Security Threats and Threat Motives to Computer Networks

3

3.1 Introduction

In February, 2002, the Internet security watch group CERT Coordination Center first disclosed to the global audience that global networks, including the Internet, phone systems, and the electrical power grid, are vulnerable to attack because of weakness in programming in a small but key network component. The component, an Abstract Syntax Notation One, or ASN.1, is a communication protocol used widely in the Simple Network Management Protocol (SNMP).

There was widespread fear among government, networking manufacturers, security researchers, and IT executives because the component is vital in many communication grids, including national critical infrastructures such as parts of the Internet, phone systems, and the electrical power grid. These networks were vulnerable to disruptive buffer overflow and malformed packet attacks.

This example illustrates but one of many potential incidents that can cause widespread fear and panic among government, networking manufacturers, security researchers, and IT executives when they think of the consequences of what might happen to the global networks.

The number of threats is rising daily, yet the time window to deal with them is rapidly shrinking. Hacker tools are becoming more sophisticated and powerful. Currently, the average time between the point at which a vulnerability is announced and when it is actually deployed in the wild is getting shorter and shorter.

Traditionally, security has been defined as a process to prevent unauthorized access, use, alteration, theft, or physical damage to an object through maintaining high confidentiality and integrity of information about the object and making information about the object available whenever needed. However, there is a common fallacy, taken for granted by many, that a perfect state of security can be achieved; they are wrong. There is nothing like a secure state of any object, tangible or not, because no such object can ever be in a perfectly secure state and still be useful. An object is secure if the process can maintain its highest intrinsic value. Since the intrinsic value of an object depends on a number of factors, both internal and external

J.M. Kizza, *Guide to Computer Network Security*, Computer Communications and Networks, DOI 10.1007/978-3-319-55606-2_3

to the object during a given time frame, an object is secure if the object assumes its maximum intrinsic value under all possible conditions. The process of security, therefore, strives to maintain the maximum intrinsic value of the object at all times.

Information is an object. Although it is an intangible object, its intrinsic value can be maintained in a high state, thus ensuring that it is secure. Since our focus in this book is on global computer network security, we will view the security of this global network as composed of two types of objects: the tangible objects such as the servers, clients, and communication channels and the intangible object such as information that is stored on servers and clients and that moves through the communication channels.

Ensuring the security of the global computer networks requires maintaining the highest intrinsic value of both the tangible objects and information—the intangible one. Because of both internal and external forces, it is not easy to maintain the highest level of the intrinsic value of an object. These forces constitute a *security threat* to the object. For the global computer network, the security threat is directed to the tangible and the intangible objects that make up the global infrastructure such as servers, clients, communication channels, files, and information.

The threat itself comes in many forms, including viruses, worms, distributed denial of services, and electronic bombs, and derives many motives, including revenge, personal gains, hate, and joy rides, to name but a few.

3.2 Sources of Security Threats

The security threat to computer systems springs from a number of factors that include:

Weaknesses in the network infrastructure and communication protocols that create an appetite and a challenge to the hacker mind

The rapid growth of cyberspace into a vital global communication and business network on which international commerce and business transactions are increasingly being performed and many national critical infrastructures are being connected

The growth of the hacker community whose members are usually experts at gaining unauthorized access into systems that run not only companies and governments but also critical national infrastructures

The vulnerability in operating system protocols whose services run the computers that run the communication network

The insider effect resulting from workers who steal and sell company databases and the mailing lists or even confidential business documents

Social engineering

Physical theft from within the organizations of things such as laptop and handheld computers with powerful communication technology and more potentially sensitive information

Security as a moving target

3.2.1 Design Philosophy

Although the design philosophy on which both the computer network infrastructure and communication protocols built have tremendously boosted was cyberspace development, the same design philosophy has been a constant source of the many ills plaguing cyberspace. The growth of the Internet and cyberspace in general was based on an *open architecture work in progress* philosophy. This philosophy attracted the brightest minds to get their hands dirty and contribute to the infrastructure and protocols. With many contributing their best ideas for free, the Internet grew in leaps and bounds. This philosophy also helped the spirit of individualism and adventurism, both of which have driven the growth of the computer industry and underscored the rapid and sometimes motivated growth of cyberspace.

Because the philosophy was not based on clear blueprints, new developments and additions came about as reactions to the shortfalls and changing needs of a developing infrastructure. The lack of a comprehensive blueprint and the demand-driven design and development of protocols are causing the ever present weak points and loopholes in the underlying computer network infrastructure and protocols.

In addition to the philosophy, the developers of the network infrastructure and protocols also followed a policy to create an interface that is as user-friendly, efficient, and transparent as possible so that all users of all education levels can use it unaware of the working of the networks and therefore are not concerned with the details.

The designers of the communication network infrastructure thought it was better this way if the system is to serve as many people as possible. Making the interface this easy and far removed from the details, though, has its own downside in that the user never cares about and pays very little attention to the security of the system.

Like a magnet, the policy has attracted all sorts of people who exploits the network's vulnerable and weak points in search of a challenge, adventurism, fun, and all forms of personal gratification.

3.2.2 Weaknesses in Network Infrastructure and Communication Protocols

Compounding the problems created by the design philosophy and policy is the weakness in the communication protocols. The Internet is a packet network that works by breaking the data to be transmitted into small individually addressed packets that are downloaded on the network's mesh of switching elements. Each individual packet finds its way through the network with no predetermined route, and the packets are reassembled to form the original message by the receiving element. To work successfully, packet networks need a strong trust relationship that must exist among the transmitting elements.

As packets are disassembled, transmitted, and reassembled, the security of each individual packet and the intermediary transmitting elements must be guaranteed. This is not always the case in the current protocols of cyberspace. There are areas where, through port scans, determined users have managed to intrude, penetrate, fool, and intercept the packets.

The two main communication protocols on each server in the network, UDP and TCP, use port numbers to identify higher-layer services. Each higher-layer service on a client uses a unique port number to request a service from the server, and each server uses a port number to identify the service needed by a client. The cardinal rule of a secure communication protocol in a server is never to leave any port open in the absence of a useful service. If no such service is offered, its port should never be open. Even if the service is offered by the server, its port should never be left open unless it is legitimately in use.

In the initial communication between a client and a server, the client addresses the server via a port number in a process called a *three-way handshake*. The three-way handshake, when successful, establishes a TCP virtual connection between the server and the client. This virtual connection is required before any communication between the two can begin. The process begins by a client/host sending a TCP segment with the synchronize (SYN) flag set; the server/host responds with a segment that has the acknowledge valid (ACK) and SYN flags set, and the first host responds with a segment that has only the ACK flag set. This exchange is shown in Fig. 3.1. The three-way handshake suffers from a *half-open* socket problem when the server trusts the client that originated the handshake and leaves its port door open for further communication from the client.

As long as the half-open port remains open, an intruder can enter the system because while one port remains open, the server can still entertain other three-way handshakes from other clients that want to communicate with it. Several half-open ports can lead to network security exploits including both TCP/IP and UDP protocols: Internet Protocol spoofing (IP spoofing), in which IP addresses of the source element in the data packets are altered and replaced with bogus addresses, and SYN flooding where the server is overwhelmed by spoofed packets sent to it.

In addition to the three-way handshake, ports are used widely in network communication. There are well-known ports used by processes that offer services. For example, ports 0 through 1023 are used widely by system processes and other highly privileged programs. This means that if access to these ports is compromised, the intruder can get access to the whole system. Intruders find open ports via port scans. The two examples below from G-Lock Software illustrate how a port scan can be made [1]:

- *TCP connect( ) scanning* is the most basic form of TCP scanning. An attacker's host is directed to issue a connect( ) system call to a list of selected ports on the target machine. If any of these ports is listening, connect( ) system call will succeed; otherwise, the port is unreachable and the service is unavailable.

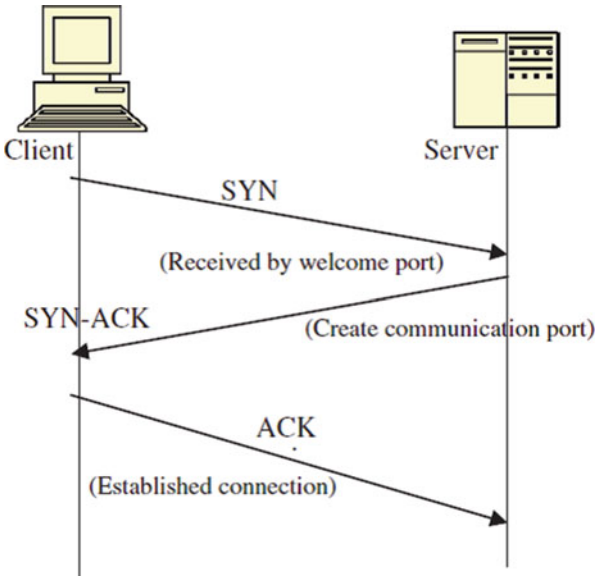

Fig. 3.1 A three-way handshake

- *UDP Internet Control Message Protocol (ICMP) port unreachable scanning* is one of the few UDP scans. Recall from Chap. 1 that UDP is a connectionless protocol; so, it is harder to scan than TCP because UDP ports are not required to respond to probes. Most implementations generate an ICMP port_unreachable error when an intruder sends a packet to a closed UDP port. When this response does not come, the intruder has found an active port.

In addition to port number weaknesses usually identifiable via port scans, both TCP and UDP protocols suffer from other weaknesses.

Packet transmissions between network elements can be intercepted and their contents altered such as in *initial sequence number attack*. Sequence numbers are integer numbers assigned to each transmitted packet, indicating their order of arrival at the receiving element. Upon receipt of the packets, the receiving element acknowledges it in a two-way communication session during which both the transmitting elements talk to each other simultaneously in full duplex.

In the initial sequence number attack, the attacker intercepts the communication session between two or more communicating elements and then guesses the next sequence number in a communication session. The intruder then slips the spoofed IP addresses into the packets transmitted to the server. The server sends an acknowledgment to the spoofed clients. Infrastructure vulnerability attacks also include session attacks, packet sniffing, buffer overflow, and session hijacking. These attacks are discussed in later chapters.

The infrastructure attacks we have discussed so far are of the penetration type where the intruder physically enters the system infrastructure, either at the transmitting element or in the transmitting channel levels, and alters the content of

packets. In the next set of infrastructure attacks, a different approach of vulnerability exploitation is used. This is the distributed denial of services (DDoS).

The DDoS attacks are attacks that are generally classified as nuisance attacks in the sense that they simply interrupt the services of the system. System interruption can be as serious as destroying a computer's hard disk or as simple as using up all the available memory of the system. DDoS attacks come in many forms, but the most common are the following: smurfing, ICMP protocol, and ping of death attacks.

The "smurf" attack utilizes the broken down trust relationship created by IP spoofing. An offending element sends a large amount of spoofed ping packets containing the victim's IP address as the source address. Ping traffic, also called Protocol Overview Internet Control Message Protocol (ICMP) in the Internet community, is used to report out-of-band messages related to network operation or mis-operation such as a host or entire portion of the network being unreachable, owing to some type of failure. The pings are then directed to a large number of network subnets, a subnet being a small independent network such as a LAN. If all the subnets reply to the victim address, the victim element receives a high rate of requests from the spoofed addresses as a result, and the element begins buffering these packets. When the requests come at a rate exceeding the capacity of the queue, the element generates ICMP source quench messages meant to slow down the sending rate. These messages are then sent, supposedly, to the legitimate sender of the requests. If the sender is legitimate, it will heed the requests and slow down the rate of packet transmission. However, in cases of spoofed addresses, no action is taken because all sender addresses are bogus. The situation in the network can easily deteriorate further if each routing device itself takes part in smurfing.

We have outlined a small part of a list of several hundred types of known infrastructure vulnerabilities that are often used by hackers to either penetrate systems and destroy, alter, or introduce foreign data into the system or disable the system through port scanning and DDoS. Although for these known vulnerabilities, equipment manufacturers and software producers have done a considerable job of issuing patches as soon as a loophole or a vulnerability is known, quite often, as was demonstrated in the Code Red fiasco, not all network administrators adhere to the advisories issued to them.

Furthermore, new vulnerabilities are being discovered almost everyday either by hackers in an attempt to show their skills by exposing these vulnerabilities or by users of new hardware or software such as what happened with the Microsoft Windows IIS in the case of the Code Red worm. Also, the fact that most of these exploits use known vulnerabilities is indicative of our abilities in patching known vulnerabilities even if the solutions are provided.

3.2.3 Rapid Growth of Cyberspace

There is always a security problem in numbers. Since its beginning as ARPANET in the early 1960s, the Internet has experienced phenomenal growth, especially in

the last 10 years. There was an explosion in the numbers of users, which in turn ignited an explosion in the number of connected computers.

Just less than 20 years ago in 1985, the Internet had fewer than 2000 computers connected, and the corresponding number of users was in the mere tens of thousands. However, by 2001, the figure has jumped to about 109 million hosts, according to Tony Rutkowski at the Center for Next Generation Internet, an Internet Software Consortium. This number represents a significant new benchmark for the number of Internet hosts. At a reported current annual growth rate of 51% over the past 2 years, this shows continued strong exponential growth, with an estimated growth of up to 1 billion hosts if the same growth rate is sustained [2].

This is a tremendous growth by all accounts. As it grew, it brought in more and more users with varying ethical standards, added more services, and created more responsibilities. By the turn of the century, many countries found their national critical infrastructures firmly intertwined in the global network. An interdependence between humans and computers and between nations on the global network has been created that has led to a critical need to protect the massive amount of information stored on these network computers. The ease of use of and access to the Internet and large quantities of personal, business, and military data stored on the Internet was slowly turning into a massive security threat not only to individuals and business interests but also to national defenses.

As more and more people enjoyed the potential of the Internet, more and more people with dubious motives were also drawn to the Internet because of its enormous wealth of everything they were looking for. Such individuals have posed a potential risk to the information content of the Internet, and such a security threat has to be dealt with.

Statistics from the security company Symantec show that Internet attack activity is currently growing by about 64% per year. The same statistics show that during the first 6 months of 2002, companies connected to the Internet were attacked, on average, 32 times per week compared to only 25 times per week in the last 6 months of 2001. Symantec reports between 400 and 500 new viruses every month and about 250 vulnerabilities in computer programs [3].

In fact, the rate at which the Internet is growing is becoming the greatest security threat ever. Security experts are locked in a deadly race with these malicious hackers that at the moment looks like a losing battle with the security community.

3.2.4 The Growth of the Hacker Community

Although other factors contributed significantly to the security threat, in the general public view, the number one contributor to the security threat of computer and telecommunication networks more than anything else is the growth of the hacker community. Hackers have managed to bring this threat into news headlines and people's living rooms through the ever-increasing and sometimes devastating attacks on computer and telecommunication systems using viruses, worms, DDoS, and other security attacks.

Table 3.1 Global hacker groups

0–9	**I**	**R**
The 414s	*Impact Team*	Red Hacker Alliance
A	Infonomicon	Redhack
AnonCoders	IPhone Dev Team	**S**
Anontune	Iranian Cyber Army	Securax
Anonymous (group)	Islamic State Hacking Division	Sofacy Group
Antisec Movement	Israeli Elite Force	Syrian Electronic Army
APT29	**L**	**T**
B	L0pht	Team Elite
*B*acktrace Security	Lazarus Group	TeaMp0isoN
C	Legion of Doom (hacking)	TeslaTeam
Chaos Computer Club	Level Seven (hacking group)	TESO (Austrian hacker group)
Croatian Revolution Hackers	Lizard Squad	The Shadow Brokers
Cult of the Dead Cow	LulzSec	The Shmoo Group
Cyber-collection	LulzRaft	The Unknowns
CyberBerkut	**M**	Titan Rain
Cyberwarfare in China	MalSec	**U**
D	Masters of Deception	UGNazi
Dark0de	Mazafaka (hacker group)	UXu
Decocidio	Milw0rm	**W**
Derp (hacker group)	Moonlight Maze	W00w00
Digital DawgPound	**N**	World of Hell
F	Network Crack Program Hacker (NCPH) Group	**X**
FinnSec Security	NullCrew	Xbox Underground
G	**O**	XDedic
Gay Nigger Association of America	Operation High Roller	**Y**
Genocide2600	Operation Sundevil	Yemen Cyber Army
Ghost Security	OurMine	
Global kOS	**P**	
GlobalHell	P.H.I.R.M.	
Goatse Security	Pakbugs	
H	Pangu Team	
HacDC	Phone Losers of America	
Hack Canada	Plover-NET	
HackBB	Port7Alliance	
Hacker Bible	Power Racing Series	
Hacker Dojo		
HackerspaceSG		
Hacktivismo		
Hackweiser		

(continued)

Table 3.1 (continued)

Harford Hackerspace		
Helith		
Hell (forum)		
Honker Union		
HubCityLabs		

Reference source: http://en.wikipedia.org/wiki/Category:Hacker_groups. Last modified on 2 June 2016, at 22:14

Until recently most hacker communities worked underground forming groups global like some in Table 3.1. Today, hackers are no longer considered as bad to computer networks as it used to be, and now hackers are being used by governments and organization to do the opposite of what they were supposed to be doing, defending national critical networks and hardening company networks. Increasingly, hacker groups and individuals are being used in clandestine campaigns of attacking other nations. So hacker groups and individuals are no longer as much under the cloud of suspicion as causing mayhem to computer networks, and many are now in the open. In fact hacker Web sites like www.hacker.org with messages like "The hacker explores the intersection of art and science in an insatiable quest to understand and shape the world around him. We guide you on this journey." are legitimately popping up everywhere.

However, for long, the general public, computer users, policy makers, parents, and law makers have watched in bewilderment and awe as the threat to their individual and national security has grown to alarming levels as the size of the global networks have grown and national critical infrastructures have become more and more integrated into this global network. In some cases, the fear from these attacks reached hysterical proportions, as demonstrated in the following major attacks that we have rightly called the big "bungs."

3.2.4.1 The Big "Bungs"

The Internet Worm

On November 2, 1988, Robert T. Morris, Jr., a computer science graduate student at Cornell University, using a computer at MIT, released what he thought was a benign experimental, self-replicating, and self-propagating program on the MIT computer network. Unfortunately, he did not debug the program well before running it. He soon realized his mistake when the program he thought was benign went out of control. The program started replicating itself and at the same time infecting more computers on the network at a faster rate than he had anticipated. There was a bug in his program. The program attacked many machines at MIT and very quickly went beyond the campus to infect other computers around the country. Unable to stop his own program from spreading, he sought a friend's help. He and his friend tried unsuccessfully to send an anonymous message from Harvard over

the network, instructing programmers how to kill the program—now a worm—and prevent its reinfection of other computers. The worm spread like wildfire to infect some 6000 networked computers, a whopping number in proportion to the 1988 size of the Internet, clogging government and university systems. In about 12 h, programmers in affected locations around the country succeeded in stopping the worm from spreading further. It was reported that Morris took advantage of a hole in the debug mode of the Unix *sendmail* program. Unix then was a popular operating system that was running thousands of computers on university campuses around the country. Sendmail runs on Unix to handle e-mail delivery.

Morris was apprehended a few days later; taken to court; sentenced to 3 years, probation, a $10,000 fine, and 400 h of community service; and dismissed from Cornell. Morris's worm came to be known as the Internet worm. The estimated cost of the Internet worm varies from $53,000 to as high as $96 million, although the exact figure will never be known [4].

Michelangelo Virus

The world first heard of the Michelangelo virus in 1991. The virus affected only PCs running MS-DOS 2.xx and higher versions. Although it overwhelmingly affected PCs running DOS, it also affected PCs running other operating systems such as Unix, OS/2, and Novell. It affected computers by infecting floppy disk boot sectors and hard disk master boot records. Once in the boot sectors of the bootable disk, the virus then installed itself in memory from where it would infect the partition table of any other disk on the computer, whether a floppy or a hard disk.

For several years, a rumor was rife, more so many believe, as a scare tactic by antivirus software manufactures that the virus is to be triggered on March 6 of every year to commemorate the birth date of the famous Italian painter. But in real terms, the actual impact of the virus was rare. However, because of the widespread publicity it received, the Michelangelo virus became one of the most disastrous viruses ever, with damages into millions of dollars.

Pathogen, Queeg, and Smeg Viruses

Between 1993 and April 1994, Christopher Pile, a 26-year-old resident of Devon in Britain, commonly known as the "Black Baron" in the hacker community, wrote three computer viruses, *Pathogen*, *Queeg*, and *Smeg*, all named after expressions used in the British sci-fi comedy "Red Dwarf." He used *Smeg* to camouflage both *Pathogen* and *Queeg*. The camouflage of the two programs prevented most known antivirus software from detecting the viruses. Pile wrote the *Smeg* in such a way that others could also write their own viruses and use *Smeg* to camouflage them. This meant that the *Smeg* could be used as a locomotive engine to spread all sorts of viruses. Because of this, Pile's viruses were extremely deadly at that time. Pile used a variety of ways to distribute his deadly software, usually through bulletin boards and freely downloadable Internet software used by thousands in cyberspace.

Pile was arrested on May 26, 1995. He was charged with 11 counts that included the creation and release of these viruses that caused modification and destruction of

computer data and inciting others to create computer viruses. He pleaded guilty to 10 of the 11 counts and was sentenced to 18 months in prison.

Pile's case was in fact not the first one as far as creating and distributing computer viruses was concerned. In October 1992, three Cornell University students were each sentenced to several hundred hours of community service for creating and disseminating a computer virus. However, Pile's case was significant in that it was the first widely covered and published computer crime case that ended in a jail sentence [5].

Melissa Virus

On March 26, 1999, the global network of computers was greeted with a new virus named Melissa. Melissa was created by David Smith, a 29-year-old New Jersey computer programmer. It was later learned that he named the virus after a Florida stripper.

The Melissa virus was released from an "alt.sex" newsgroup using the America OnLine (AOL) account of Scott Steinmetz, whose username was "skyroket." However, Steinmetz, the owner of the AOL account who lived in the western US state of Washington, denied any knowledge of the virus, let alone knowing anybody else using his account. It looked like Smith hacked his account to disguise his tracks.

The virus, which spreads via a combination of Microsoft's Outlook and Word programs, takes advantage of Word documents to act as surrogates and the users' e-mail address book entries to propagate it. The virus then mailed itself to each entry in the address book in either the original Word document named "list.doc" or in a future Word document carrying it after the infection. It was estimated that Melissa affected more than 100,000 e-mail users and caused $80 million in damages during its rampage.

The Y2K Bug

From 1997 to December 31, 1999, the world was gripped by apprehension over one of the greatest myths and misnomers in the history. This was never a bug, a software bug as we know it, but a myth shrouded in the following story. Decades ago, because of memory storage restrictions and expanse of time, computer designers and programmers together made a business decision. They decided to represent the date field by two digits such as "89" and "93" instead of the usual four digits such as "1956." The purpose was noble, but the price was humongous.

The bug, therefore, is: On New Year's Eve of 1999, when world clocks were supposed to change over from 31/12/99 to 01/01/00 at 12:00 midnight, many computers, especially the older ones, were supposed not to know which year it was since it would be represented by "00." Many, of course, believed that computers would then assume anything from year "0000" to "1900," and this would be catastrophic.

Because the people who knew much were unconvinced about the bug, it was known by numerous names to suit the believer. Among the names were:

millennium bug, Y2K computer bug, Y2K, Y2K problem, Y2K crisis, Y2K bug, and many others.

The good news is that the year 2000 came and went with very few incidents of one of the most feared computer bug of our time.

The Goodtimes E-mail Virus

Yet another virus hoax, the *Goodtimes virus*, was humorous, but it ended up being a chain e-mail annoying everyone in its path because of the huge amount of "e-mail virus alerts" it generated. Its humor is embedded in the following prose: Goodtimes will re-write your hard drive. Not only that, but it will also scramble any disks that are even close to your computer. It will recalibrate your refrigerator's coolness setting so all your ice cream melts. It will demagnetize the strips on all your credit cards, make a mess of the tracking on your television, and use subspace field harmonics to scratch any CD you try to play.

It will give your ex-girlfriend your new phone number. It will mix Kool-Aid into your fish tank. It will drink all your beer and leave its socks out on the coffee table when company is coming over. It will put a dead kitten in the back pocket of your good suit pants and hide your car keys when you are running late for work.

Goodtimes will make you fall in love with a penguin. It will give you nightmares about circus midgets. It will pour sugar in your gas tank and shave off both your eyebrows while dating your current girlfriend behind your back and billing the dinner and hotel room to your Visa card.

It will seduce your grandmother. It does not matter if she is dead. Such is the power of Goodtimes; it reaches out beyond the grave to sully those things we hold most dear.

It moves your car randomly around parking lots so you can't find it. It will kick your dog. It will leave libidinous messages on your boss's voice mail in your voice! It is insidious and subtle. It is dangerous and terrifying to behold. It is also a rather interesting shade of mauve.

Goodtimes will give you Dutch Elm disease. It will leave the toilet seat up. It will make a batch of methamphetamine in your bathtub and then leave bacon cooking on the stove while it goes out to chase gradeschoolers with your new snowblower.

Distributed Denial of Service (DDoS)

February 7, 2000, a month after the Y2K bug scare and Goodtimes hoax, the world woke up to the real thing. This was not a hoax or a myth. On this day, a 16-year-old Canadian hacker nicknamed "Mafiaboy" launched his distributed denial-of-service (DDoS) attack. Using the Internet's infrastructure weaknesses and tools, he unleashed a barrage of remotely coordinated blitz of GB/s IP packet requests from selected, sometimes unsuspecting, victim servers which, in a coordinated fashion, bombarded and flooded and eventually overcame and knocked out Yahoo servers for a period of about 3 h. Within 2 days, while technicians at Yahoo and law enforcement agencies were struggling to identify the source of the

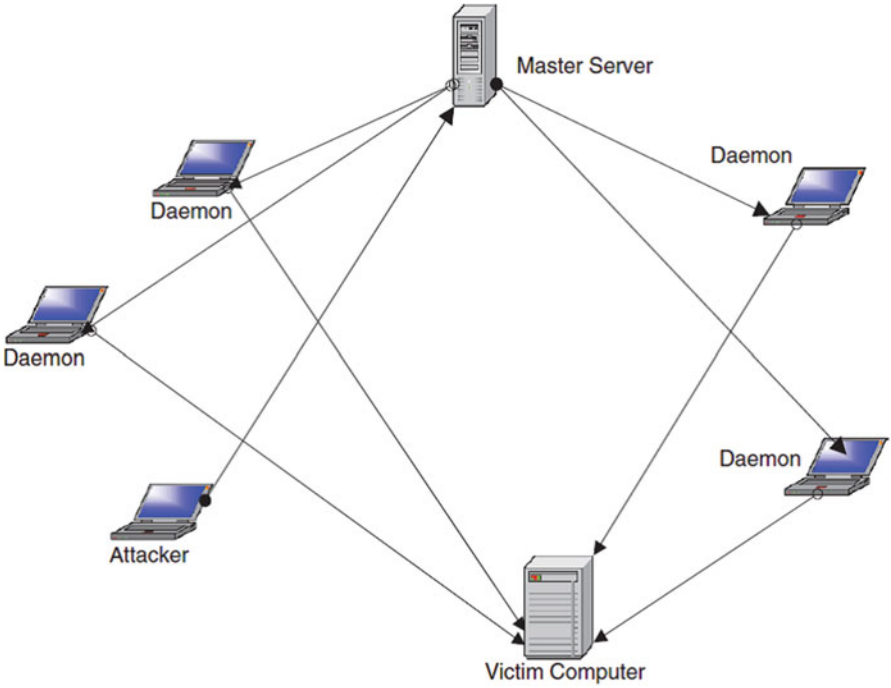

Fig. 3.2 The working of a DDOS attack

attacker, on February 9, 2000, Mafiaboy struck again, this time bombarding servers at eBay, Amazon, Buy.com, ZDNet, CNN, E*Trade, and MSN.

The DDoS attack employs a network consisting of a master computer responsible for directing the attacks, the "innocent" computers commonly known as "daemons" used by the master as intermediaries in the attack, and the victim computer—a selected computer to be attacked. Figure 3.2 shows how this works.

After the network has been selected, the hacker instructs the master node to further instruct each daemon in its network to send several authentication requests to the selected network nodes, filling up their request buffers. All requests have false return addresses; so, the victim nodes can't find the user when they try to send back the authentication approval. As the nodes wait for acknowledgments, sometimes even before they close the connections, they are again and again bombarded with more requests. When the rate of requests exceeds the speed at which the victim node can take requests, the nodes are overwhelmed and brought down.

The primary objective of a DDoS attack are multifaceted, including flooding a network to prevent legitimate network traffic from going through the network, disrupting network connections to prevent access to services between network nodes, preventing a particular individual network node from accessing either all network services or specified network services, and disrupting network services to either a specific part of the network or selected victim machines on the network.

The Canadian judge stated that although the act was done by an adolescent, the motivation of the attack was undeniable and had a criminal intent. He, therefore, sentenced the Mafiaboy, whose real name was withheld because he was under age, to serve 8 months in a youth detention center and 1 year of probation after his release from the detention center. He was also ordered to donate $250 to charity.

Love Bug Virus

On April 28, 2000, Onel de Guzman, a dropout from AMA computer college in Manila, Philippines, released a computer virus onto the global computer network. The virus was first uploaded to the global networks via a popular Internet Relay Chat program using Impact, an Internet ISP. It was then uploaded to Sky Internet's servers, another ISP in Manila, and it quickly spread to global networks, first in Asia and then Europe. In Asia, it hit a number of companies hard, including the Dow Jones Newswire and the *Asian Wall Street Journal*. In Europe, it left thousands of victims that included big companies and parliaments. In Denmark, it hit TV2 channel and the Danish parliament, and in Britain, the House of Commons fell victim too. Within 12 h of release, it was on the North American continent, where the US Senate computer system was among the victims [6].

It spread via Microsoft Outlook e-mail systems as surrogates. It used a rather sinister approach by tricking the user to open an e-mail presumably from someone the user knew (because the e-mail usually came from an address book of someone the user knew). The e-mail, as seen in Fig. 3.3, requests the user to check the attached "Love Letter." The attachment file was in fact a Visual Basic Script, which contained the virus payload. The virus then became harmful when the user opened the attachment. Once the file was opened, the virus copied itself to two critical system directories and then added triggers to the Windows registry to ensure that it ran every time the computer was rebooted. The virus then replicated itself, destroying system files including Web development such as ".js" and ".css" and multimedia files such as JPEG and MP3, searched for log-in names and passwords in the user's address book, and then mailed itself again [6].

de Guzman was tracked down within hours of the release of the virus. Security officials, using a caller ID of the phone number and ISP used by de Guzman, were led to an apartment in the poor part of Manila where de Guzman lived.

The virus devastated global computer networks, and it was estimated that it caused losses ranging between $7 billion and $20 billion [7].

Palm Virus

In August 2000, the actual palm virus was released under the name of Liberty Trojan horse, the first known malicious program targeting the Palm OS. The Liberty Trojan horse duped some people into downloading a program that erased data.

Another palm virus shortly followed Palm Liberty. On September 21, 2000, McAfee.com and F-Secure, two of the big antivirus companies, first discovered a really destructive palm virus they called Palm OS/Phage. When Palm OS/Phage is executed, the screen is filled with a dark gray box, and the application is terminated. The virus then replicates itself to other Palm OS applications.

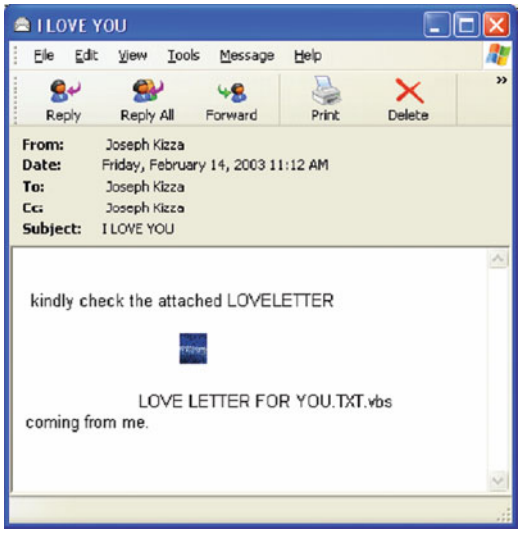

Fig. 3.3 The love bug monitor display

Wireless device viruses have not been widespread, thanks to the fact that the majority of Palm OS users do not download programs directly from the Web but via their desktop and then sync to their palm. Because of this, they have virus protection available to them at either their ISP's Internet gateway, at the desktop, or at their corporation.

The appearance of a Palm virus in cyberspace raises many concerns about the security of cyberspace because PDAs are difficult to check for viruses as they are not hooked up to a main corporate network. PDAs are moving as users move, making virus tracking and scanning difficult.

Anna Kournikova Virus

On February 12, 2001, global computer networks were hit again by a new virus, Anna Kournikova, named after the Russian tennis star. The virus was released by 20-year-old Dutchman Jan de Wit, commonly known in the hacker underworld community as "OnTheFly." The virus, like the I LOVE YOU virus before it, was a mass-mailing type. Written in Visual Basic scripting language, the virus spreads by mailing itself, disguised as a JPEG file named *Anna Kournikova*, through Microsoft Windows, Outlook, and other e-mail programs on the Internet.

The subject line of mail containing the virus bears the following: "Here ya have,;0)," "Here you are ;-)," or "here you go ;-)." Once opened, Visual Basic Script copies itself to a Windows directory as "AnnaKournikova.jpg.vbs." It then mails itself to all entries in the user's Microsoft Outlook e-mail address book. Figure 3.4 shows the Anna Kournikova monitor screen display.

Spreading at twice the speed of the notorious "I LOVE YOU" bug, Anna quickly circumvented the globe.

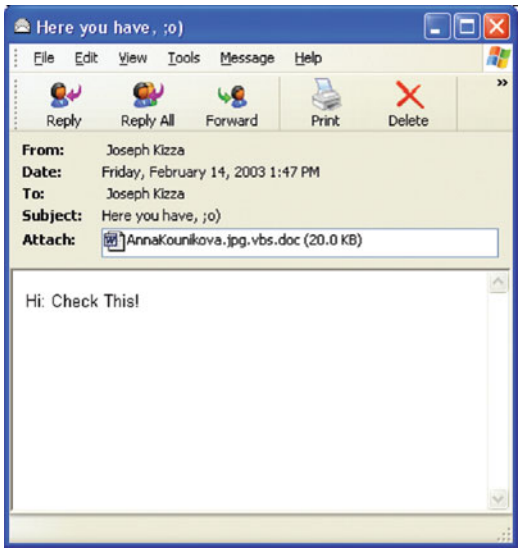

Fig. 3.4 Anna Kournikova monitor display

Security experts believe Anna was of the type commonly referred to as a "virus creation kit," "a do-it-yourself program kit" that potentially makes everyone able to create a malicious code.

Code Red: "For One Moment Last Week, the Internet Stood Still."[1]

The Code Red worm was first released on July 12, 2001, from Foshan University in China, and it was detected the next day July 13 by senior security engineer Ken Eichman. However, when detected, it was not taken seriously until 4 days later when engineers at eEye Digital cracked the worm code and named it "Code Red" after staying awake with "Code Red"—labeled Mountain Dew [8]. By this time, the worm had started to spread, though slowly. Then on July 19, according to Rob Lemos, it is believed that someone modified the worm, fixing a problem with its random-number generator. The new worm started to spread like wildfire spreading, leaping from 15,000 infections that morning to almost 350,000 infections by 5 p.m. PDT [8].

The worm was able to infect computers because it used a security hole, discovered the month before, in computers using Microsoft's Internet Information Server (IIS) in the Windows NT4 and Windows 2000 Index Services. The hole, known as the Index Server ISAPI vulnerability, allowed the intruder to take control of a security vulnerability in these systems, resulting in one of several outcomes, including Web site defacement and installation of denial-of-service tools. The following Web defacement "*HELLO! Welcome to* http://www.worm.com*! Hacked By Chinese!*" usually resulted. The Web defacement was done by the worm

[1]Lemos, Rob. "Code Red: Virulent worm calls into doubt our ability to protect the Net," CNET News.com, July 27, 2001.

connecting to TCP port 80 on a randomly chosen host. If the connection was successful, the attacking host sent a crafted HTTP GET request to the victim, attempting to exploit a buffer overflow in the Indexing Service [9].

Because Code Red was self-propagating, the victim computer would then send the same exploit (HTTP GET request) to another set of randomly chosen hosts.

Although Microsoft issued a patch when the security hole was discovered, not many servers were patched before Code Red hit. Because of the large number of IIS servers on the Internet, Code Red found the going easy, and at its peak, it hit up to 300,000 servers. But Code Red did not do as much damage as feared; because of its own design flaw, the worm was quickly brought under control.

SQL Worm

On Saturday, January 25, 2003, the global communication network was hit by the SQL worm. The worm, which some refer to as the "SQL Slammer," spreads to computers that are running Microsoft SQL Server with a blank SQL administrator password. Once in the system, it copies files to the infected computer and changes the SQL administrator password to a string of four random characters.

The vulnerability exploited by the slammer warm preexisted in the Microsoft SQL Server 2000 and in fact was discovered 6 months prior to the attack. When the vulnerability was discovered, Microsoft offered a free patch to fix the problem; however, the word never got around to all users of the server software.

The worm spread rapidly in networks across Asia, Europe, and the United States and Canada, shutting down businesses and government systems. However, its effects were not very serious because of its own weaknesses that included its inability to affect secure servers and its ease of detection.

Hackers View 8 Million Visa/MasterCard, Discover, and American Express Accounts

On Monday, February 17, 2003, the two major credit card companies Visa and MasterCard reported a major infiltration into a third-party payment card processor by a hacker who gained access to more than 5 million Visa and MasterCard accounts throughout the United States. Card information exposed included card numbers and personal information that included social security numbers and credit limits.

The flood of the hacker victims increased by two on Tuesday, February 18, 2003, when both Discover Financial Services and American Express reported that they were also victims of the same hacker who breached the security system of a company that processes transactions on behalf of merchants.

While MasterCard and Visa had earlier reported that around 2.2 million and 3.4 million of their own cards were respectively affected, Discover Financial Services and American Express would not disclose how many accounts were involved. It is estimated, however, that the number of affected accounts in the security breach was as high as 8 million.

3.2.5 Vulnerability in Operating System Protocol

One area that offers the greatest security threat to global computer systems is the area of software errors, especially network operating systems errors. An operating system plays a vital role not only in the smooth running of the computer system in controlling and providing vital services, but by playing a crucial role in the security of the system in providing access to vital system resources. A vulnerable operating system can allow an attacker to take over a computer system and do anything that any authorized super user can do, such as changing files, installing and running software, or reformatting the hard drive.

Every OS comes with some security vulnerabilities. In fact many security vulnerabilities are OS specific. Hacker looks for OS-identifying information like file extensions for exploits.

3.2.6 The Invisible Security Threat: The Insider Effect

Quite often, news media reports show that in cases of violent crimes such as murder, one is more likely to be attacked by someone one does not know. However, real official police and court records show otherwise. This is also the case in network security. Research data from many reputable agencies consistently show that the greatest threat to security in any enterprise is the guy down the hall.

In 1997, the accounting firm Ernst & Young interviewed 4226 IT managers and professionals from around the world about the security of their networks. From the responses, 75% of the managers indicated that they believed authorized users and employees represent a threat to the security of their systems. Forty-two percent of the Ernst and Young respondents reported they had experienced external malicious attacks in the past year, while 43% reported malicious acts from employees [10].

The inside threat to organizational security comes from one of its own, the untrustworthy member of the organization. This "insider threat" is a person possibly who has privileged access to classified, sensitive, or propriety data and who uses this unique opportunity to remove information from the organization and transfer to unauthorized outsider users.

According to Jack Strauss, president and CEO of SafeCorp, a professional information security consultancy in Dayton, Ohio, company insiders intentionally or accidentally misusing information pose the greatest information security threat to today's Internet-centric businesses. Strauss believes that it is a mistake for company security chiefs to neglect to lock the backdoor to the building, to encrypt sensitive data on their laptops, or not to revoke access privileges when employees leave the company [11].

3.2.7 Social Engineering

Besides the security threat from the insiders themselves who knowingly and willingly are part of the security threat, the insider effect can also involve insiders unknowingly being part of the security threat through the power of *social engineering*. Social engineering consists of an array of methods an intruder such as a hacker, both from within or outside the organization, can use to gain system authorization through masquerading as an authorized user of the network. Social engineering can be carried out using a variety of methods, including physically impersonating an individual known to have access to the system, online, and telephone and even by writing. The infamous hacker Kevin Mitnick used social engineering extensively to break into some of the nation's most secure networks with a combination of his incredible solid computer hacking and social engineering skills to coax information, such as passwords, out of people.

3.2.8 Physical Theft

As the demand for information by businesses to stay competitive and nations to remain strong heats up, laptop computer and PDA theft is on the rise. There is a whole list of incidents involving laptop computer theft such as the reported disappearance of a laptop used to log incidents of covert nuclear proliferation from a sixth-floor room in the headquarters of the US State Department in January, 2000. In March of the same year, a British accountant working for the MI5, a British national spy agency, had his laptop computer snatched from between his legs while waiting for a train at London's Paddington Station. In December 1999, someone stole a laptop from the car of Bono, lead singer for the megaband U2; it contained months of crucial work on song lyrics. And according to the computer-insurance firm Safeware, some 319,000 laptops were stolen in 1999, at a total cost of more than $800 million for the hardware alone [12]. Thousands of company executive laptops and PDA disappear every year with years of company secrets.

3.3 Security Threat Motives

Although we have seen that security threats can originate from natural disasters and unintentional human activities, the bulk of cyberspace threats and then attacks originate from humans caused by illegal or criminal acts from either insiders or outsiders, recreational hackers, and criminals. The FBI's foreign counterintelligence mission has broadly categorized security threats based on terrorism; military espionage; economic espionage, targeting the National Information Infrastructure; vendetta and revenge; and hate [13].

3.3.1 Terrorism

Our increasing dependence on computers and computer communication has opened up the can of worms, we now know as electronic terrorism. Electronic terrorism is used to attack military installations, banking, and many other targets of interest based on politics, religion, and probably hate. Those who are using this new brand of terrorism are a new breed of hackers, who no longer hold the view of cracking systems as an intellectual exercise but as a way of gaining from the action. The "new" hacker is a cracker who knows and is aware of the value of information that he/she is trying to obtain or compromise. But cyberterrorism is not only about obtaining information; it is also about instilling fear and doubt and compromising the integrity of the data.

Some of these hackers have a mission, usually foreign power-sponsored or foreign power-coordinated that, according to the FBI, may result in violent acts, dangerous to human life, that are a violation of the criminal laws of the targeted nation or organization and are intended to intimidate or coerce people so as to influence the policy.

3.3.2 Military Espionage

For generations, countries have been competing for supremacy of one form or another. During the Cold War, countries competed for military spheres. After it ended, the espionage turf changed from military aim to gaining access to highly classified commercial information that would not only let them know what other countries are doing but also might give them either a military or commercial advantage without them spending a great deal of money on the effort. It is not surprising, therefore, that the spread of the Internet has given a boost and a new lease on life to a dying Cold War profession. Our high dependency on computers in the national military and commercial establishments has given espionage a new fertile ground. Electronic espionage has many advantages over its old-fashion, trench-coated, sun-glassed, and gloved Hitchcock-style cousin. For example, it is less expensive to implement; it can gain access into places that would be inaccessible to human spies; it saves embarrassment in case of failed or botched attempts; and it can be carried out at a place and time of choice.

3.3.3 Economic Espionage

The end of the Cold War was supposed to bring to an end-spirited and intensive military espionage. However, in the wake of the end of the Cold War, the United States, as a leading military, economic, and information superpower, found itself a constant target of another kind of espionage, economic espionage. In its pure form, economic espionage targets economic trade secrets which, according to the 1996 US Economic Espionage Act, are defined as all forms and types of financial,

business, scientific, technical, economic, or engineering information and all types of intellectual property including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, and/or codes, whether tangible or not, stored or not, and compiled or not [14]. To enforce this act and prevent computer attacks targeting American commercial interests, US Federal Law authorizes law enforcement agencies to use wiretaps and other surveillance means to curb computer-supported information espionage.

3.3.4 Targeting the National Information Infrastructure

The threat may be foreign power sponsored or foreign power coordinated, directed at a target country, corporation, establishments, or persons. It may target specific facilities, personnel, information, or computer, cable, satellite, or telecommunication systems that are associated with the National Information Infrastructure.

Activities may include the following [15]:

- Denial or disruption of computer, cable, satellite, or telecommunication services
- Unauthorized monitoring of computer, cable, satellite, or telecommunication systems
- Unauthorized disclosure of proprietary or classified information stored within or communicated through computer, cable, satellite, or telecommunication systems
- Unauthorized modification or destruction of computer programming codes, computer network databases, stored information, or computer capabilities
- Manipulation of computer, cable, satellite, or telecommunication services resulting in fraud, financial loss, or other federal criminal violations

3.3.5 Vendetta/Revenge

There are many causes that lead to vendettas. The demonstrations at the last World Trade Organization (WTO) in Seattle, Washington, and subsequent demonstrations at the meetings in Washington, D.C., of both the World Bank and the International Monetary Fund are indicative of the growing discontent of the masses who are unhappy with big business, multinationals, big governments, and a million others. This discontent is driving a new breed of wild, rebellious, young people to hit back at systems that they see as not solving world problems and benefiting all of mankind. These mass computer attacks are increasingly being used as paybacks for what the attacker or attackers consider to be injustices done that need to be avenged. However, most vendetta attacks are for mundane reasons such as a promotion denied, a boyfriend or girlfriend taken, an ex-spouse given child custody, and other situations that may involve family and intimacy issues.

3.3.6 Hate (National Origin, Gender, and Race)

Hate as a motive of security threat originates from and is always based on an individual or individuals with a serious dislike of another person or group of persons based on a string of human attributes that may include national origin, gender, race, or mundane ones such as the manner of speech one uses. Then incensed, by one or all of these attributes, the attackers contemplate and threaten and sometimes carry out attacks of vengeance often rooted in ignorance.

3.3.7 Notoriety

Many, especially young, hackers try to break into a system to prove their competence and sometimes to show off to their friends that they are intelligent or superhuman in order to gain respect among their peers.

3.3.8 Greed

Many intruders into company systems do so to gain financially from their acts.

3.3.9 Ignorance

This takes many forms but quite often it happens when a novice in computer security stumbles on an exploit or vulnerability and without knowing or understanding it uses it to attack other systems.

3.4 Security Threat Management

Security threat management is a technique used to monitor an organization's critical security systems in real time to review reports from the monitoring sensors such as the intrusion detection systems, firewall, and other scanning sensors. These reviews help to reduce false positives from the sensors, develop quick response techniques for threat containment and assessment, correlate and escalate false positives across multiple sensors or platforms, and develop intuitive analytical, forensic, and management reports.

As the workplace gets more electronic and critical company information finds its way out of the manila envelopes and brown folders into online electronic databases, security management has become a full-time job for system administrators. While the number of dubious users is on the rise, the number of reported criminal incidents is skyrocketing, and the reported response time between a threat and a real attack is down to 20 min or less [15]. To secure company resources, security managers have

to do real-time management. Real-time management requires access to real-time data from all network sensors.

Among the techniques used for security threat management are risk assessment and forensic analysis.

3.4.1 Risk Assessment

Even if there are several security threats all targeting the same resource, each threat will cause a different risk, and each will need a different risk assessment. Some will have low risk, while others will have the opposite. It is important for the response team to study the risks as sensor data come in and decide which threat to deal with first.

3.4.2 Forensic Analysis

Forensic analysis is done after a threat has been identified and contained. After containment, the response team can launch the forensic analysis tools to interact with the dynamic report displays that have come from the sensors during the duration of the threat or attack if the threat results in an attack. The data on which forensic analysis should be performed must be kept in a secure state to preserve the evidence. It must be stored and transferred, if this is needed, with the greatest care, and the analysis must be done with the utmost professionalism possible if the results of the forensic analysis are to stand in court.

3.5 Security Threat Correlation

As we have noted in the previous section, the interval time between the first occurrence of the threat and the start of the real attack has now been reduced about 20 min. This is putting enormous pressure on organizations' security teams to correspondingly reduce *the turnaround time,* the time between the start of an incident and the receipt of the first reports of the incident from the sensors. The shorter the turnaround time, the quicker the response to an incident in progress. In fact, if the incident is caught at an early start, an organization can be saved a great deal of damage.

Threat correlation, therefore, is the technique designed to reduce the turnaround time by monitoring all network sensor data and then use that data to quickly analyze and discriminate between real threats and false positives. In fact, threat correlation helps in:

- Reducing false positives because if we get the sensor data early enough, analyze it, and detect false positives, we can quickly re-tune the sensors so that future false positives are reduced.

- Reducing false negatives; similarly by getting early sensor reports, we can analyze it, study where false negatives are coming from, and re-tune the sensors to reveal more details.
- Verifying sensor performance and availability; by getting early reports, we can quickly check on all sensors to make sure that they are performing as needed.

3.5.1 Threat Information Quality

The quality of data coming from the sensor logs depends on several factors including:

- Collection—When data is collected, it must be analyzed. The collection techniques specify where the data is to be analyzed. To reduce on bandwidth and data compression problems, before data is transported to a central location for analysis, some analysis is usually done at the sensor, and then reports are brought to the central location. But this kind of distributed computation may not work well in all cases.
- Consolidation—Given that the goal of correlation is to pull data out of the sensors, analyze it, correlate it, and deliver timely and accurate reports to the response teams and also given the amount of data generated by the sensors and further the limitation to bandwidth, it is important to find good techniques to filter out relevant data and consolidate sensor data either through compression or aggregation so that analysis is done on only real and active threats.
- Correlation—Again given the goals of correlation, if the chosen technique of data collection is to use a central database, then a good data mining scheme must be used for appropriate queries on the database that will result in outputs that will realize the goals of correlation. However, many data mining techniques have problems.

3.6 Security Threat Awareness

Security threat awareness is meant to bring widespread and massive attention of the population to the security threat. Once people come to know of the threat, it is hoped that they will become more careful, more alert, and more responsible in what they do. They will also be more likely to follow security guidelines.

Exercises

1. Although we discussed several sources of security threats, we did not exhaust all. There are many such sources. Name and discuss five.
2. We pointed out that the design philosophy of the Internet infrastructure was partly to blame for the weaknesses and hence a source of security threats. Do

you think a different philosophy would have been better? Comment on your answer.
3. Give a detailed account of why the three-way handshake is a security threat.
4. In the chapter, we gave two examples of how a port scan can be a threat to security. Give three more examples of port scans that can lead to system security compromise.
5. Comment on the rapid growth of the Internet as a contributing factor to the security threat of cyberspace. What is the responsible factor in this growth? Is it people or the number of computers?
6. There seems to have been an increase in the number of reported virus and worm attacks on computer networks. Is this really a sign of an increase, more reporting, or more security awareness on the part of the individual? Comment on each of these factors.
7. Social engineering has been frequently cited as a source of network security threat. Discuss the different elements within social engineering that contribute to this assertion.
8. In the chapter, we gave just a few of the many motives for security threat. Discuss five more, giving details of why there are motives.
9. Outline and discuss the factors that influence threat information quality.
10. Discuss the role of data mining techniques in the quality of threat information.

Advanced Exercises

1. Research the effects of industrial espionage, and write a detailed account of a profile of a person who sells and buys industrial secrets. What type of industrial secrets is likely to be traded?
2. The main reasons behind the development of the National Strategy to Secure Cyberspace were the realization that we are increasingly dependent on the computer networks, the major components of the national critical infrastructure are dependent on computer networks, and our enemies have the capabilities to disrupt and affect any of the infrastructure components at will. Study the National Information Infrastructure and the weaknesses inherent in the system, and suggest ways to harden it.
3. Study and suggest the best ways to defend the national critical infrastructure from potential attackers.
4. We indicated in the text that the best ways to manage security threats is to do an extensive risk assessment and more forensic analysis. Discuss how reducing the turnaround time can assist you in both risk assessment and forensic analysis. What are the inputs into the forensic analysis model? What forensic tools are you likely to use? How do you suggest to deal with the evidence?
5. Do research on intrusion detection and firewall sensor false positives and false negatives. Write an executive report on the best ways to deal with both of these unwanted reports.

References

1. G-Lock Software TCP and UDP port scanning examples. http://www.glocksoft.com/tcpudpscan.htm
2. Rutkowski T Internet survey reaches 109 million host level. Center for next generation internet. http://www.ngi.org/trends/TrendsPR0102.txt
3. Battling the Net Security Threat, Saturday, 9 November, 2002, 08:15 GMT, http://news.bbc.co.uk/2/hi/technology/2386113.stm
4. Derived in part from a letter by Severo M. Ornstein. Commun ACM, June 1989 32(6)
5. Virus Writer Christopher Pile (Black Barron) Sent to Jail for 18 Months Wednesday 15 November 1995. http://www.gps.jussieu.fr/comp/VirusWriter.html
6. Hopper I Destructive 'I LOVE YOU' Computer virus strikes worldwide. CNN Interactive Technology. http://www.cnn.com/2000/TECH/computing/05/04/iloveyou/.
7. Former student: bug may have been spread accidentally. CNN Interactive. http:/www.cnn.com/2000/ASIANOWsoutheast/05/11/iloveyou.02/
8. National Security Threat List. http://rf-web.tamu.edu/security/SECGUIDE/T1threat/Nstl.htm
9. CERT® Advisory CA-2001–19 'Code Red' worm exploiting buffer overflow in IIS indexing service DLL. http://www.cert.org/advisories/CA-2001–19.html
10. Is IT safe? InfoTrac. Tennessee electronic library. HP Professional 1997, 1(12):14–20
11. Insider abuse of information is biggest security threat, SafeCop says. InfoTrac. Tennessee electronic library. Business Wire. November 10, 2000, p. 1
12. Hollows P Security threat correlation: the next battlefield. eSecurityPlanetcom. http://www.esecurityplanet.com/views/article.php/10752_1501001
13. Awareness of National Security Issues and Response [ANSIR]. FBI's Intelligence Resource Program. http://www.fas.org/irp/ops/ci/ansir.htm
14. Grosso A (2000) The economic espionage ACT: touring the minefields. Commun ACM 43 (8):15–18
15. ThreatManager ™ – the real-time security threat management suite. http://www.open.com/responsenetworks/products/threatmanager/threatmanager.htm?ISR1