and often very heavy. However, for a server or key personal computer (such as one used to run a business or key part thereof) they are also a very good investment.

Minimising the Impact of Error, Failure or Loss

Whilst physical threats need to be protected against, most data is lost or corrupted following user error or hardware failure. The best defence against this is an appropriate back-up strategy, triggered on both a time and event basis and with appropriate physical resilience. In other words, users need to ensure that they take regular backs-ups at regular intervals and before and after making key data changes. They also need to store multiple back-ups on different media in different locations. There is no such thing as a permanent store of any form of computer data. Nor is any storage location entirely safe (although the cloud data centres run by Google, Amazon, IBM, Microsoft and other computing industry giants are pretty well protected these days!). Whilst any back-up strategy does require the selection of appropriate storage media, user education is often an equally key a consideration. Taking regular back-ups is at best only half of the story. Far too many individuals and businesses keep their back-up media—be they removable hard drives, optical disks and even USB memory sticks, in an entirely insecure manner in the same physical location as their computer. Even in corporate IT departments this has been known. Such practice has to significantly reduce the value of back-ups.

When making their disaster recovery plans and addressing the key computer security questions, the location of back-up media needs careful consideration. Even on a domestic level, most households could keep a few writable CD or DVD disks (or even SD cards) of key back-ups (including photographs and their music collection) in a secure location (in the roof or under a floorboard or with family and friends or wherever), and which would provide significantly increased data storage resilience. However, unfortunately most people still only ever think of this kind of simple strategy after it is too late.

Passwords and Appropriate User Authentication

Physically protecting computer equipment and data against damage or loss is a large element of computer security. However, another large element is limiting access to all or part of a system or data store to authorised users only.

In the broadest of terms, user authorisation within any security system can be verified via one three means:

- Something known by the individual (a piece of information such as a password)
- Something possessed by the individual (a physical token such a credit, security or ID card), or
- A biometric characteristic of the individual (for example their signature, finger print, retinal scan or DNA).

For good security, two of the above measures should be employed for what is known as "two-factor security". For example, to obtain money from a bank cash machine both a card and a PIN (personal identification number password) are required.

Where computer security is concerned, one measure of user verification will almost always be a password given the relative technical ease with which this can be implemented. Computer keyboards, mobile computers and dedicated input devices that include finger print readers are also becoming more common, and can be combined with passwording to achieve two-factor security. ID cards and even retinal scans are also used in conjunction with passwords on high-end security systems. However, any system that requires a token or biometric to be read has proved difficult to rollout en-mass. This said, recently some banks have started to provide each customer with a reader device into which their bank card is inserted. This allows for two-factor security, as the unit displays a number for each transaction that is uniquely in sequence with their bank.

Today at least, and probably in practice for many years to come, one-factor security based on passwords is all that is available for identifying authorised users in the majority of computing situations. This in turn means that users must be educated to use strong passwording—or in other words, to choose and use passwords in a manner that makes the password difficult to either fathom or otherwise obtain by an unauthorised party.

To be classed as "strong", passwords,

- Should be at least six and preferably eight or more characters in length.

- Should be mixed case alphanumeric (a mix of apparently random upper and lower case letters and numbers is best).
- Should be changed regularly (at least every three months is a common rule).
- Should be known only to the user.
- Should not be obviously related to the user.
- Should be different for each application used.
- Should not be based on data (such as a favourite place) listed publically on Facebook or another social networking site, and
- Should not be written down (let alone stuck on a post-it note on the side of a computer!)

Users should also try and ensure password security by following the measures as outlined below under "Internet Security".

Maintaining Confidentiality

In part the confidentiality of data is protected via physical security measures and appropriate user authentication precautions as already outlined above. However, effective security should plan for what happens if these measures fail, and how data confidentiality can be protected even if computer equipment or media fall into the wrong hands. This is particularly important when it comes to the protection of sensitive information such as financial data. The confidentiality of the data on stolen hardware or of data accessed by unauthorised users can be protected via encryption. For example, software such as the open-source TrueCrypt (available from www.truecrypt.org) can be used to encrypt the data on any storage device (for example a USB key carried in your pocket). Office documents can also or alternatively be protected by securing them with a password. This can be a particularly sensible thing to do when e-mailing sensitive documents, or posting them by snail mail on removable media. In an office package such as the freely downloadable OpenOffice, password protecting a file is as simple as ticking the "save with password" option when selecting "Save As".

Data confidentiality also needs to be protected on output and disposal. In the case of the former, in an open plan office environment precautions should be taken when sending documents containing confidential information to a communal network printer. In the case of the latter, printed output containing sensitive data needs to be disposed of securely (eg via shredding and/or incineration), as do waste media (such as discarded optical disks). At the end of a computer's life or when components are being upgraded, care also needs to be taken to ensure that discarded hard disk drives (including those located in external hard drive units) are appropriately erased before disposal.

Internet Security

The connection of most computers in the world to the Internet, coupled with the growth of cloud computing, has inevitably broadened significantly the scope of computer security and control vulnerabilities. Before the widespread adoption of personal computers, rogue programmers with malicious or criminal intent would try to "hack" into big computing facilities via the phone network. Then, once personal computing really took told, the focus for many such malicious programmers shifted to writing computer viruses that could be unknowingly distributed on floppy disks, and which could hence disrupt the operation of those millions of computers not connected to the telephone network.

Today, this situation has evolved again, with many personal computers having an “always on” broadband connection which makes them potentially prone to unauthorised access via a computer network. And on top of this, the virus writers are still at work, the fruits of their corruptive programming labours now distributed both online and via physical storage media.

Whilst there are very real security risks associated with both the consumer and business use of the Internet, it is also the case than many such security concerns are perceptual. To an extent, all that has really changed over the past few years has been the willingness of people and organizations to conduct their affairs over the world-wide web.

The sensible use of a credit card over the web is not that much more secure that it was five years ago. The fact that it has become the norm is therefore due to the fact that the risk/benefit ratio of doing e-business has shifted significantly in favour of the “benefit” side in the eyes of the value-seeking majority. Care, of course, does need to be taken. For a start these days it is foolish in the absolute extreme to run any computer with an Internet connection without antivirus software. Such software—such as the range of Norton security software available from www. symantec.com—is most usually commercially purchased with a yearly subscription for regular updates to its virus definition database. However, it is possible to obtain antivirus software for free. Indeed, my own current recommendation for PC owners is to install Microsoft Security Essentials. For most people this is a very good option, does not hog resources, comes from a reputable organization—and is free!

In addition (though often bundled with) antivirus software, all computers with a potentially always-on Internet connection should be protected via a firewall. Whilst antivirus software is intended to detect and prevent infestation with malicious software (including viruses and other "malware"), the job of a firewall is to regulate the network communications a computer receives, permitting or denying such communications based on how trusted the communications source is considered to be.

Firewalls can be implemented via either hardware or software. A personal computer firewall will almost certainly be software based, although increasingly some form of hardware firewall is being incorporated into wireless ADSL routers (wireless access points). Like antivirus software, a firewall needs to be regularly updated with the latest threat information to be most effective. Windows XP, Vista and Windows 7 all include a software firewall, although many people choose to adopt third party firewall software as an alternative to this.

In addition to antivirus software and a firewall, user vigilance and even plain common sense provide one of the most effective defences against potential Internet-related security vulnerabilities. For example, users should be educated never to open unsolicited (spam) emails, and doubly-so never to open any e-mail attachments included with such e-mails (and as may be automatically opened by some configurations of e-mail software). Viruses and other malware (such as “sniffer” software intended to record and communicate usernames and passwords) can be attached as “Trojan” (horses) to e-mails. However, it is only when the user opens such messages and executes their attachments that corruption or security risks can occur.

Users also need to ensure that they use strong passwording when setting up accounts for web transactions. They should also never permit their browser software to remember their login details for a website unless they are absolutely certain of who else may have access to the computer they are using. Indeed, it is still potentially unwise to let even a single-user PC remember passwords for activities such as online shopping or online banking. This is because the theft of the PC would permit direct access to the user’s bank and other online accounts.

Talking of online transactions, users should also be careful only to conduct business online with trusted websites and over secure (encrypted) connections. Trusted websites are those that are well known, have an established trading history, and which advertise contact points for both online and off-line customer support. Secure connections can be identified by looking for the letters “HTTPS” (a secure version of the hypertext transfer protocol that facilitates web communications) at the start of the web address seen at the top of a web browser window. HTTPS connections exchange digital certificates to encrypt communications via what is known as a “secure socket layer” (SSL). As a basic rule, never enter your credit card details into a web page without first checking that the address of the page starts “HTTPS”.

For users of cloud computing services such as SaaS applications, all of the above points relating to good Internet security clearly apply. Computing in the cloud is still deemed by many to be risky. However, it can also bring security advantages as user data is protected off-site in large vendor data centres. For example users of Google Docs are always safe in the knowledge that their files are always securely stored on two different servers in two different data centres. For private individauls and small companies, such a high level of off-site data protection and replication is hard to achieve by other means.

In addition to using antivirus software, a firewall, strong passwords, and uploading regular operating system and browser updates, it is doubly important for users of the cloud to ensure the security of the computer they use to access their chosen online services. In particular care needs to be taken to make certain that they never leave active accounts on a device that may be stolen or otherwise accessed by inappropriate users. For example, files held in Google Docs or indeed another other SaaS application are not at all secure if a user leaves their netbook or smartphone in a public place and all anybody has to do to gain access is to boot up the machine and visit the appropriate web address. SaaS users who share desktop PCs—or who for example use public desktop computers in cyber cafes—ought also to be very careful indeed to ensure that they log-out from cloud services whenever they finish using them.

Disaster Recovery Planning

Both individuals and in particular businesses should have plans in place to cover the eventuality of hardware failure or loss and/or data loss or corruption. Such disaster recovery or "business continuity" plans need to address how data would be recovered, what hardware would be used to run critical applications, and by whom. Such plans particularly need to take into account any current use of out-of-date software applications that may not be able to be replaced and/or run on replacement hardware and operating systems. To recover back-ups of data that cannot be run on any available hardware and software will not in any way ensure business continuity!

Depending on the types of threat they are intended to cover, disaster recover plans may rely on one of a mix of strategies (and a mix is arguably often best). One option is on-site standby, where duplicate systems exist that can be used to run critical operations (provided that data is still available or can be recovered). Such duplicate systems need not necessarily be standing idle waiting for disaster (as they would be in a nuclear power station), but may be everyday systems used in one part of the business that are prepared to run key applications from other parts of a business if the need arises. As an alternative to on-site standby, some sort of off-site standby is very common. If a company has multiple buildings or premises, then it makes sense both to hold off-site back-ups across these locations, and to ensure that key system functionality can be duplicated across sites.

Some businesses also have "reciprocal agreements" with other companies to make use of their computers to run key operations in the event of a disaster (such as a fire that destroys their premises). Often small and medium-sized companies make such reciprocal agreements with nearby schools who have suitable computer suites which they are prepared to offer as an off-site standby provision for a reasonable cost. For larger organizations, or those highly dependent on computing continuity, "hot-site agreements" can be made with firms that offer commercial disaster recovery as a service, and who can deliver (for a price) portable working computer rooms at very short notice.

As a final element of disaster recovery planning, replacement purchase plans should be in place. In the event of fire or theft, the last thing most individual users or companies would want to be thinking about is where to purchase new computer equipment from, and what specification to choose. Not least this is an issue because direct-specification let alone exact-model replacements for any items of computer hardware or software more than a year old are incredibly unlikely to be available.

Data Protection Legislation

We live in a world where data is held on everybody and used and inter-linked for a very wide range of purposes. In an attempt to provide some redress against inappropriate data use, in the United Kingdom the Data Protection Act (DPA) 1998 protects data held on living individuals. Any individual can submit a subject action request to any party that holds data on them. This allows them to obtain a copy of all data held on them within 40 days of the subject action request being received. Following a subject action request, individuals can challenge the validity of the data held on them, and if appropriate can claim compensation relating to any inaccuracy or misuse.

The Data Protection Commissioner is charged with ensuring that all data in the UK “shall be obtained and subsequently processed in a fair and lawful manner”. All organizations have to have a “data controller” who, with a few limited exceptions, must register all data stored with the Data Protection Commissioner.

They must also be open about the data’s purpose, and ensure its accuracy and security. Whilst the Data Protection Act protects individuals on whom data it held, it does not protect data itself or computer systems. Such protection is provided in the United Kingdom by the Computer Misuse Act (CMA) 1990.

This created three levels of offence, and which make it illegal to gain unauthorised access to computer material; to gain unauthorised access with intent to commit or facilitate further offences; and to make an authorised modification of computer material. The last of these offences in theory at least makes it illegal to write and distribute computer viruses.

How to Secure a Computer

The confidentiality, availability and the integrity of the data is the most important aspect of the computer security. Computer security refers to securing your computer from the unauthorized access and from internal and external threats like virus, spyware, Trojan horses, phishing attacks, hackers and intruders. There are a large number of techniques that can be used to protect your computer from all these threats. In this chapter you will learn that how to secure your computer from the most common security threats. Security can be implemented from the operating system to computer hardware level. Following is an overview of some of the common PC threats and the solutions from preventing them.

Computer Viruses

Computer viruses are the one of the most common threats to a computer. Any online computer can be attacked by the viruses and other online threats in less than 20 minutes if it has not been using a proper security mechanism. A virus infected computer can transmitted the viruses to the other connected computers in a network. Viruses can harm your computer in a variety of ways such as they can corrupt data, corrupt the hard disk, delete the operating system files and can crash the system. Install an up-to-dated antivirus software and regularly scan your computer to get rid of the potentially dangerous computer viruses.

Spyware

Spyware is another big threat for the online computers. Spyware enter in your computer through the numbers of ways such as when you visit a spyware infected website, install spyware infected software and access online spyware infected online application. To get rid of the spyware, install an up-to-date anti spyware software and regularly scan your computer with it.

Phishing

Phishing attack is another growing threat for the online computers. Phishing is a type of online deception techniques that is designed to steal your confidential information, passwords, credit card information and important login and password through the fraudulent emails. The best solution to avoid this treat is to not open the E-mail attachments from the unknown and unreliable sources. Secondly, never give your personal information to anyone even the emails claim to be delivered from big sources. Companies like LifeLock.com offer protection for your identity and personal information if your computer is attacked.

Firewall and System Probing

If you haven't implemented a firewall system on your computer then chances are that your computer can be accessed by the unauthorized users and hackers. The best solution to avoid this problem and keep your privacy intact is to install and configure a software or hardware firewall into your system.

Physical Threats

The physical threats to a computer involves the physically damage to the computer components with the fire, water and destructions. The best solution to avoid the physical threats to your important computer system and data is to set an off-site replication. Replicate your data regularly at some remote location.

Employee's Sabotage

An organization's employees are most familiar with the computers inside an organization. There are a lot of examples where the annoyed employees of a company are involved in sabotaging the computer system. Employee's sabotage include entering data incorrectly, destroying system hardware, deleting data, changing data, changing the passwords and entering the data incorrectly. The best way to avoid the situations like these is to delete the employees' account after they leaves the company so that they can't no more access company's systems. Secondly, regularly monitor the activities of the employees and restrict their access to the sensitive resources in the overall IT infrastructure.

Vendor's Default Password Attack

Vendors of the computer systems have the default passwords at many different hardware and software components like the router, system BIOS and others. It is very important to change the default password of the computer devices and applications.

Human Error

Errors and the omissions are the great threats to the integrity of the data and the computer system. Data entry operators, programmers, system administrators often make errors that can compromise the system's security. The effect of the various security threats caused by the human errors varies. Employee's training and awareness training should be given to the employees to avoid such kinds of errors that can lead to the financial losses for a company.

Options for Securing Confidential Electronic Data

Confidential data, including personal information, must be secured against theft, loss, and inadvertent sharing. This page is designed to provide you with information about how to secure confidential electronic data.

The options are especially important if you are using:

- A computer to access confidential data, including personal information.

- Mobile devices such as laptops, USB keys, smartphones, tablet devices, portable hard drives, flash drives, etc.
- Any computing device that is used by other people.

Currently Available Options

Consider the sensitivity of the information you are using, where you are accessing, using or sending it, and choose the appropriate option. Portable devices are a great convenience but also increase the risk that confidential information will be lost, stolen, or inadvertently shared.

- One way to limit security risks for confidential electronic data is not to store it on your own devices. Computing and Communications Services (CCS) and some departments provide servers that are designed to provide secure locations to save confidential data. This has security advantages over saving confidential data directly on your computer, particularly in the event your computer is lost or stolen. CCS provides personal and shared-access folders on file servers free of charge for faculty and staff. Click here to request access to the Central File and Print Services (CFAPS). Some other academic and administrative depart-ments offer similar services.
- If you need to access data stored on the server from a remote location, you can do so securely using RU-VPN- a virtual private network system that encrypts data in transit between Ryerson's servers and your computer. Clickhere to request access to RU-VPN
- For very sensitive data, you can set up encrypted folders containing private or confidential data on devices like laptops or shared workstations. The

folders can be stored on the server (recommended) or on your hard-drive. Current operating systems such as the most recent releases of Windows and Mac OS support folder-level encryption.

- If you must use portable devices like USB keys and Flash drives, purchase devices that support password protection and encryption. For example Ryerson's bookstore sells the Kingston Data Traveler Vault - Privacy.

Password Protection of Workstations, Laptops, Phones, and Tablets

All computers, including mobile devices, should be password protected. Information on choosing a strong password is available here. Whenever screen savers are used, they should be configured so that a password is required to exit screen saver mode.

Permission to Take Data Off Campus

In some cases Ryerson departments may have policies in place that restrict the transport of data off campus. If you are unsure, check with your Chair, Director or Manager first.

New Security Tools

CCS has purchased the Sophos Endpoint Security and Data Protection system. The system provides malware and virus protection. It also includes the ability to encrypt data and recover lost encryption keys. The new system with encryption enabled will be available at the end of October 2011.

Computer Security Basics

Making a computer secure requires a list of different actions for different reasons. There is a secondary rule that says security is an on going process. No matter how well a system is designed, if it is never changed that gives any potential infiltrator all the time in the world to examine the security for flaws. The information described here is neither detailed nor comprehensive. This should, however, serve as a good overview of the types of security measures sometimes taken. What measures are appropriate are best determined on a case by case basis.

Physical Security

Theft is the physical threat of most concern and rightfully so. Keeping rooms locked is a good idea, but not always feasible. Keeping computers locked to a wall or table is a good deterrent against a casual, shoplifting style, theft but it will not deter a professional with a shopping list. We have seen a thief use a crow bar to remove a computer along with a portion of the formica table top (they were then foolish enough to take it to a repair shop with the table top still attached). There are very loud alarms which sound when the power cable is unplugged. A combination of locks and alarms is an excellent theft prevention system for computer labs which must be publicly accessible, particularly at late hours.

Computer hardware is protected from fire damage by smoke detectors and sprinkler systems just like any other equipment. Computers are unique in that the most costly damage is the loss of data which can be prevented by storing back up tapes in remote locations.

Surge protectors and uninterruptable power supplies are a low cost investment that can save very costly equipment damage. These are particularly important if the computer must be used continuously or if your region is prone to severe thunder storms or frequent power outages. Some surge protectors have the ability to protect the phone line going to a modem also. The modem and mother board can be more readily damaged by lightning hitting a phone line than by lightning hitting the power lines because the computer power supply provides a minimal amount of protection.

Data Integrity

Backing up data is the single most important step in preventing data loss. Entire companies have gone out of business due to losing valuable information. An enormous amount of man hours are spent every year reproducing information which was lost in some manner. Back ups can be on removable disks, tapes, paper printouts or other computer systems. It is important to periodically put copies of these back ups in remote physical locations to prevent loosing the original and back up data through fire, etc. In today's world, virus protection is a necessity for any PC or Macintosh and viruses are starting to appear on UNIX systems also. No system is completely safe from viruses since manufacturers have inadvertently shipped new computers with viruses on the hard drive and minted CDs with viruses.

For very important data, RAID systems are used. RAID stands for "Redundant Array of Inexpensive Disks". A RAID system is a computer with eight or more hard drives and software for storing data on those drives. Every byte of data is spread across all of these drives along with a parity bit that tells if it was an odd or even byte. In the event that a disk fails, it's contents can be completely reconstructed from the data on the other seven disks. This is a good way to store critical data which could not be reproduced, but the expense may not be justified otherwise.

Data Security

The primary threat to data security is illegal computer hackers. Studies show that the largest percentage of hackers are young men motivated by status with other hackers, malicious intent or the excitement of a challenging game. There have also been even more harmful cases of corporate spying and embezzlement of funds. Accounts on both multiuser machines and micro computers can be protected by passwords. Passwords can be very effective or not effective at all. Insecure password include ones that are easily guessed, never changed, shared or written down somewhere. Some systems, particularly UNIX, have password files which are encrypted but readable by all users. Hackers have developed automated programmes, such as "crack", to break the passwords in these files by raw brute force, trial & error techniques. Since it could take months to crack well chosen passwords, some systems use a password aging system that requires all users to set new passwords periodically. There are also programmes to prevent users from setting easily guessed passwords such as words in the dictionary, common names or permutations on the account name.

Systems holding data belonging to multiple users, such as UNIX or Windows NT, set an owner for each file and permissions defining who is allowed to read or write to it. Many hacker attacks are centered around finding flaws in the file permission system. There are ways to set default permissions and ways to control how much individual users can control their own file permissions.

Since most security attacks are now initiated from a remote location via the network, many organizations now separate their internal networks from the Internet with a firewall. A firewall is a piece of software running on a dedicated machine with two network boards. The software can filter which network traffic is allowed to pass between the internal and external networks. This is a very effective security measure, but there is an unfortunate tendency for organizations to make the firewall their only security measure making any breach of security across the firewall a breach for every machine in the whole organization. An even higher level of security can be achieved by not having any connection between the internal network and the internet or not even having an internal network.

Data encryption provides a second layer of security. Once someone gains access to data, that data is useless if it has been scrambled by an encryption programme which requires a second password to unscramble it. Passwords themselves should always be stored in an encrypted form.

Today's encryption systems are similar to military code systems but not as sophisticated as the systems used by the armed forces. Almost all encrypted data can be unencrypted without the password by the use of a very large amount of time on very powerful computers. Security is provided by making the encryption complex enough that no one would be likely to have enough computer power to break say a message about the merger next month in less than six months, at which time the message is no longer valuable.

There must always be someone able to fix a computer system by using a second password protected account called "system", "administrator", "root" or "superuser" which bypasses the file permission system.

One of the most serious security attacks is one which gains the password to this account. As well as particularily stringent security for this account, the encryption systems, ensure that there is a second layer of protection against this type of attack. This also provides for a segmented internal security system, if such is necessary.

E-mail is particularly insecure. Mail messages are simple ascii files that travel across the network where no password is necessary to get to them. E-mail is easily forged and can be altered.

Of course, no one would have any particular reason for tampering with many personal messages, but people conducting sensitive business transactions over E-mail would be wise to use some sort of E-mail encryption system, such as PGP. These systems have several functions including encrypting the message itself, verifying who sent the message and verifying that it was not tampered with.

Audit trails are a means for the system administrators to find out if security has been breached and how much damage was done. Audit trails are records made by various pieces of software to log who logged into a system, from where and what files were accessed.

How Hackers Get In

Here is the typical sequence of steps used to gain illegal entry into a computer system.

- *Learn about the system.* Trying to connect to a system using networking utilities like telnet and ftp will be unsuccessful without a password, but even unsuccessful logins will often still display the machine manufacturer, and version of the operating system.

- *Look for openings.* Try known security flaws on that particular machine and operating system. Unless the system administrator is very diligent about installing security patches, many machines have openings in the security just waiting to be found.
- *Try sniffing to get a password.* Sniffing is when a machine has software to watch all of the network traffic and saves the messages corresponding to a valid user entering their password from a remote location.
- *Try spoofing.* Many machines share disks with other machines that are classified as "trusted hosts". In order to share the data on these disks the two machines must communicate without a password. Spoofing is when someone configures a third machine to use the network address of one of the trusted hosts to impersonate that machine. If the spoofing machine responds faster than the true trusted host, communications will be carried out with it unnoticed. Spoofing requires that the infiltrator have physical access to the network in a location that falls close to the target machine in the network topology, which usually means being physically close to the target machine.
- *Get into the system and cover tracks.* Once one of the above techniques is successful in gaining access to the system, the first order of business is to alter any records that would reveal the presence of an illegal entry to the system administrators.

- *Try to get superuser access*. Just as there are many ways to get into a user account, there are many ways to get into the root level account or get equivalent access to the machine.
- *Make back doors*. Once entry has been gained, that access can be used to intentionally install security breaches so that the hacker can still get back into the system if the original method of entry is cut off.
- *Use the system*. At this point, the hacker can steal data, destroy information, alter files, use CPU time, lock everyone else out of the system, etc.

How to Combat Illegal Entry

Here are a list of ways to make computers more secure and some minimal suggestions for when they should be used. For systems that are critical to operation, all of these and more may be warranted.

- *Physical security*. Keep doors locked if feasible. Install locks on accessible but attended machines. Install locks and alarms on machines left unattended.
- *Back up files*. This should be done on all computers.
- *Use a surge suppressor*. All computers.
- *Use an uninterruptable power supply*. Critical systems.
- *Periodic virus checking*. All PC and Macintosh computers. High volume or critical multiuser machines.
- *Continual memory resident virus checking*. PCs or Macs used by many people, such as in public labs. When data routinely comes from many sources.

- *Firewalls.* For organizations that can conduct business with limits on the internet services accessible from inside the organization. Where outside access to company data could do significant harm to the business.
- Having no internet connection or no internal network at all is done when data is particularly sensitive or reliability is of key importance. Bank record systems and air traffic control systems are some examples.
- Programmes to enforce the use of good passwords. Systems with a moderate to large number of users.
- *Password aging.* Systems which have a large number of users or are a likely target for illegal entry.
- *Remove old accounts.* Old, unused accounts are just that many more passwords for someone to find out. If it is not feasible to remove old accounts, the passwords can still be deleted. This is done by setting a null password for which no possible password will give acccess to the account.
- *Smart cards.* There are various varieties of smart cards to act as passwords electronically. One example is a card with a number that changes every ten seconds and has its internal clock synchronized to one in the central computer. This way, even if someone get the password, it is only good for ten seconds. This expense is only warranted when someone would have a clear motive for trying to break into a system.
- *Install security patches to the operating system.* Invisible security patches should be installed anytime

systems are being upgraded. On systems with many users or that are likely targets for illegal entry, the system administrator should install new patches frequently or perhaps instantly when available. Many break ins occur within 24 hours of when a security flaw and patch is announced. This occurs when someone has targeted a particular machine and hopes to figure out how to take advantage of the flaw before the system administrators upgrade the system. For this reason, many flaws are not announced until a patch or temporary work around can be announced with them. Networking patches and network software uprgrades are particularily important.

- *Security checking software*. There are programmes, like Satan, which will test a system for many known security flaws. These programmes were created so that administrators can test the integrity of the system, but they are also a favourite tool for the first step in infiltrating a system. It is a good idea to do this periodically. The software can be set to check many machines on a network without interrupting the people using those machines. There are programmes to check the system from the inside as well as checking network vulnerabilities.
- *Break in detection software*. There are also pieces of software to alert the system administrators when security is being tested by a known technique. This is a good way to know of an attack before they have gained entry.

- Some level of audit trail should be kept on any multiuser system and any system with sensitive data. Some level of auditing is built into many multiuser operating systems. An audit trail has to be maintained before a break in occurs in order to do any good.
- Use software to prevent sniffing, such as Kerberos or secure shell. These software packages allow remote logins to be authenticated, without sending an unencrypted password over the network. We have seen an increase in sites using these systems, particularily where many users login to machines remotely. The difficulty is setting up a system which is secure and reliable as well as not inconveniencing the users.
- *Encryption of disk files.* Disk files should be kept encrypted when the data is particularly important. Passwords, social security numbers and credit card numbers should always be encrypted. Many accounting systems use encryption.
- Do not use your credit card over the web unless your browser (not their web page) identifies it as a secure server. Even at that it is advisable only to do so with reputable companies that you are familiar with. You should never need a credit card number to get something that is free.
- Encrypted E-mail software should be used when someone would have a reason to want to see, forge or alter E-mail messages.

- *Random manual monitoring.* For a few businesses that deal with very sensitive information and must use networks, the security administrators will occasionally manually look at the information being passed over the network, particularly through the firewall. This probably is not warranted unless security is important enough to be paying someone solely as a security manager.
- *Hiring tiger teams*. A tiger team is a group of honest expert hackers that are hired to break into your system in order to give you an analysis of your security. This is generally done by banks or others with extremely sensitive data.

Data Security Technologies

Disk Encryption

Disk encryption refers to encryption technology that encrypts data on a hard disk drive. Disk encryption typically takes form in either software or hardware. Disk encryption is often referred to as on-the-fly encryption ("OTFE") or transparent encryption.

Hardware based Mechanisms for Protecting Data

Software based security solutions encrypt the data to prevent data from being stolen. However, a malicious programme or a hacker may corrupt the data in order to make it unrecoverable or unusable. Similarly, encrypted operating systems can be corrupted by a malicious programme or a hacker, making the system unusable. Hardware-based security solutions can prevent read and write access to data and hence offers very strong protection against tampering and unauthorized access.

Hardware based or assisted computer security offers an alternative to software-only computer security. Security tokens such as those using PKCS#11 may be more secure due to the physical access required in order to be compromised. Access is enabled only when the token is connected and correct PIN is entered. However, dongles can be used by anyone who can gain physical access to it. Newer technologies in hardware based security solves this problem offering fool proof security for data.

Working of Hardware based security: A hardware device allows a user to login, logout and to set different privilege levels by doing manual actions. The device uses biometric technology to prevent malicious users from logging in, logging out, and changing privilege levels. The current state of a user of the device is read by controllers in peripheral devices such as harddisks. Illegal access by a malicious user or a malicious programme is interrupted based on the current state of a user by harddisk and DVD controllers making illegal access to data impossible. Hardware based access control is more secure than protection provided by the operating systems as operating systems are vulnerable to malicious attacks by viruses and hackers. The data on hard disks can be corrupted after a malicious access is obtained. With hardware based protection, software cannot manipulate the user privilege levels, it is impossible for a hacker or a malicious programme to gain access to secure data protected by hardware or perform unauthorized privileged operations. The hardware protects the operating system image and file system privileges from being tampered. Therefore, a completely secure system can be created using a combination of hardware based security and secure system administration policies.

Backups

Backups are used to ensure data which is lost can be recovered.

Data Masking

Data Masking of structured data is the process of obscuring (masking) specific data within a database table or cell to ensure that data security is maintained and sensitive information is not exposed to unauthorized personnel. This may include masking the data from users (for example so banking customer representatives can only see the last 4 digits of a customers national identity number), developers (who need real production data to test new software releases but should not be able to see sensitive financial data), outsourcing vendors, etc.

Data Erasure

Data erasure is a method of software-based overwriting that completely destroys all electronic data residing on a hard drive or other digital media to ensure that no sensitive data is leaked when an asset is retired or reused.

5

Malicious Computer Attacks

Mafiaboy: Denial-of-Service Attacks Outside the Political Arena

On February 2000, news reports indicated that that Yahoo, Cable News Network, eBay, Amazon.com, E Trade, and Buy.com, (among other sites) experienced distributed denial of service ("DDOS") attacks. The challenges to apprehending the suspects proved substantial. In many cases, the attackers used "spoofed" IP addresses, so that the address that appeared on the target's log was not the true address of the system that sent the messages.

The FBI was able to identify a 16-year old Canadian teenager, known as "Mafiaboy" as a suspect by reviewing Internet chat room logs that showed Mafiaboy asking others what sites he should take down - before the sites were attacked. For example, there was discussion of a possible denial of service attack on CNN before CNN's site was taken down. Mafiaboy was arrested in April 2000. In January of 2001, Mafiaboy pleaded guilty to 56 counts of “mischief to data” in relation to the DDOS attacks from February 2000. He was charged with “a DDOS attack that brought down CNN.com, Amazon.com, eBay, Dell Computer and others between February 8 and 14, 2000. The teenager eventually received a sentence of eight months in detention followed by a year of probation for his actions. The judge also required him to donate $250 to charity. Mafiaboy allegedly caused more than US $1.5 billion in damage in connection with the various DDOS attacks.

Worms and Viruses

Both worms and viruses are malicious programs which propagate uncontrollably over the Internet. A worm program is to designed to invade a computer and replicate itself by sending the worm to other computers on a network or in the user’s address book. Worms cause damage by clogging up computer networks, slowing down or even crippling individual computers and shared servers.

Unlike worms, which do nothing but replicate themselves, viruses both replicate themselves and carry a malicious payload. This malicious payload may be a program which immediately corrupts or deletes data on the infected machine. Or the virus may unleash a “logic bomb” which lies dormant on the machine and destroys data when the infected computer’s clock reaches a certain date.

In the past, viruses and worms were spread through floppy disks and infected macro attachments to common files like Microsoft Word documents. Today, many viruses and worms are spread through e-mail and activated when the user opens an e-mail attachment. A “Trojan horse” is an e-mail attachment that appears benign. When the user opens the Trojan horse, however, a hidden worm or virus is activated that can damage the user’s computer and send itself to other computers on the user’s network.

In May of 2000, companies and individuals around the world were stricken by the “Love Bug,” a virus (or, technically, a “worm”) that traveled as an attachment to an e-mail message and propagated itself extremely rapidly through the address books of Microsoft Outlook users. According to the General Accounting Office, “The [Love Bug] virus reportedly hit large corporations such as AT&T, TWA, and Ford Motor Company; media outlets such as the Washington Post and ABC news; international organizations such as the International Monetary Fund, the British Parliament, and Belgium’s banking system; state governments; school systems; and credit unions, among many others, forcing them to take their networks off-line for hours.” Further the virus/worm also reportedly penetrated at least 14 federal agencies—including the Department of Defense (DOD), the Social Security Administration, the Central Intelligence Agency, the Immigration and Naturalization Service, the Department of Energy, the Department of Agriculture, the Department of Education, the National Aeronautics and Space Administration (NASA), along with the House and Senate. Damage estimates from the virus range upwards of $10 billion.

Investigative work by the FBI’s New York Field Office, with assistance from the NIPC, traced the source of the virus to the Philippines within 24 hours. The FBI then worked, through the LEGAT in Manila, with the Philippines' National Bureau of Investigation, to identify the perpetrator. The speed with which the virus was traced back to its source is unprecedented. The investigation in the Philippines was hampered by the lack of a specific computer crime statute. Nevertheless, Onel de Guzman was charged on June 29, 2000 with fraud, theft, malicious mischief, and violation of the Devices Regulation Act. However, those charges were dismissed in August 2000 by Philippine authorities upon determining that traditional laws did not apply to these newer high-tech cybercrimes.

As a postscript, it is important to note that the Philippine government on June 14, 2000 approved the E-Commerce Act, which now specifically criminalizes computer hacking and virus propagation.

Hacking

Hacking involves penetrating a secure area by subverting its security measures. Hackers might accomplish this by setting up programs like "war dialers" that try thousands of common passwords until one is accepted. A hacker may set up "packet sniffers," programs that scan data from the target system's network ports to find out more about a network and penetrate it more easily.

Once hackers penetrate the servers that host their target's computer systems, they can alter or remove files, steal information and erase the evidence of those activities. While many hackers break security systems just out of curiosity, other hackers, however, have attempted to use their skills for illegal personal financial gain.

Hacking for Financial Gain

Zezov and Yarimaka are both charged in a four-count Superseding Indictment with one count of unauthorized computer intrusion; one count of conspiracy; one count of interfering with commerce by using extortion; and one count of extortion of a corporation using threatening communications.

According to the Complaints filed in this case, Zezov gained unauthorized access to the internal Bloomberg Computer System from computers located in Almaty, Kazakhstan. In the Spring of 1999, Bloomberg provided database services, via a system known as the "Open Bloomberg," to Kazkommerts Securities ("Kazkommerts") located in Almaty, Kazakhstan. Zezov is employed by Kazkommerts and is one of four individuals at Kazkommerts associated with Kazkommerts' contract with Bloomberg.

In addition, according to the Complaints, Zezov sent a number of e-mails to Michael Bloomberg, the company's founder, under the name "Alex," demanding that Bloomberg pay him $200,000 in exchange for Zezov's telling Bloomberg how he was able to infiltrate Bloomberg's computer system.

According to the Complaints, in e-mail communications to Michael Bloomberg, Zezov demanded that $200,000 be deposited into an offshore account, and Bloomberg opened an account at Deutsche Bank in London and deposited $200,000 into the account.

As described in the Complaint against Yarimaka, Yarimaka and Zezov flew from Kazakhstan to London, and on August 10, 2000, Yarimaka and Zezov met with Bloomberg L.P. officials, including Michael Bloomberg, and two London

Metropolitan police officers, one posing as a Bloomberg L.P. executive and the other serving as a translator. At the meeting, Yarimaka allegedly claimed that he was a former Kazakhstan prosecutor and explained that he represented "Alex" and would handle the terms of payment. According to the Complaint, Yarimaka and Zezov reiterated their demands at the meeting. Shortly after the meeting Yarimaka and Zezov were arrested in London. The United States sought their extradition from England and, after being extradited, Yarimaka and Zezov arrived in the United States on May 17, 2002.

If convicted, Yarimaka and Zezov each face up to 5 years in prison on the conspiracy charge, up to 20 years in prison on the interference with commerce by using extortion charge; 2 years in prison for the extortion of a corporation using threatening communications charge; and 1 year in prison for the unauthorized computer intrusion charge. Each defendant faces a maximum fine of $250,000, twice the gross gain or loss resulting from the crime for each count.

Evolution and Profile of the Attacker

There is a growing convergence of technically savvy computer crackers with financially motivated criminals. Historically, most computer crime on the Internet has not been financially motivated: it was the result of either curious or malicious technical attackers, called crackers. This changed as the Internet became more commercialised. Financially motivated actors, spammers and fraudsters, soon joined crackers to exploit this new potential goldmine. Criminals have fully adopted the techniques of crackers and malicious code authors.

These are financially motivated people, who pursue their goals considerably more aggressively than an average cracker. They have the monetary means to buy the required expertise to develop very sophisticated tools to accomplish their goals of spamming and scamming the public. The perpetrators of these attacks vary considerably. At the low end are script kiddies, who are usually unsophisticated users that download malicious software from hacker web sites and follow the posted instructions to execute an attack on some target. These attacks are often only annoyance attacks, but they can be more severe.

At the next level are hackers who are trying to prove to their peers or to the world that they can compromise a specific system, such as a government web site. Next are insiders, who are legitimate users of a system that either access information that they should not have access to or damage the system or data because they are disgruntled. Insiders are often less knowledgeable then hackers, but they are often more dangerous because they have legal access to resources that the hackers need to access illegally. Next are organisational level attacks. In this case, the organisation's resources are used to get information illegally or to cause damage or deny access to other organisations to further the attacking organisation's gain. These can be legitimate organisations, such as two companies bidding on the same contract where one wants to know the other's bid in order to make a better offer.

They could also be criminal organisations that are committing fraud or some other illegal activity. At the highest level is the nation state that is trying to spy on or cause damage to another state. This level used to be called "national lab" attackers, because the attackers have a substantial amount of resources at their disposal, comparable to those that are available to researchers at a national lab, such as Los Alamos Laboratory or Lawrence Livermore Laboratory. After the September 11, 2001 terrorist attacks on the World Trade Center, the idea of nation state level cyber attacks being carried out by terrorists became a big concern.

Cyber crime Case Study: The Emerging Threat of Internet Bots

Network intrusions, data theft using Trojan horses, viruses and worms are among the threats security experts worry about on a regular basis. However, something more dangerous is emerging. Botnets, with their proliferation, sophistication and criminal use are emerging as the number one security threat. The recent arrest of 20-year old Californian man who made $60,000 by selling access to botnets to spammers and hackers is evidence of the growing menace.

A bot is a malicious software programme that invades computer so that it can covertly be controlled by a remote attacker. A bot is seeded by attackers through worms, viruses or other means to exploit desktop and server vulnerabilities. They are then herded into botnets, which can then be controlled from a central command point that can force zombie machines to work together to perform any issued task. Botnets are evolving and getting nastier. Previously, they were controlled exclusively through Internet Relay Chat (IRC) channels, but are now increasingly being manipulated through other means, such as Web, instant messaging or peer-to-peer systems.

Moreover, bots are using rootkits to conceal itself from the user of the machine. “Kernel level rootkits are extremely dangerous as they conceal their malicious code and cannot be removed by most anti-virus or antispyware programmes,” says Martin Overton, security specialist at IBM Global Service.

“The state of bot technology has reached the point that the state of Web technology has,” says Peter Tipett, CTO at Cybertrust, whose security experts found more than 12,000 people contributing to bots or renting out botnets. “Instead of fighting with each other, these guys are working together and posting their code. It’s evil open source. We are getting a rich set of commands and capabilities used by the bad guys.” Apart from evolving as sophisticated security threats, their presence is growing exponentially. Network-security experts identify and shut down botnets with 10 to 100 compromised hosts several times a day.

Crackdowns on large botnets with 10,000 or more hosts are rarer, but they still occur weekly, said Johannes Ullrich, chief technology officer for the Internet Storm Center, which detects, analyses, and disseminates information about Internet-related security problems.

“Security investigators have even found one botnet of 100,000 computers,” Ulrich noted. Research conducted by Symantec found that on average more than 60,000 botnets were activated each day in the first half of this year.

They also noted that this is an increase of more than 140 per cent from the previous year’s semi-annual count. The following sections discuss how hackers profile and select their victims, attack techniques and their criminal usage and defences home users and system administrators can undertake to mitigate the risk of these attacks.

Profiling and Target Selection

Hackers are diligently profiling hosts and choosing targets that can provide them with longest survivability and carry out large scale attacks, and prevent their detection.

High Bandwidth: One of the most sought after hosts are the machines connected to the Internet using high-bandwidth broadband. This can provide an attacker with an enormous cumulative bandwidth to carry out large scale DDoS attacks on target severs. Availability: Hosts with broadband connection are always connected to Internet and thus are the most sought after targets. This ensures hackers can carry out attacks round the clock without depending on whims of the users with dial-up connection which may connect to Internet at irregular intervals.

Low User Awareness and Monitoring Capability

Attackers prefer hosts where users have low security awareness and do not have access control mechanism like firewalls installed on their computers. The absence of such defences along with un-patched operating systems create ideal victims for hackers to break into and then install and maintain bots over a long period of time without being identified or traced.

Location

One of the prime goals of these cyber-criminals is to avoid detection after they commit crimes. They achieve this by selecting hosts that are geographically far away from their location. This makes very difficult for law enforcement officers to detect bots back to hackers. Also international prosecution being time consuming, expensive and non-standardised process that varies for each country, unfortunately ends up helping these cyber-criminals to go Scot-free. The typical profile that fits the above criteria is that of residential broadband connection that has low or no access control mechanism or university subnets connected to Internet with minimal monitoring, high bandwidth with high availability.

Attack Techniques

Bots generally employ one of several attack methods, but sometimes use multiple techniques to create a network of compromised computers. Some of these approaches are quite sophisticated, such as Phatbot, which can generate a new encryption for itself each time it infects a new system. This makes it difficult for the software to find a common code signature for and thus recognise Phatbot. According to Ken Dunham, director of malicious code for Security Consultancy iDefence, Phatbot has successfully evaded detection by mutating itself from spyware to launch vitriolic DDoS attacks on compromised networks. The following are some of the ways that attackers use to create networks of bots for themselves.

Chat

IRC is the most common used technique, including those in the large Phatbot/Agobot and Sdbot/Robot families as a way to communicate and receive commands from hackers. IRC has a built in mechanism for multicast capabilities which let attackers quickly send commands to all parts of a botnet without writing new code for the bot.

Peer-to-Peer

Many bots take advantage of peer -to-peer communication to infect computers with vulnerabilities. They connect to open-source file sharing technology such as Gnutella and work with the WASTE file-sharing protocol. WASTE uses a distributed directory rather than a central server which lets bots easily find each other and communicate with one another.

They can thus exchange hacker commands or other attack-related information among themselves. An attacker can initiate the process by serving as a peer in P2P network sending commands to one bot, which can then pass them onto the others. Thus, hackers don't have to communicate to bots via IRC multicasting. Decentralised-based bot systems are harder for security officials to trace or shutdown than systems using a single IRC source.

E-mail Attachments/Worms

Many hackers use methods such as e-mail attachments or worms to infect computers. Bots don't replicate or spread on their own, but they can use the worms' functionality to do so. In fact, hackers can spread bots more quickly with worms than with other methods.

In addition, Botnets can spread worms faster than worms can spread on their own. The Symantec Security Response team said 2004's Witty worm, which infected and crashed tens of thousands of servers, was probably launched by a botnet.

According to Huger, “we saw Witty break out more or less at the same time from a hundred or more machines. The machines were all over the world but they had something in common: they were on our bot list of compromised computers,” he noted.

Criminal use of Bots and Botnets

Bots can serve several purposes both legitimate and illegitimate. One legitimate purpose is to support the operation of IRC channels by conferring special administrative privileges or designated users. However, most of the common uses are criminally motivated for monetary gains or for destructive purposes.

Distributed Denial-of-Service Attacks

A DDoS attack is an attack on a computer system that causes a loss of service to users, typically the loss of network connectivity and services by consuming of the bandwidth of the victim network or overloading the computational resources of the victim’s system. Most commonly implemented and often used are TCP SYN and UDP flood attacks. One of the most common uses of DDoS attacks is to wrest control of an IRC channel from its founder and founder’s delegates. To take over an IRC channel, attackers conduct a DoS attack against one or more of the network’s servers. If they can succeed in downing a server they can split the network into two or more disconnected segments.

If in a given segment there are no users joined to a particular channel of interest, the attacker can join that channel and seize the founder’s privileges. Apart from the role in taking over IRC channels, attackers can launch successful DDoS attack against Internet sites. Let us assume if a given botnet has around 15,000 compromised hosts and has an associated bandwidth of 56kbps, a simultaneous attack by the entire botnet would direct almost 850 Mbps at its target – enough to cripple almost all e-commerce sites.

These estimates are conservative because most of these compromised machines have cable modem and DSL hosts. Moreover, because bots are widely distributed within the IP address space, filtering or blocking such DDoS attacks is not easy. At best, it requires cooperation between the target and multiple service providers. DDoS is not just limited to web servers; virtually any service available on the Internet can be a target of such an attack.

Higher-level protocols can be used to increase the load even more effectively by using very specific attacks, such as running exhaustive search queries on the victim's web site. Recursive HTTP flooding means that the bots start from a given HTTP link and follow all links on the provided web site in a recursive way. This is also called spidering. Further research also showed that botnets are used to run commercial DDoS attacks against competing corporations. Jay R. Echouafni and Joshua Schictel, alias EMP, ran botnets to send spam and carry out paid DDoS attacks to take a competitor's web site down. Echouafni was indicted on August 25, 2004 on multiple charges of conspiracy and causing damage to protected computers.

Spamming

Some bots enable SOCKS v4/v5 proxy – a generic proxy protocol for TCP/IPbased networking protocol on a compromised machine which allows them to launch spam attacks. Using bots and thousands of zombies (compromised machines) attackers can send massive amounts of bulk e-mails. These bots can also add special functionality to harvest e-mail-addresses. Harvested e-mail addresses help them to send phishing mail which appears to victims to come from legitimate sources.

Sniffing Traffic

Bots can be used as a packet sniffer to watch for interesting clear-text data passing by compromised machine. The sniffers are mostly used to retrieve sensitive information like usernames and passwords. They can also provide information about other Internet bots if it has been compromised more than once. This allows one to "steal" another's botnet.

Keylogging

If the compromised machine uses encrypted communication channels, then just sniffing the network packets on the victim's computer is useless since the appropriate key to decrypt the packets is missing. But most bots also offer features to help in this situation.

With the help of a keylogger it is very easy for an attacker to retrieve sensitive information. An implemented filtering mechanism further helps in stealing secret data. If the keylogger runs on thousands of compromised machines in parallel, it is easy to imagine how quickly PayPal accounts are harvested.

Spreading New Malware

In most cases, botnets are used to spread new bots. This is very easy since all bots implement mechanisms to download and execute a file via HTTP or FTP. But spreading an e-mail virus using a botnet is also attractive. A botnet with 10,000 hosts which acts as the starting base for a mail virus allows very fast spreading and thus causes more harm. The Witty worm, which attacked the ICO protocol parsing implementation in Internet Security System (ISS) products is suspected to have been initially launched by a botnet due to the fact that the attacking hosts were not running any ISS services.

Attacking IRC Chat Networks

Botnets are also used for attacks against Internet Relay Chat (IRC) networks. Popular among attackers is especially the so called "clone attack." In this kind of attack, the controller orders each bot to connect a large number of clones to the victim IRC network. The victim is flooded by a service request from thousands of bots or thousands of channel-joins by these cloned bots. In this way, the victim IRC network is brought down - similar to a DDoS attack.

Manipulating online polls/games

Online polls/games are getting more and more attention and it is rather easy to manipulate them with botnets. Since every bot has a distinct IP address, every vote will have the same credibility as a vote cast by a real person. Online games can be manipulated in a similar way. Mass identity theft Often the combination of different functionality can be used for large scale identity theft, one of the fastest growing crimes on the Internet. Phishing e-mails that pretend to be legitimate ask their intended victims to go online and submit their private information. These fake e-mails are generated and sent by bots via their spamming mechanism. These same bots can also host multiple fake web sites pretending to be Ebay, PayPal, or a bank, and harvest personal information. In addition, keylogging and sniffing of traffic can also be used for identity theft.

Defending Against Bots and Botnets

Defence against botnet infection and attack can be classified in three stages: prevention, detection and response. These stages need to be treated differently from home and system administrator perspective.

Prevention

The most common way for bots to compromise hosts is by exploiting the known vulnerabilities in the operating system or installed applications. Home users should follow guidelines regarding safe use by updating the installed OS and applications to defend their computers from being infected by attackers.

If available, they should activate the auto-patch update facilities included in many popular operating systems and applications. Users should always install the latest version of anti-virus software and practice safe handling of common web applications such as web browsers, e-mail, and instant messaging. In addition to this, every system administrator should be given training on online security and privacy issues. A high level of awareness on these issues is the best course in preventing malicious bots from infecting computers. They should implement access control measures and regularly monitor the generated logs on access control/ peripheral devices.

Detection

Home users can use Microsoft Antispyware and Antivirus software, which are able to detect and respond to known types of bots, but are not effective for new bots on net. Online resources for scanning a system can also be employed, like the Symantec online security checker which will scan the system for commonly used Trojan ports. In addition to detection techniques used by home users, system administrators can employ network based tools to monitor perimeter defence devices to detect anomalies in Internet traffic. Slow network response, unexpectedly high volumes of traffic, traffic on unusual ports, and unusual system behaviour indicate the presence of malicious software including bots. Tools like network packet sniffers can be used not only to identify but also to isolate the subnet/ machine which is generating malicious traffic. Analysis of the logs generated by network sniffer can also be used for finding IRC servers used, the names of the attacker's private channels and authentication keys.

Responses

As soon as the user realises that his/her computer has been compromised, the computer should be physically disconnected from the network. This denies access to the attackers and helps limit the potential damage both to user's own system and to other systems on the Internet. They should immediately update anti-virus software and check OS and application vendor sites for latest patches. If the user stores bank or credit card information on PC, the user should assume them to have been compromised and contact the appropriate organisation. Any passwords or secure data should be no more be used and changed at once. Apart from response measures suggested for the home user, system administrators should isolate infected subnets to prevent the spread of bots. They can asses the damage with the help of a network packet sniffer by identifying the number of machines infected by bots within a subnet. They can assist the incident response team by preserving data on the affected system and relevant system logs like firewalls, mail servers, IDS, DHCP servers, and proxies.

End

Growth of network models like IRC and easily available tools to edit bots has provided attackers, many whom have very limited knowledge of the underlying technology, the ability to create large botnets that are scalable and automated. Sophisticated bots are incorporating encryption and shape-shifting polymorphism in their code, and finding wider uses for rootkits, code that allows a permanent and undetectable presence of computer, to conceal itself from the user of the machine and creating nightmarish scenarios for security experts.

Moreover, hackers are also diligently picking victims with poorly implemented access control mechanisms, minimal monitoring to avoid detection, high bandwidth and software that is easy to infect and that allows for propagation. Bots are creating difficult challenges; nevertheless, users can fight back by proactively following best practices as recommended by the operating system and application vendors to prevent their machines from getting compromised in the first instance. Some of the reactive methodologies outlined include using packet sniffers, monitoring firewalls and preserving critical logs to help incident response teams track down the attackers. However, none of these, in isolation are effective. High level security awareness among users and diligent monitoring of the systems are the most effective and real defences against the growing menace of bots. Further, much research is being done at universities and institutions using honeynets to learn about attacker's tools, tactics, and motives, while developing ways to track these criminals. Government should encourage these research efforts as they may provide a future arsenal for law enforcement agencies against bots, the fastest emerging threat on net, which if left unchecked may jeopardise the safety of cyber world in coming years.

Hacking into the Department of Defense

On February 23, 2000, Ikenna Iffih, age 28, of Boston, Massachusetts, was charged with using his home computer to illegally gain access to a number of computers, including those controlled by NASA and an agency of the U.S. Department of Defense, where, among other things, he allegedly intercepted login names and passwords, and intentionally caused delays and damage in communications.

In April 1999, Iffih obtained unauthorized access to a corporate internet account which he then used to illegally access a computer controlled and operated by the U.S. Defense Logistics Agency. Iffih then concealed his actual computer address through a service known as "telnet proxy" which created the appearance that his address was that of the government's computer. Once "hidden", Iffih accessed, without authorization, the web site of internet service provider, ZMOS, and recklessly caused damage to the ZMOS computer located in the State of Washington. As a result, ZMOS, which hosts corporate web pages and provides internet service for corporate customers, suffered a significant loss of business.

Beginning in May 1999 and continuing until August, 1999, Iffih obtained unauthorized access to the same corporate internet account this time using it to access the NASA computer research project web server located in Maryland. Iffih seized control of the NASA computer, allowing him to read, delete or modify any files on the system. He then installed a "sniffer" program onto the system to intercept and save login names and passwords of users that were transferred over the NASA system for his own later use. The compromised NASA web server did not contain classified or sensitive information and was not involved in any way with satellite command or control.

Iffih also used the NASA computer as a platform to launch attacks on other computer systems, such as an attack on the U.S. Department of the Interior's web server where he defaced its web page with hacker graphics.

Iffih accessed various computers operated by Northeastern University from which he illegally copied a file containing the names, dates of birth, addresses and social security numbers of numerous men and women affiliated with the University, either as students, faculty, administration or alumni. Investigators are not aware of any use or dissemination of this information. Northeastern University cooperated fully with investigators on this matter.

On June 29, 2000, Iffih pleaded guilty in federal court to three felony counts. Count one pertained to intentionally intercepting and endeavoring to intercept login names and passwords transmitted to and through a National Aeronautics and Space Administration ("NASA") computer. Count two was intentionally and without authorization accessing a web site, used for interstate and foreign commerce, owned by Zebra Marketing Online Services ("ZMOS"), causing significant damage. Count three was willful and malicious interference with a U.S. Government communication system, that of the Defense Logistics Agency, and obstructing, hindering and delaying the transmission of communications over such system.

On November 17, 2000, he was sentenced to 6 months home detention, placed on supervised release for 48 months, and ordered to pay $5,000 in restitution to victim ZMOS.

Legalizing Hacking by Hollywood?

The growth of peer-to-peer (P2P) networks has been staggering, even by Internet standards. From non-existence a few years ago, today nearly a dozen P2P networks have been deployed, a half-dozen have gained widespread acceptance, and one P2P network alone is responsible for 1.8 billion downloads each month. The steady growth in broadband access, which exponentially increases the speed, breadth, and usage of these P2P networks, indicates that P2P penetration and related downloading will continue to increase at a breakneck pace.

Unfortunately, the primary current application of P2P networks is unbridled copyright piracy. P2P downloads today consist largely of copyrighted music, and as download speeds improve, there has been a marked increase in P2P downloads of copyrighted software, games, photographs, karaoke tapes, and movies. Books, graphic designs, newspaper articles, needlepoint designs, and architectural drawings cannot be far behind. The owners and creators of these copyrighted works have not authorized their distribution through these P2P networks, and P2P distribution of this scale does not fit into any conception of fair use. Thus, there is no question that the vast majority of P2P downloads constitute copyright infringements for which the works' creators and owners receive no compensation.

The massive scale of P2P piracy and its growing breadth represents a direct threat to the livelihoods of U.S. copyright creators, including songwriters, recording artists, musicians, directors, photographers, graphic artists, journalists, novelists, and software programmers. It also threatens the survival of the industries in which these creators work, and the seamstresses, actors, Foley artists, carpenters, cameramen, administrative assistants, and sound engineers these industries employ. As these creators and their industries contribute greatly both to the cultural and economic vitality of the U.S., their livelihoods and survival must be protected.

While pursuit of many of these components to the P2P piracy solution requires no new legislation, I believe legislation is necessary to promote the usefulness of at least one such component. Specifically, enactment of the legislation I introduce today is necessary to enable responsible usage of technological self-help measures to stop copyright infringements on P2P networks. One approach that has not been adequately explored is to allow technological solutions to address technological problems. Technological innovation, as represented by the creation of P2P networks and their subsequent decentralization, has been harnessed to facilitate massive P2P piracy. It is worth exploring, therefore, whether other technological innovations could be harnessed to combat this massive P2P piracy problem. Copyright owners could, at least conceptually, employ a variety of technological tools to prevent the illegal distribution of copyrighted works over a P2P network. Using interdiction, decoys, redirection, file-blocking, spoofs, or other technological tools, technology can help prevent P2P piracy.

There is nothing revolutionary about property owners using self-help — technological or otherwise — to secure or repossess their property. Satellite companies periodically use electronic countermeasures to stop the theft of their signals and programming. Car dealers repossess cars when the payments go unpaid. Software companies employ a variety of technologies to make software non-functional if license terms are violated. However, in the context of P2P networks, technological self-help measures may not be legal due to a variety of state and federal statutes, including the Computer Fraud and Abuse Act of 1986. In other words, while P2P technology is free to innovate new, more efficient methods of P2P distribution that further exacerbate the piracy problem, copyright owners are not equally free to craft technological responses to P2P piracy.

Through the legislation I introduce today, Congress can free copyright creators and owners to develop technological tools to protect themselves against P2P piracy. The proposed legislation creates a safe harbor from liability so that copyright owners may use technological means to prevent the unauthorized distribution of that owner's copyrighted works via a P2P network.

This legislation is narrowly crafted, with strict bounds on acceptable behavior by the copyright owner. For instance, the legislation would not allow a copyright owner to plant a virus on a P2P user's computer, or otherwise remove, corrupt, or alter any files or data on the P2P user's computer.

The legislation provides a variety of remedies if the self-help measures taken by a copyright owner exceed the limits of the safe harbor. If such actions would have been illegal in the absence of the safe harbor, the copyright owner remains subject to the full range of liability that existed under prior law. If a copyright owner has engaged in abusive interdiction activities, an affected P2P user can file suit for economic costs and attorney's fees under a new cause of action. Finally, the U.S. Attorney General can seek an injunction prohibiting a copyright owner from utilizing the safe harbor if there is a pattern of abusive interdiction activities.

This legislation does not impact in any way a person who is making a fair use of a copyrighted work, or who is otherwise using, storing, and copying copyrighted works in a lawful fashion. Because its scope is limited to unauthorized distribution, display, performance or reproduction of copyrighted works on publicly accessible P2P systems, the legislation only authorizes self-help measures taken to deal with clear copyright infringements. Thus, the legislation does not authorize any interdiction actions to stop fair or authorized uses of copyrighted works on decentralized, peer-to-peer systems, or any interdiction of public domain works. Further, the legislation doesn't even authorize self-help measures taken to address copyright infringements outside of the decentralized, P2P environment.

This proposed legislation has a neutral, if not positive, net effect on privacy rights. First, a P2P user does not have an expectation of privacy in computer files that she makes publicly accessible through a P2P file-sharing network - just as a person who places an advertisement in a newspaper cannot expect to keep that information confidential. It is important to emphasize that a P2P user must first actively decide to make a copyrighted work available to the world, or to send a worldwide request for a file, before any P2P interdiction would be countenanced by the legislation. Most importantly, unlike in a copyright infringement lawsuit, interdiction technologies do not require the copyright owner to know who is infringing the copyright. Interdiction technologies only require that the copyright owner know where the file is located or between which computers a transmission is occurring.

No legislation can eradicate the problem of peer-to-peer piracy. However, enabling copyright creators to take action to prevent an infringing file from being shared via P2P is an important first step toward a solution. Through this legislation, Congress can help the marketplace more effectively manage the problems associated with P2P file trading without interfering with the system itself.

6

Computer Insecurity

Assurance Problems and Sources of Credibility in Cyber Contracting

Securing property rights is not enough, if one is to enjoy the potential benefits of low cost communication in cyberspace. Individuals must have others to communicate with, and for many kinds of communication, this requires the development of trust and/or recourse. This is one reason for the relatively rapid growth in and relatively large size of B2B trading on the internet, compared to B2C trading. Much of the B2B trading in e-commerce is probably being carried out between firms that had off-line repeat-deal trading relationships and are simply moving on line in order to lower transactions costs.

They already have trust relationships. Others may not have previously established trust relationships but they may belong to the same business community (e.g., trade association) or the firms may have built off-line reputations that they can take with them when they move on line. Some new businesses also have developed on-line and engage in B2B e-commerce, of course, and these new firms have to establish trust relationships or have access to recourse if they are going to flourish. Similar points can be made about on-line B2C trading, of course. Many on-line retailers have pre-existing off-line reputations. These firms are relatively likely to be able to establish profitable on-line businesses relatively quickly. New retailers who only operate on line will face higher costs as they attempt to establish credibility. Thus, for instance, a 2004 survey of on-line retailers found that 93 percent of the firms who had on-line web sites as well as off-line catalog business reported making a profit, as did 85 percent of the traditional retailers (i.e., firms with real-space retail stores) who had established web sites (Tedeschi 2004a: 1). On the other hand, only 67 percent of the retailers who sell exclusively through the internet, described as a group as "still struggling to achieve profitability," reported profits, and many of them had suffered substantial losses the year before. Survival of such firms clearly requires that they solve the assurance problem. The same is true for individuals who may want to engage in many other kinds of on-line interactions.

Building Trust in Cyberspace

When two strangers initiate an interaction, such as trade, the typical process involves several small steps rather than an immediate large commitment. The two strangers start by attempting to gather information about the potential partner, and if nothing negative is discovered, they make a small commitment (e.g. a small trade). If that is successful, additional transactions occur and they can get larger, but substantial commitments will not occur until a strong trust relationship develops. This can take some time, so the payoff to investments in establishing such relationships are delayed and very uncertain, making the incentives to do so relatively weak and suggesting that the emergence of cooperative interaction based on such sources of trust may be slow. However, while trust can develop through repeated dealing, it can also be achieved through investments in reputation building.

Firms that exclusively trade on the internet are not in a position to invest in some of the non-salvageable assets that traditional firms do, such as elaborate store fronts (elaborate Web pages might be a substitute, but they are not likely to be seen as large investments). Advertising is an option, however. On-line advertising is ubiquitous, of course.

Spam is cheap, and probably does nothing for the reputations of firms choosing that method of advertising (indeed, it is probably viewed as a signal of unreliability for many internet users), but many on-line services also survive on advertising revenues, much as television networks do. Such advertising is probably perceived to be very inexpensive, however, so it may not be an effective method of reputation building. Of course, even though advertising appears to be inexpensive, high levels of advertising could be effective, and it appears that many firms believe that it will be. AOL paid $435 million for Advertising.com, a firm that sells ads on a network of web sites, for instance, and Modem Media was bought by Digitas in a $200 million stock transaction.

Ives (2004: 1) reports that $5.6 billion was spent on online advertising during the first nine months of 2004, citing TNS Media Intelligence, an organization that tracks advertising spending. This was a 25.8 percent increase over the same period in 2003. However, this was only about 5.5 percent of total advertising spending ($102.5 billion) for the period, "a stubbornly small portion" (Ives 2004: 1) approximately equal to the amount spent on radio advertising, suggesting that these investments are probably not as effective at signaling reliability as off-line advertising (e.g., celebrity endorsements, television adds during prime time, etc.). As a consequence, many cyber firms attempting to use this means of building recognition and reputation have resorted to advertising in the physical universe too. Television and magazine advertising by firms trying to establish themselves in internet markets is now common place. Cyberspace actually offers means of building reputation that are likely to be less effective in real space, however, because information can be spread very rapidly and cheaply

Specialists in the supply of information have developed. For instance, some companies send free products to prominent reviews on sites like Epinions.com and Slashdot.org even though the reviewers have no official status or credentials.

These forums have developed methods for measuring the reputations of their review contributors, and some, such as Epinions, actually pay small fees to reviewers, determined by how readers react to the reviews. Epinions also allow users to comment on individual reviews as well as on products, and teams of experienced users of the site are used as monitors to detect efforts by a producer or employ to "plug" a product. Similarly, Slashdot measures how frequently a person contributes and how valuable other users feel that contributions are, and then gives each user a "karma" rating that determines their access to some of the site's privileges.

Perhaps the most widely cited and studied on-line reputation mechanism has been developed on eBay. EBay acts as an on-line intermediary through which sellers post auctions and buyers bid. It obtains its revenues form seller fees following a successful auction, and it has developed an innovative feedback mechanism that facilitates reputation formation and reputation-based sanctions.

Following an auction, the buyer and the seller can give a "grade" (+1, 0, -1) to the other party in the exchange, and provide a textual comment. EBay then displays several aggregations of the grades received by both sellers and buyers (an overall rating that ads the grades from the person's entire eBay history; the percent positive, the date the person first registered on the site, a summery of recent reviews, and the entire feedback record). A large portion of its traders are repeat players. In fact, it has been estimated that around 500,000 people make full- or part-time livings through on-line auction sales (Murphy 2004: 1).

Reputation has become very valuable for both buyers and sellers. Sellers with good reputations obtain higher prices, expand their sales if they want to, and survive to sell again and again (e.g., Dewally and Ederington (2003), Resnick, et al. (2003), Cabral and Hortacsu (2004)). Indeed, people who have recognized reputation status can get better deals than infrequent sellers, so they are increasingly able to act as agents for others who want to trade only infrequently.

In 2003 there were an estimated 30,000 people doing so through eBay's trading assistants program, and several new "store-front" firms had opened up as consignment operations "specifically to take in merchandise to sell on eBay" (Alexander 2003: 1). These firms were competing for business on the basis of price, and AuctionBytes, an Internet newsletter provides a chart comparing prices among these consignment shops so sellers can obtain information about alternatives without visiting several locations. Buyer reputation also matters. After all, feedback on buyers is also posted, so sellers can avoid selling to those who have reputations for being difficult to deal with because there are so many potential buyers in the on-line auction market.

Individuals clearly can build reputations in cyberspace, but there are alternatives as well. Certifications of quality and/or performance can be purchased. For instance, in response to customer complaints about fraud by sellers in travel auctions, eBay introduced a rule requiring all sellers of vacation packages, cruises, lodging, and air travel to register with SquareTrade, a privately owned seller-verification company that also provides dispute resolution. SquareTrade will certify the seller only if he or she verifies the company's name, contact information, and location.

Sellers often do not have to be required to seek certification, however. For example, Dewally and Ederington (2003) examine the impact of quality certification by Comic Guaranty LLC of comic books sold through eBay and find that certified comic books command a 50 percent higher price on average, and their prices are higher regardless of the seller's eBay reputation (reputation also significantly influenced price, as suggested by other studies, such as Resnick, et al. (2003), and Cabral and Hortacsu (2004)). Certification providers like Comic Guaranty LLC, Professional Sports Authenticator, and numerous others generally have developed reputations for specializing in the inspection and grading of specific types of items in real space (e.g., comic books, sports cards), but their certifications carry tremendous weight in cyberspace market. Other certification providers have developed on line in order to provide on-line firms with their "seals of approval" regarding various aspects of quality or performance.

VeriSign Inc. is a leading supplier of encryption technology and public key arrangements. In addition to supplying the encryption/public-key services, VeriSign also provides a digital certificate "verifying that messages sent with a public key are sent by the entity to whom VerisSign distributed that key, an audit service that monitors the entity's use of and continued security of their public key infrastructure (guaranteeing that this entity is the only one with access to the private key for example) and a 'legal' authority to revoke or suspend a certificate in the even that an entity does not pass an audit".

A VeriSign customer gets a "trustmark" which is posted on his or her website. Clicking on the trustmark moves the user to VeriSign's secure server where the current information and status of the customer's digital certification is displayed. This does not completely solve the assurance problem, of course, since the users must be confident that the site that they have been transported to is actually VeriSign's website, and they must trust VeriSign. However, as Hadfield (2000: 29) notes, such certification options takes "a commitment problem which arises at thousands or even millions of websites and folds them back to a commitment problem for a single entity: VeriSign Inc.… Fundamentally, this structure moves the commitment problem from an entity (the individual e-commerce website) that faces incentives for security breach (because it is costly to maintain security or because there are gains to be had from distributiong information that is suppose to be kept secret) to an entity that faces incentives for security maintenance." After all, the value offered by certification companies like VeriSign is their ability to provide secure systems and their reputation for providing audits and revocations of certification from customers who fail to meet their security requirements.

Similar certification procedures are developing to take care of other consumer protection and privacy concerns that arise in e-commerce. A group of internet firms, including Microsoft and AOL have started a organization called the Online Privacy Alliance. This group, in conjunction with the Electronic Frontier Foundation (a non-profit organization promoting freedom of expression in cyberspace, and funded by founders of Lotus Development Corporation and Apple Computers) and The Boston Consulting Group, started TRUSTe, a non-profit corporation which has established a set of practices regarding respect for user privacy, and which provides a "trustmark" to firms that adopt those practices. TRUSTe performs audits of firms to make sure that they adhere to the practices. Certified firms have a seal that, when clicked, takes users to the firms' privacy statements, as well as a "click-to-verify" seal that takes the user to TRUSTe's secure server where the seal is authenticated. TRUSTe monitors compliance through regular reviews and by submitting user information that contains identifiers that are then tracked through the firm's system. In addition, it has a "watchdog" site where users can report privacy-policy violations and other concerns. These reports are made available to users of TRUSTe's website. TRUSTe also maintains a dispute resolution process to resolve complaints by users who feel that their private information has been misused.

Certification of quality and performance standards is also available in cyberspace. Several suppliers of certification have developed. For instance, the American Institute of Chartered Public Accountants and the Canadian Institute of Chartered Accountants (AICOA/CICA) offer a WebTrust program. This combined group established procedures for auditing on-line business practices regarding privacy, security, and the handling of complaints about quality and performance. Firms that obtain a favorable report from a CPA or CA with a WebTrust license, are issued an Enrollment Identification (EID) that allows them to apply for certification by a private firm like VeriSign that has an agreement to manage a WebTrust seal. Clicking on the seal takes the user to the certificate and the accounting report. Periodic audits ensure continuing compliance. Firms with WebTrust seals also must agree to submit consumer complaints that are not resolved through negotiation to a WebTrust-approved third-party dispute resolution process of on-line binding arbitration. Similarly, BBBOnline offers a "Reliability seal" to certify that an on-line business is "reliable" and "trustworthy,"along with a three-stage dispute resolution process.

Certification seals are non-salvageable assets, of course, and such investments provide a potential method of building reputation quickly. Non-salvageable assets provide a source of recourse against those who have invested in them, because information about wrongful behavior can cause the investment to lose value. Certification can be withdrawn, for instance, and reputation build through good behavior (e.g., as on eBay) or good reviews (e.g., as from Epinions reviewers) can lose value as a result of changes in the willingness to deal with the wrongdoer by others who receive the negative information. Other methods of punishment are also available to individuals in cyberspace, but as reputation mechanisms (including certification) develop, such methods are likely to become relatively less important.

Security and Systems Design

Most current real-world computer security efforts focus on external threats, and generally treat the computer system itself as a trusted system. Some knowledgeable observers consider this to be a disastrous mistake, and point out that this distinction is the cause of much of the insecurity of current computer systems - once an attacker has subverted one part of a system without fine-grained security, he or she usually has access to most or all of the features of that system. [citation needed] Because computer systems can be very complex, and cannot be guaranteed to be free of defects, this security stance tends to produce insecure systems.

The 'trusted systems' approach has been predominant in the design of many Microsoft software products, due to the long-standing Microsoft policy of emphasizing functionality and 'ease of use' over security. Since Microsoft products currently dominate the desktop and home computing markets, this has led to unfortunate effects.

However, the problems described here derive from the security stance taken by software and hardware vendors generally, rather than the failing of a single vendor. Microsoft is not out of line in this respect, just far more prominent with respect to its consumer marketshare.

It should be noted that the Windows NT line of operating systems from Microsoft contained mechanisms to limit this, such as services that ran under dedicated user accounts, and Role-Based Access Control (RBAC) with user/group rights, but the Windows 95 line of products lacked most of these functions. Before the release of Windows 2003 Microsoft has changed their official stance, taking a more locked down approach.

On 15 January 2002, Bill Gates sent out a memo on Trustworthy Computing, marking the official change in company stance. Regardless, Microsoft's operating system Windows XP is still plagued by complaints about lack of local security and inability to use the fine-grained user access controls together with certain software (esp. certain popular computer games).

Financial Cost

Serious financial damage has been caused by computer security breaches, but reliably estimating costs is quite difficult. Figures in the billions of dollars have been quoted in relation to the damage caused by malware such as computer worms like the Code Red worm, but such estimates may be exaggerated.

However, other losses, such as those caused by the compromise of credit card information, can be more easily determined, and they have been substantial, as measured by millions of individual victims of identity theft each year in each of several nations, and the severe hardship imposed on each victim, that can wipe out all of their finances, prevent them from getting a job, plus be treated as if they were the criminal. Volumes of victims of phishing and other scams may not be known.

Individuals who have been infected with spyware or malware likely go through a costly and time-consuming process of having their computer cleaned. Spyware and malware is considered to be a problem specific to the various Microsoft Windows operating systems, however this can be explained somewhat by the fact that Microsoft controls a major share of the PC market and thus represent the most prominent target.

Reasons

There are many similarities (yet many fundamental differences) between computer and physical security. Just like real-world security, the motivations for breaches of computer security vary between attackers, sometimes called hackers or crackers. Some are teenage thrill-seekers or vandals (the kind often responsible for defacing web sites); similarly, some web site defacements are done to make political statements.

However, some attackers are highly skilled and motivated with the goal of compromising computers for financial gain or espionage. An example of the latter is Markus Hess who spied for the KGB and was ultimately caught because of the efforts of Clifford Stoll, who wrote an amusing and accurate book, The Cuckoo's Egg, about his experiences. For those seeking to prevent security breaches, the first step is usually to attempt to identify what might motivate an attack on the system, how much the continued operation and information security of the system are worth, and who might be motivated to breach it. The precautions required for a home PC are very different for those of banks' Internet banking system, and different again for a classified military network. Other computer security writers suggest that, since an attacker using a network need know nothing about you or what you have on your computer, attacker motivation is inherently impossible to determine beyond guessing. If true, blocking all possible attacks is the only plausible action to take.

Vulnerabilities

To understand the techniques for securing a computer system, it is important to first understand the various types of "attacks" that can be made against it. These threats can typically be classified into one of these seven categories:

Exploits

Software flaws, especially buffer overflows, are often exploited to gain control of a computer, or to cause it to operate in an unexpected manner. Many development methodologies rely on testing to ensure the quality of any code released; this process often fails to discover extremely unusual potential exploits. The term "exploit" generally refers to small programs designed to take advantage of a software flaw that has been discovered, either remote or local. The code from the exploit program is frequently reused in trojan horses and computer viruses. In some cases, a vulnerability can lie in certain programs' processing of a specific file type, such as a non-executable media file.

Eavesdropping

Any data that is transmitted over a network is at some risk of being eavesdropped, or even modified by a malicious person. Even machines that operate as a closed system (ie, with no contact to the outside world) can be eavesdropped upon via monitoring the faint electro-magnetic transmissions generated by the hardware such as TEMPEST. The FBI's proposed Carnivore program was intended to act as a system of eavesdropping protocols built into the systems of internet service providers.

Malware and Threat Evolution

Viruses started appearing on dedicated networks such as the ARPANET in the 1970s. The boom in personal computers, initiated by Apple in the early 1980s, led to a corresponding boom in viruses. In 1981 the first virus in the wild came into being even before the experimental work that defines viruses of today. Founded on the Apple II operating system, it was spread on Apple II floppy disks containing the operating system. While the viruses of the 1980s targeted a variety of operating systems and networks, most viruses today are written to exploit vulnerabilities in the most commonly used software: Microsoft Windows.

The increasing number of vulnerable users is now being actively exploited by virus writers. The first malicious programmes may have shocked users, by causing computers to behave in unexpected ways. However, the viruses which started appearing in the 1990s present much more of a threat: they are often used to steal confidential information such as bank account details and passwords. Classic file viruses reigned supreme in the 90s; however they have almost totally disappeared today. There are currently about 10 file viruses that are still active.

They experience peaks of activity when they infect the executable files of worms: the file virus will then travel as far as the infected worm file. For instance, samples of MyDoom, Netsky and Bagle that are infected by file viruses such as Funlove, Xorala, Parite or Spaces. On the whole, there is very little danger that classic file viruses will cause any major epidemics. The trends in epidemiology that are observed today have their primary roots in the second half of 2003. Internet worms Lovescan, Sobig, Blaster, Slammer and Sobre all not only caused global epidemics, but also profoundly changed the malware landscape.

Each of these malicious programmes set new standards for virus writers. In 2003, we witnessed the emergence of an attack type that combines exploitation of server and workstation vulnerabilities with the characteristics of virus and Trojan horses. By using more efficient attack vectors and, therefore, minimizing the human effort required to deliver attacks and use the compromised systems, the risks related to newly discovered vulnerabilities moved up in the risk measurement scale. Optimising costs, achieving greater efficiency, and applying the minimum necessary effort to accomplish goal are central concepts to modern day life. Therefore, it is not difficult to identify the same approach in the vulnerability exploitation techniques and attack trends.

The appearance of many efficient worms as a result of attackers' attempts to maximize their bang for the "bug" are examples. They compromise a very large number of systems with minimal effort. The steadily increasing amount of cross-site scripting and SQL injection vulnerabilities discovered and disclosed during 2003 point to another path of less resistance into vulnerable networks. These vulnerabilities have rather simple ways of exploitation and they provide casual attackers with a high yield, direct access to internal networks, compromise of database servers and their content, and indirect ways of attacking unsuspecting users of third-party systems. The level of sophistication in worms seen in 2003 and the installation of backdoors and tools with elaborate communication protocols and auto update capabilities indicate that attackers are trying to optimise the management of large amounts of newly acquired assets.

Classic e-mail worms are on the decline, with network and instant messaging worms exploiting relatively lax security to take their place in early 2005. IM worms were at the peak of their development in spring and summer 2005, and showed the highest growth rate among all classes of network worms.

In the first six months of this year, an average of 28 new IM worms were detected every month. It should be stressed here that when P2P worms were at the peak of their evolution in 2003, approximately 10 new variants were detected every week. However, the situation changed afterwards and the flood of IM worms suddenly dried up. AOL and MSN, both of which have proprietary IM clients, were the main targets for such worms.

Both companies took measures to protect their users. Firstly, by blocking the transmission of files with names and extensions which were known to be used by IM worms. In spite of the fact that IM worms rarely use file transmission as a propagation method, the move did have a noticeable effect. The next step was to block the worms' main method of propagation, hyperlinks leading to files containing the body of the worm. These actions closed the majority of security loopholes being exploited by virus writers. And most importantly, they closed the loopholes which IM worms based on source code circulating in the computer underground used. Most of the code used in IM worms is of fairly low quality. The majority of these worms are created by script kiddies who have no significant programming skills.

When the off the shelf code was no longer effective, these self styled virus writers were unable to create new propagation methods on their own, and this led to a sharp drop in the number of new worms. Improved antivirus technologies, and increased user awareness of security issues are clearly forcing virus writers and hackers to use new approaches to access users' information and systems, mostly in the form of phishing attacks. Malicious users are starting to use viruses which propagate by exploiting vulnerabilities within web applications, particularly Internet Explorer, rather than network and e-mail worms. One consequence of this is an increase in the number of compromised sites. Exploits for IE are placed on compromised sites, which means that users who visit these sites will have trojan programmes downloaded to their machines.

To date Linux-based platforms have mainly been the victims of rootkit attacks and simple file viruses. However, the growing number of publicised vulnerabilities means that the increased number of users switching to Linux will not remain untouched by new malware. Handheld devices, such as PDAs and cell phones are almost household appliances for many people. Virus writers have been quick to take advantage of their growing popularity. The first trojan for Palm OS appeared in September 2000.

And finally, the increasing interest in on-line games, with the potential profits to be made in this area, make it more than likely that malicious code designed to steal such information will continue to evolve rapidly. The first Trojan for gaming consoles had also been discovered.

Sony PlayStationPortable was the first victim - the Trojan targeting this device deleted system files causing the console to cease functioning correctly. This behaviour is very similar to Trojans for mobile phones. It may be that these new Trojans for gaming consoles signal the start of a new interest among virus writers.

Evolution of Exploit Frameworks

Cyber criminals increasingly rely on powerful exploitation frameworks to launch their attacks. Free tools like Metasploit and commercial tools like CORE IMPACT and Immunity CANVAS have revolutionised the attackers' methodology. Previously, upon finding a vulnerability, the attacker either had to create custom exploit code from scratch or scour the Internet to find such code to exploit the hole.

Today, instead of scraping together a bunch of individual exploits, these integrated exploit frameworks include around one hundred or more exploits to compromise target systems. One property of the exploit tools is the separation of the exploit from the payload. An exploit is the software that takes advantage of a flaw, letting the attacker load and execute a programme of the attacker's choosing.

The code triggered by the exploit is known as the payload. Old-fashioned attacks tightly bundled exploits and payloads together. An attack might exploit a database buffer overflow with the purpose of adding a user for the attacker to the local administrators group. But, with this tight integration, the attackers were stuck with the given payload attached to the given exploit for the given vulnerability. Taking the payload from one attack and embedding it with another exploit required some serious machine-language fine tuning, and was often impossibly difficult.

To remedy the situation, today's exploit frameworks include an arsenal of different exploits and an arsenal of different payloads, each offering a different effect the attacker wants to have on the victim. So today, the attacker can use a tool like Metasploit to choose an exploit, such as a buffer overflow in lsass.exe, originally used by the Sasser worm last year. Then, the attacker can choose from more than a dozen different payloads. Metasploit packages the payload with the exploit, and then launches it at the target. The real effect of these frameworks in separating the exploits and the payloads is now reverberating through the industry.

Developers who create fresh exploits for new flaws don't have to reinvent the payload wheel every time. Thus, they can focus their time on perfecting their exploits and producing them much more quickly. Moreover, those developers who don't focus on exploits can now zoom in on the production of high-quality payloads.

Defence Evolution

Computer security has been reactive for most part. That is, system administrators and security professionals are usually reacting to the latest attack. After they fix the vulnerability that allowed the attack, the attackers look for new vulnerabilities to exploit for new attacks. Trends in worm and virus delivery mechanisms and infection speed have also changed. Not long ago, a virus warning and the patch to vaccinate computers against it would appear days before the virus began spreading.

Today, too often the first sign of a virus is that a part of the network goes down. Flash worms such as SQL Slammer have paved the way for future worms to carry payloads that directly target their victims and wreak havoc on government, business, and societal structures. Existing technologies such as firewalls, intrusion detection systems, intrusion protection systems, virtual private networks (VPNs), and virus scanners provide integrated security solutions. Not surprisingly, security has become a massive industry, and it is now a focal point for virtually every organisation. Proactively eliminating just the known threats places an impractical burden on existing server and network infrastructures.

Eliminating unknown threats or zero day attacks, which as the name implies reveal themselves only when they first occur, requires real-time solutions that can identify unique attacks without overburdening the network with security and management overhead. The imagination of social engineers knows no bounds. Social engineers are highly aware of Internet user psychology and are well able to exploit current anxieties. In connection with this it should be stressed that the attempts of some companies to create a browser which is capable of determining the veracity of any site visited, or a browser which protects information stored on the potential victim machine is very hard to be one hundred percent successful.

Cyber Victims

Early exploits were mass attacks which affected the whole Internet community. Between 1996 and 2000, high-profile web sites such as eBay, the U.S., Department of Commerce, UNICEF, the New York Times and Microsoft all fell victim to hackers or defacers. The Melissa virus caused company e-mail servers to shut down. A fraudulent web page that was designed to appear to be a Bloomberg financial news story resulted in the shares of a small tech company increasing 31 percent in response to the "news." As the new millennium began, a huge, distributed DoS attack shut down major Web sites such as Yahoo! and Amazon.

Apache, RSA Security, and Western Union were hacked. The Code Red worm attacked thousands of web servers, and the Sircam virus hit e-mail accounts all over the world. As of today, spam accounts for fifty percent of all e-mail sent, a staggering 12.4 billion messages a day, worldwide. Malicious users are now changing their focus from conducting mass attacks to targeting specific business structures, and these attacks are tailored to each individual case. Identity thefts and credit card fraud are prevalent attacks affecting the public directly. Social engineering remains a threat, and the methods used are continuing to evolve.

The biggest mass mailings were comparable in size to the activity shown in December of 2004 through and January, when cyber scammers exploited the tsunami in South East Asia. Cyber criminals target people who are new to the Internet gullible. With huge numbers of people connecting to the Internet for the first time every year, cyber criminals always have a fresh crop of Net newbies on which to prey. Elderly people, youngster and kids are also among the top targets.

Current Situation

The Computer Security Institute (CSI) announced the results of its 10th annual Computer Crime and Security Survey. The survey showed that virus attacks continue as the source of the greatest financial losses, accounting for 32 percent of the overall reported losses. Theft of proprietary information also showed a significant increase in average loss per respondent, more than double that of last year. Also unauthorised access showed a dramatic increase and replaced denial of service as the second most significant contributor to computer crime losses, accounting for 24 percent of overall reported losses and showing a significant increase in average dollar loss. On a better note the total dollar amount of financial losses resulting from security breaches is decreasing, with an average loss of $204,000 per respondent, down 61 percent from last year's average loss of $526,000. However the percentage of organisations reporting computer intrusions to law enforcement has continued its multiyear decline. Respondents cited the concern over negative publicity as the key reason for not reporting intrusions to law enforcement.

Criminal and Legal Aspects of Fighting Computer Crime

Nowadays, intensive use of computer technologies in various spheres of human activity has significantly changed an idea of a place and a role of information in present-day society. National information resources have appeared as a new economic category. They became one of the most important factors of post industrial world development. Society is getting features of an information society. This happens owing to development of computer technologies processing information.

Unfortunately, new kinds of crime as "computer crime", "cyber terrorism" and "information war" appeared. Special anxiety is related to crimes in sphere of computers. Number of computers in developed countries is constantly growing. Trend of increase in such crimes is extending. We have a number of cases illustrating computer technologies use for criminal purposes. Serious problems of information security constantly arise as homeland is integrating in the Internet.

A united policy is realized at the state level on purpose of national interests security maintenance from threats in information sphere; a balance of need for free information exchange and admissible restrictions for its distribution are established; the legislation is being improved; activity of state authorities on safety in the information environment is being coordinated; state information resources are being protected at defence enterprises; native telecommunication and information means are being developed; information structure of IT development is being improved; means of search, collecting, storage, processing and the analysis of information are being unified on purpose of entering global information infrastructure.

The urgency of research in this issue is caused also by a problem of increase in efficiency of fighting computer criminality on the part of law enforcement. Creating of the corresponding legal base in law enforcement agencies is of high priority.

In process of studying the legislative experience in foreign countries, some separate scientists drafted recommendations and offers on criminal legal regulation of this field in native legislation.

According to D. Azarov "regulations in the new Criminal Code concerning responsibility for crimes in sphere of computers and computer systems demand a careful analysis. We consider that it is necessary to take into account experience of other European countries in this sphere. Issues of criminalization and, probably, decriminalization of certain actions in sphere of computers, systems and networks demand a further studying. The international experience shows a presence of certain actions that belong to a category of computer crimes, and crimes of some other character, rather than those which attributes are determined in the Criminal Code".

Especially, European Council experts in criminal law suggest to criminalize such socially dangerous acts in sphere of computer information:

1) computer fraud;
2) computer forgery;
3) damage of computer information or software;
4) computer sabotage;
5) unauthorized access;
6) unauthorized interception.

The analysis of law that regulates public information relations in Ukraine, allows to assert that our government takes measures of stimulating the infrastructure development on the basis of the newest technologies, along with necessary measures of containment and counteraction to negative events in sphere of computer technologies.

Among top-priority steps of state policy in sphere of counteraction to computer criminality is an appearance of new Section 16 in the Criminal Code of Ukraine-"Crimes in Sphere of Computers, Systems and Networks". Having recognized information as a subject of theft, assignment, extortion and other criminal acts, criminal law has confirmed status of information as an object of the property right that is coordinated with substantive regulations of information legislation. Till recently, criminal legal doctrine unreasonably unfilled information from the list of possible subjects of theft or other property crimes.

In this connection, appearance of the mentioned section in the Code is natural and objective necessity of legal means in process of solving problems related to fundamental modification of technology, world outlook of people, international relationship under conditions of a wide scope computerization of information sphere.

As is well-known, "Illegal interference with operation of computers, systems and networks", that is an illegal interference with operation of automated computers, systems or networks resulted in distortion or erasing of computer information or destroying its carriers, and also to spreading of computer viruses by using software and hardware designed for illegal penetration into these machines, systems or networks and capable of distortion or erasing computer information or destroying its carriers";

"Theft, misappropriation, extortion of computer information or its capture by swindling or abusing official position" and the "Violation of automated electronic computer operating rules": violation of operating rules of automated computers, systems or networks on the part of a person responsible for their operation, if it has entailed theft, distortion or erasing of computer information, security means, or illegal copying of computer information, or essential infringement of such facilities, systems or networks operation.

The components of crimes defined in the mentioned section are correlated with existing needs of public legal actuality. Also, they are aimed at protection maintenance of the corresponding rights, liberties and legitimate interests of individuals and legal entities. Unfortunately, these legal norms have some weaknesses at the same time.

The owner of automated system is any person that legally uses services of information processing as the proprietor of such system (computer, systems or networks) or as the person that has the right to use such system.

It always has a character of fulfilment of certain actions, and it can be a penetration into computer system by use of special technical means or software, allowing to overcome installed systems of protection from illegal application of obtained passwords or masking under a kind of a legal user with purpose of penetration into computer system.

So, "illegal interference with operation of automated computers, systems and networks that has led to distortion or destruction of computer information or carriers of such information" as penal action. This component of crime is of material character. Consequences are obligatory element of the crime. The person who has performed the specified actions in forms, not defined in the Article 361, is not subject to criminal liability.

The Criminal Code has established the responsibility for distribution of computer viruses. But an obligatory element of the objective side of this crime lies in the way of its commitment, namely: by application a software and/or other means with intent of illegal penetration into automated machines, systems and networks and capable to cause distortion or destruction of computer information or carriers of such information. If the person distributes a computer virus in a different way or by application of other instruments and means which are not bearing the above-stated attributes in aggregate, such person is not subject to the responsibility according to the Criminal Code.

Direct object of a crime is the information property right, that is the broken right of the proprietor's ownership, use or control over information. Interpretation of this term in a context of automated systems is placed in the Article 1 of the Automated Systems Information Security Law "... information in automated systems is a set of all data and programs used in automated systems, irrespectively of means of their physical and logic representation... ".

Displays of the objective side of crime components are: actions like distortion or destruction of computer information or carriers of such information, and also distribution of... carriers of such information, and also distribution of computer virus.

As used here, destruction of information is its loss, when information in sphere of computers, systems and networks ceases to exist for individuals and legal entities that have full or limited property right to it. Termination of access to information should be considered as blocking of information. Such actions can be performed, for example, with the help of electromagnetic, laser and other effect on data carriers in which info is materialized or with the help of which it is transferred; by forming of signals of means and blocks of programs effecting information, its carriers and means of technical protection that causes violation of integrity of information, its distortion or destruction.

Distortion of information is a modification of its contents, violation of its integrity, including partial destruction. Establishing of a mode of access to information is regulated by the Information Law. It defines the order of reception, use, distribution and retention of information. Depending on a mode of access, information is divided into open information and information with restricted access (confidential and secret). According to the Article 30 of the mentioned law, confidential information is data which is in ownership, use or order of separate individuals or legal entities and is distributed, at their will, according to the terms provided for by them.

Citizens and legal entities that own information of professional, business, industrial, commercial and other character, having obtained it due to own means, or such which is a subject of their professional, business, industrial, commercial and other interest and does not break secret provided for by law, have the right to define independently a mode of access to it, including its belonging to the confidential category, and establish a system (ways) of its protection.

Secret information is information containing data, making state and others secret defined by the law, disclosure of which cause damage to the person, society and the state.

We offer to understand the damage caused by criminal acts (direct and indirect losses) which size is equal or exceeds 100 minimal free incomes of citizen as heavy consequences.

The components of this crime are characterized by presence of the general subject. Commitment of such actions by the person which professional duties include preservation or processing of such information should be admitted as the attribute that burdens the responsibility.

Material components structure of the crime is chosen for developing of the first part of this norm. The structure establishes the necessity of criminal consequences approach, like distortion or destruction of computer information or carriers of such information.

The Article directly defines mental attitude of the person to own actions, therefore the guilt form of such person is intention only.

Unfortunately, the Criminal Code does not adjust a situation when interference with operation of automated computers, systems or networks is performed owing to careless actions. Thus, the significant amount of possible infringements and even actions which are really performed with intent, as it is hard to prove the intent of the computer criminal during investigation of circumstances of intervention (e.g. a person that usually uses e-mail in the Internet, probably not deliberately but also owing to carelessness, may distribute computer viruses).

Theft, assignment, extortion of computer information or its abstraction by swindle or official position abusing (referring to the Article 362) concerns only "computer" crimes. They make the majority among files of offences in sphere of computers, systems and networks.

The definition of "computer information", introduced by the legislation, is very important. In our opinion, it is necessary to understand it as an aggregate of all identified and owned date, used in computers, systems and networks. The identified information is information fixed in the machine carrier with essential properties allowing to identify it.

The given norm of the Criminal Code, naturally, does not contain concrete technical requirements. It refers to departmental instructions and the rules establishing the operating procedure and which should be set specially by the authorized person and be brought to users. Application of the specified Article to the Internet is impossible; its effect applies only to local networks of organizations.

An investigatory relation should be established between the fact of violation of operation rules of automated computers and the fact of caused essential harm. It should be completely proved, that consequences come exactly from violations of operation rules.

Determining of essential harm provided for by the Article 361 is an evaluating process. The harm is determined by court in each concrete case, in view of all circumstances, however it is obvious, that essential harm should be less significant, rather than essential consequences. A criminal realizes that he is breaking operation rules; he foresees an opportunity and inevitability of illegal influence on information and causing essential harm or meaningly wishes causing such harm. Such action is punished by deprivation of the right to occupy certain positions or by engaging in certain work for the term up to five years or correctional work for the term up to two years.

Part 1 of the Article 363 of the Criminal Code is complicated for interpretation of the contents. Grammatical, logical and system structural analysis of all the Article allows to say that illegal copying of computer information and essential infringement of operation of automated computers, systems and networks are not forms of crime provided for by this Article, and make up only a set of possible consequences which can arise as a result of its commitment. Part 2 of the Article 363 has a blanket reference to described in the Part 1 illegal action.

One more feature of crime is provided for by the Article 363 of the Criminal Code. Only a special subject accounts for its commitment, it is the person responsible for operation of automated computers, systems and networks.

Legal Policies on Cyber crime

In its nascent stages, cyber crime enjoyed a special legal status that belied common practice used in adjudicating crimes. Hacking was commonly perceived as a prank perpetrated by teenagers. Later, the lone, highly skilled attacker working against a high value target was mythologised and revered in some ways. The media and movie industry continued to foster the notion, so that when Kevin Mitnick was arrested in 1995, there was a relative groundswell of support for his release, despite having broken into systems, stolen millions of dollars in proprietary software, "altered information, corrupted system software, and eavesdropped on users, sometimes prevented or impeded legitimate use."

The idea that cyber crime was "different" from regular crime persisted into the dawn of the Internet age, helped along by an unwillingness among police to get involved in patrolling and investigating cyberspace. Such reluctance may have been due to lack of reference points in law, low rates of successful prosecutions and international resistance to help track cross-border crimes. The perception that cyber criminals are different entities has now been thoroughly discouraged. Indeed, "prosecutors are starting to make aggressive use of the Computer Fraud and Abuse Act, which carries penalties of up to 20 years in prison. The lengthiest sentence so far has been nine years, issued in December." There is no longer any calls to be lenient on a those who use computers to exploit, steal and abuse privileges, such as the Californian software executive who conspired to steal trade secrets from a competitor by illegally accessing network and computer systems.

The change in these commonly held notions happened gradually, but importantly, there is now a strong sense of civic empowerment given to the government to apprehend cyber criminals, which when coupled with the renewed diligence attributed to preventing terrorism, has allowed legislation to evolve rapidly in the past few years. As computers have become more integral to daily life, allowing users to conduct higher value operations, they have naturally become targets for those imbued with the criminal tendency.

Most users have recognised the threat and the need for protection, even if they ignore certain precautions, like maintaining the secrecy of passwords. If users notice that they can no longer effectively use their workstations, legislation has usually been proposed, albeit after a lengthy period of discussion. For example, a few years ago, spam was threatening to overwhelm the usefulness of e-mail. Subsequently, congress passed the CAN-SPAM Act of 2003, which made certain practices, like harvesting e-mail addresses, illegal, while imposing maximum fines of up to one million dollars.

Despite flaws that some detractors have brought up, such as continuing to allow e-mail addresses to be sold to third parties, the act has provided a legal threshold to base decisions upon and brought notoriously flagrant spammers to justice. In a broader sense, the government has reacted to the demand for better enforcement and the need to extend legal jurisdiction over crimes that may have not been crimes before. The Cyber Security Enchancement Act of 2002, which fell under the Homeland Security Act, and the USA PATRIOT Act both instituted changes to deal with cyber crime. Other, more comprehensive laws, like the Fraud and Related Activity in Connection with Computers, located in the the US Criminal Code and Unlawful Access to Store

Communications have been codified for a longer period of time. The increase in awareness of cyber criminality has begun to manifest itself with the passage of laws, creation of organisations and advisory committees and powers granted to enforcement agencies. Their application to current cyber crime has found varying degrees of success. What needs to then be examined and discussed with the aforementioned issues in mind are the crafting of laws, enforcement and effectiveness. These have to be multiplexed across national and international settings, while being interpreted within a framework of technology and trends that are rapidly evolving. Only then can a broad understanding of the legal policies surrounding cyber crime be achieved.

International Cyber Crime

A significant problem that arises when working with cyber crime is that most crimes transit data through a multititude of international borders before reaching the final, intended target. Such circuitousness has a deleterious effect on investigating cyber crimes as well as the application of laws. An illustrative example of the legal hurdles faced with international incidents comes from the "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" manual for the United State Department of Justice. The manual reports that when seeking assistance from ISPs overseas, officers must work "with the consent of that country," which means certain formalities need to be resolved before proceeding.

First, prior permission of the foreign government must be obtained. Next, approval from the Justice Department's Office of International Affairs, and finally a clear indication that the actions would not be objectionable in the foreign country. The process is long and unwieldy, especially since, by the time the necessary paper work is filed, ISPs may have already deleted the information. Or in a worse case, after the information is obtained, it will then be discovered that the attacker went through another country, forcing the process to be repeated. Many developing countries are short on the resources and technical knowledge needed to expedite this process, causing the investigation to fail.

By 1997, the problem was being recognised internationally and the G-8 Justice and Interior Ministers noted that to be "consistent with the principles of sovereignty and the protection of human rights, nations must be able to collect and exchange information internationally, especially within the short time frame so often required when investigating international high-tech crimes." To aid this process they created a Point of Contact network which required participating countries to specify a specific group that could assist 24 hours a day, 7 days a week. By 2002, twenty countries were participating. These types of mutual legal assistance treaties (MLATs) have been effective where in the past law enforcement has been stymied.

For example, in 1992, the US government required assistance from Switzerland regarding an attack in the U.S., but since, Switzerland had no such laws regarding hacking on the books, they refused to help. In devising MLATs, a country can either create bilateral or multilateral relationships, each having its own benefits and drawbacks. Traditionally, sovereign nations have entered bilateral agreements with countries that they trust and are willing to accept each other's legal characteristics. They are quicker to negotiate, produce more detailed documents, are easier to change and allow nations to feel more comfortable sharing sensitive information. In fact, after the 2001 terrorist attacks, the US was eager to more quickly establish such ties and has concluded over 45 such agreements.

The drawbacks of course are that separate, and perhaps unequal, agreements must be reached, resulting in varying interpretations of crime and legal precedent. Multilateral pacts seem more suited to issues that are global in scale, much like cyber crime. Thus, it was with great fanfare that in November of 2001, thirty countries signed the Council of Europe's Convention on Cyber crime. The convention had been five years in the making and represents the first truly multinational attempt at defining, regulating and providing a framework for the legal issues in relation to cyber crime.

Briefly, it established conduct that is prohibited, identified required national legal processes and addressed international cooperation. At the U.S., Senate hearings on ratifying the treaty, Swartz noted "in the past, if an electronic transmission's trail led to another country, the chances were slim of successfully tracking the communication to its source or securing the evidence before deletion. With the tools provided for under the Convention, however, the ability of U.S., law enforcement to obtain international cooperation in identifying major offenders and securing evidence of their crimes so that they can be brought to justice will be significantly enhanced." Although the Senate Foreign Relations Committee approved the treaty, it has stalled in the Senate for nearly two years, as certain groups have opposed it for reasons related to civil liberties.

The current state of multinational legislation thus remains a patchwork of bilateral treaties put together piece by piece. Establishing transnational treaties is a difficult task and remains as an open policy debate. What can be agreed upon is that all nations need multilateral assistance in a global sense, not just a limited group, as cyber criminals can route through any country. Treaties, then, need to harmonise laws, while building capabilities. Most importantly, such treaties should not be used to violate human rights, even though to do so may be legal in some countries.

For example, with the current Convention on Cyber crime, China could ask the U.S., to assist in finding political dissidents and supporters of democracy and the U.S., would be obliged, under the terms of the Convention, to provide assistance. More often than not, even if a successful conviction can be obtained, extraditing a criminal is still a tough legal battle. For example, in October of 2001, a Pakistani man was charged with defacing an American-Israeli organisation's web site. The FBI, working with the U.S., Embassy in Pakistan, was able to identify the attacker and get a warrant issued for his arrest in Pakistan, yet three years later he is still at large. Clearly, there is a need for a more comprehensive international plan.

Future Trends in Legislation

The direction of legislation has slowly been proceeding to more severe and serious punishments for cyber crime. November 3 saw the first prosecution for owning and operating a botnet system. It seems probable as legislatures, federal and state, become aware of threat posed by botnets, and as methods become more advanced in discerning botcontrollers, legislation aimed at the problem will follow. Whether it will become an effective deterrent probably rests with the ability to investigate and prosecute. Another area of concern is identity theft, a process facilitated to a large degree through the Internet. California has been the first to create legislation aimed at companies with lax security regarding the protection of personal information they may store. The California Security Breach Information Act (SB-1386), which went into effect in July of 2003, forces organisations to notify individuals if there is such a security breach.

It has been a powerful method for not only making people aware of the issue, but also applying a force for change in policy within many organisations, lest they be branded as uncaring and incompetent. With more sensitive information being stored by a greater number of third parties, more states will come to the conclusion California has and indirectly apply pressure to organisations to reform. In another example, a recent piece of county legislation in Westchester, New York proposed to make it illegal for companies storing personal information to allow insecure access to their networks. In a sense, it would criminalise using a wireless network with no security measures. Although, many have pointed out specific weaknesses in the bill, the idea has been praised as a step in the right direction and an important conduit for educating the public.

Cyber crime presents a challenging position for lawmakers, as they struggle to keep up with changes in technology and in the methods used to exploit those technologies for maliciousness. Unfortunately, legal wrangling leaves the judicial system in a state that can be behind the times. It should be realised that in the end, laws can only do so much to regulate an activity. Proactive security, user education and vigilance, combined with effective forensics and enforcement remain the best remedies for combating cyber crime. Legislation still needs to enact appropriate punishments and establish frameworks, though and in that sense it has a crucial role to play in the mitigation of cyber crime.

Mitigating Cyber Crime Activity

Although it is inevitable that cyber crime will increase and continue to explore new vectors for undermining privacy, authentication and law enforcement, there will also be valid and useful attempts for mitigating the abilities of criminals, as well as the effects of cyber crime. These solutions will take form in better software, anti-spyware and anti-virus software integrated into operating systems and more user education regarding phishing and identify theft. These solutions will come primarily from software vendors themselves. On the other side, legislators will work with banks to reduce and prevent fraud, putting some of the liability with those most able to prevent it.

Finally, advanced solutions coming out of research and academia will try to inhibit the inherently anonymous and insecure nature of the Internet. With Microsoft's upcoming release of Vista, the latest version of their operating system, they'll have a new chance to focus on not only improving the general security of the system through fundamental changes, but also in providing methods for eliminating common problems, such as botnets, spyware and phishing attacks. In October of 2005, Microsoft began working together with the FTC to educate customers about botnets and the danger of allowing a computer to turn into a zombie. To deal with the problem of phishing, Microsoft released a programme in July of 2005 called the “Microsoft Phishing Filter,” which aims to invalidate the ability of phishers to reach Microsoft customers by dynamically notifying them when there is a high chance that what is being viewed is a phishing attack.

Finally, Microsoft released their “AntiSpyware” programme in January of 2005, to be included with Vista as well, that automatically scans your computer for programmes that match spyware signatures or that try to perform suspicious actions, like modifying system functionality or trying to run upon computer start up.

If cyber crime continues to grow to epidemic proportions, as all indications seem to point to, legislation will invariably step in, but more importantly, those with the most to lose will become more involved. This includes credit card companies, banks, lending operations and other organisations dealing with monetary transactions. Paypal.com has quickly come to dominate the online payment industry, while also serving as a bank in many capacities. With only an e-mail address and a password required to send money, this low hanging fruit has been one of the most heavily exploited realms for phishing attacks. In response, Paypal has offered at least a thousand dollars of purchase protection and a supposed one hundred percent protection against unauthorised payments sent from an account.

A fraud investigation team responds to queries and according to their web site, they have software that automatically monitors every transaction for inconsistencies. This last measure used by Paypal has also become fertile ground for credit cards companies, as their systems have become powerful at identifying fraudulent purchases though the use of neural networks, a type of software emerging out of the field of artificial intelligence. In some cases, this software has been able to reduce fraud by thirty percent or more. It's important to remember that the systems are not perfect solutions, but do address a large portion of illegal activity. Combined with other efforts, the goal is to reduce the effect of fraud, while making it more difficult to achieve.

Legislation will attempt to do its part as well, even though it has moved notoriously slowly when dealing with cyberthreats. The past few years have seen laws specifically crafted for spam and dealing with attacks that threaten the integrity of the infrastructure of the Internet. If the botnet problem continues to grow, coupled with identify theft, surely more action will be taken. Although, it is still unclear how effective it will be without a significant contribution to cyberforensic development and funding for the various governmental enforcement agencies responsible for handling cyber crime matters.

Another issue discussed in the Legal Policies section is the need for more international cooperation in locating, extraditing and prosecuting foreign criminals when possible, as the current system leaves much to be desired. Finally, as with any dangerous and difficult problem, there will be new and inventive ways to handle security issues coming out of research. One contribution that has limited, but not eliminated many common security flaws that are exploited, is the use of randomisation in dealing with code, data and other programmatic necessities. By introducing a factor of unpredictability, it can make the work of a hacker much more difficult and prone to error, limiting the ability of those who do not posses the skill to effect a novel attack. Other interesting proposals have included trace back systems that can remove the anonymous identity of data traveling through the Internet, devising a system for fast and accurate discovery of the source of even one packet of data.

Stopping distributed denial of service attacks and worm discovery has also been proposed as a method that can be automated and integrated into the backbone of the Internet, high speed routers. By analysing similar patterns coming from separate locations, such detectors can realise an attack while it is in its infancy and isolate infected hosts. There is also still room for ISPs to actively monitor and discourage botnets, spam and DDoS attacks from occurring. As the first link in the chain for many zombie hosts, as well as attackers, they are in a prime position for stopping spam, either by blocking outgoing mail, which most users have no need for, or by identifying when one host is sending out a large amount of data that does not match expected behaviour.

Additionally, if they noticed that a number of hosts were acting in concert, with regards to the data being disseminated from those machines, they may assume with likelihood that they are being controlled remotely. Consequently, the ISPs can examine logs to find who is sending the commands and initiate a complaint with the F.B.I. The problem holding back this kind of proactive approach has not been technical in nature, but rather legalistic, as it can be considered an invasion of privacy. Furthermore, such methods are being used to track down minor copyright violations, instead of focusing on more substantial problems, such as cyber crime and identify theft.

Looking Ahead

The future of the Internet is still up for grabs between criminals and normal users. Fears of a cyber-apocalypse still abound, while the potential extent of damage that can be caused by wide scale fraud is nearly unbounded. These anxieties should be rationally tempered with the knowledge that the problems are being addressed, although perhaps not fast enough. The usefulness of the Internet has proved itself in numerous and myriad ways that will hopefully be enough to ensure it does not become a wasteland of criminal activity and a bastion for the malicious.

The government still has an important role to play, but most of the prevention needs to be done by commercial entities producing software and those with the ability to stop fraud. Relying on consumer education programmes will only affect a percentage of possible victims. The others need to be automatically protected through measures that do not stress and require considerable participation. Security needs to be easy and effective if it is do work. Whether cyber crime is still a pertinent issue ten years from now is unknowable in a sense, but if the Internet will continue to grow, it must be solved so that the realities of cyber crime will be proportional to real-world crimes, if not better.