Interested in learning more about security?

SANS Institute InfoSec Reading Room

The Cyber Security Management System: A Conceptual Mapping

In an environment of global connection and cyber terrorism, the protection of information assets is vital to every private business, public organization and individual household. This paper looks at the cyber security management process as a complex system of interrelated elements and demonstrates the use of concept mapping techniques to expand our knowledge of the system as a whole, and of policy and technology in particular.

THE CYBER SECURITY MANAGEMENT SYSTEM: A CONCEPTUAL MAPPING

John H. Dexter

A paper submitted in partial fulfillment of
The requirements for GIAC Security
Essentials Certification, version 1.3

Global Information Assurance Certification

The SANS Institute

February 2002

The SANS Institute

Abstract

THE CYBER SECURITY MANAGEMENT SYSTEM: A CONCEPTUAL MAPPING

John H. Dexter

In an environment of global connection and cyber terrorism, the protection of information assets is vital to every private business, public organization and individual household. This paper looks at the cyber security management process as a complex system of interrelated elements and demonstrates the use of concept mapping techniques to expand our knowledge of the system as a whole, and of policy and technology in particular.

TABLE OF CONTENTS

List of Figures....ii
Introduction....1
Hacker Means....1
    Social Engineering....1
    Scanners....1
    Password Cracking....2
    IP Spoofing....2
    Trojan Horses....2
The Cyber Security Management System....3
Policy....4
    Password Management....4
    Anti-Virus....5
    Incident Handling....5
    Backup and Recovery....5
    Proprietary Information....5
Technology....6
    Perimeter Defense....7
        Firewalls....8
        Intrusion Detection Systems....9
        Virtual Private Networks....10
    Encryption....10
Summary....12
References....13

LIST OF FIGURES

Number *Page*

1. Cyber Security Management System Concept Map 3
2. Information Assets Concept Map 7
3. Protected Network 8
4. Perimeter Defense Concept Map 9
5. Cryptography Concept Map 11

Introduction

The topic of computer security is a prominent one in the world today. Nearly every day we read or hear terms like "hacker", "computer virus", "Internet worm" etc. Never before has the globe felt so small. The tentacles of cyberspace reach into our homes and offices by way of the Internet, opening up the farthest reaches of the world to us, to our business partners and our children. At the same time, this waxing connectedness leaves us vulnerable to intruders because the computers, software and networks we use have weaknesses that are easily exploitable. We become preoccupied with protecting information because we stand to lose a great deal.

While most hackers delight in benign intrusion, some can truly be characterized as cyber criminals. These are the ones whose actions can result in lost revenue, lost opportunity, ill will and incident handling expenses for the victimized company. These are the creators of malicious code that could steal an individual's identity or destroy cherished family records on a home computer. It is not our purpose here to speculate on the motivation of these intrusive individuals, or to analyze their character. Instead, we will focus on what they do and how they do it in hopes of developing a system to effectively counteract their nefarious deeds.

Hacker Means

Many hackers are mere copycats – not very innovative. They'll access any of a number of hacker websites to download malicious code (malware) developed by someone else, even if the majority of the world's systems are already inoculated against that particular attack. However, some hackers are very creative individuals who will use sophisticated techniques to create a virus, a worm or denial of service (DoS) attack, including:

Social Engineering

One way that a hacker can gain illicit access to a system is through "social engineering". Social engineering is a term used to describe deception against other humans. A hacker may devise a scheme to trick another person into providing a username and password. This is often accomplished by preying on the unsuspecting individual's willingness to help or by taking advantage of a trusting relationship. Social engineering is as simple and effective as pretending to leave the room while another is signing onto a computer, all the while peaking around the corner to get a glimpse of logon keystrokes. Social engineering does not always take place face-to-face. Clever hackers have been known to place phone calls pretending to be a corporate help desk person or other legitimate partner asking for information that could compromise access to computing resources. Imagine how many workstations are left wide open in a building when a fire alarm goes off. How long would it take for the alarm puller to drop a floppy into your desktop computer, initiate a process and be gone?

Scanners

There are numerous tools for hackers to use from afar that provide them valuable information about weaknesses in networks and systems. One category of intrusion tool is known as the scanner, or sniffer. Many operating systems come with vulnerability scanners that assist administrators in finding weaknesses. Public domain and commercial products are readily available, including SARA, Nessus,

Toneloc, PhoneSweep and Nmap. These scanners can reveal service ports that are open for attack and even details about the operating system itself. We should not be naïve enough to think that these are out of the reach of the bad guys. In addition, hackers know how to use phone scanners and war dialers to find a system on the Internet that has a modem with auto-answer capability – a juicy target!

Password Cracking

Usually plain text passwords are not exposed on systems, but their encrypted equivalents often are. Password cracking entails creating plain text passwords from their cryptographic hashes. Once the plain text password is garnered, access can be had. Password cracking tools are made available to system administrators for auditing and recovery reasons. Crack is popular for Unix systems and LC3 for NT systems. Hackers use these tools too. They'll first identify a valid userid (an easy thing to do on most systems) and then apply the system encryption scheme against an associated string of encrypted characters to reveal a clear text password.

Password cracking is accomplished using one or more of a handful of methods. A "dictionary" approach involves checking the unencrypted result against a dictionary of words. A "hybrid" algorithm extends the dictionary approach by adding numbers and special characters to the mix. Sometimes a "rule-based" method is used when the perpetrator knows something about the organization's password policy, perhaps learned through social engineering. For example, if the policy is that each password must contain at least one capital letter and at least one numeric and must be no less than six characters, this knowledge can be programmed into the rule-based cracking paradigm[1]. A "brute force" method is often used when the hacker knows nothing about the password. In this case, all alphanumeric and special characters are included in a mass substitution scheme that addresses various length passwords.

IP Spoofing

IP spoofing is a technique used by hackers as a means to gain hidden, unauthorized access to a target resource. They do this by impersonating a trusted resource. Specifically, a DoS attack may change address information in the IP header of a message to make the target resource think the message is coming from a recognized, friendly port. When this technique is deployed in high volume, the attack can effectively dominate the target machine's resources, causing the target machine to perform sluggishly, or stop processing altogether.

Trojan Horses

Infamous hacker Dan Edwards coined the term "Trojan horse" to connote " a malicious, security-breaking program that is disguised as something benign…[2]" For years, hackers have exploited security deficiencies in languages like Java/Active X and Visual Basic to plant destructive processes within seemingly harmless objects like screen savers or even text files. The most common distribution

[1] Semjanov, Pavel, "Password Cracking FAQ", 2001 http://www.password-crackers.com/pwdcrackfaq.html#I

[2] Dumbill, Edd, "Jargon Lexicon", AmigaGuide,1994 http://star.informatik.rwth-aachen.de/jargon300/Trojanhorse.html

method used for Trojan horses is to attach them to e-mail messages. The "Love Bug" affliction in May of 2000 was a Trojan horse.

In addition to password cracking, social engineering, IP spoofing and Trojan horse techniques, hackers have many other ways to perform destructive acts in the cyber realm. They have ways to hijack legitimate sessions, intercept and re-assemble IP fragments, take advantage of buffer overflows or flood a target machine with SYN requests. It is the wide and diverse nature of vulnerability today that argues for a strong cyber security management system, one that begins with comprehensive policy and applies many technologies to achieve defense in depth.

The Cyber Security Management System

The cyber security management process is a known "system" of interrelated elements that act in concert with one another to achieve the over-arching goal of the system itself -- to protect the confidentiality, integrity and availability of information. Figure 1 shows a conceptual map that organizes and represents knowledge of many of these system elements. While not all of the elements of the map will be discussed in this paper, primary attention is given to policy and technology. Driven by policy, the cyber security management process applies technology and requires effective planning in order to achieve the goal.

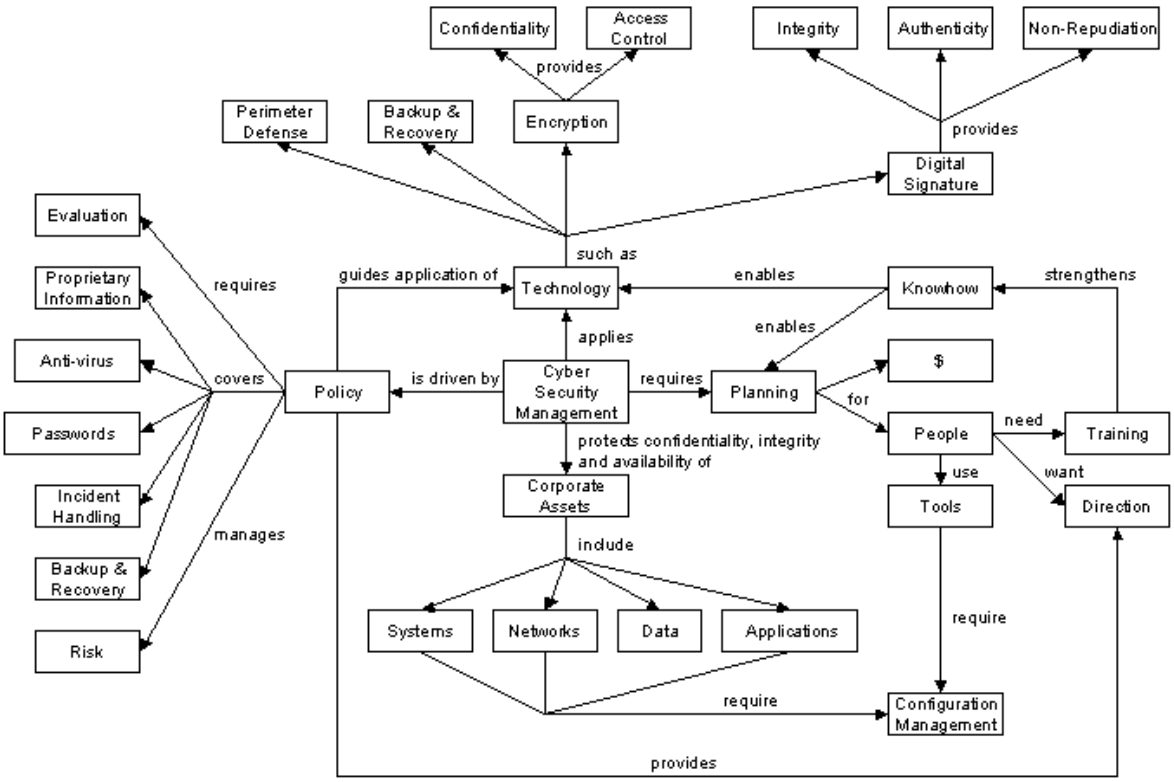

Figure 1

Policy

Despite commendable advances in protection, detection and response within the computer security industry, the risk of cyber attack is still high today. Computer Emergency Response Team (CERT®) statistics show that in the first three quarters of 2001 alone nearly 35,000 incidents and almost 2,000 vulnerabilities were reported[3]. It seems as though our information assets face a building storm of clever attacks from villainous hackers.

Policy is what can provide a beacon in this storm of cyber risk and help an organization put in place multi-level, in-depth defenses. Sound policy is a core element of the cyber security management system (see Figure 1). Without it, extensive implementations of routers, firewalls and intrusion detection systems are misguided. Indeed, policy steers the application of technology within this system.

Two important analysis efforts are required before a cyber security policy can be determined. The first of these involves a rigorous inventory of the organization's information assets. The nature of all networks, servers, desktop workstations and data should be well understood and documented before policy is set forth. It is important also to analyze how the organization's information assets are used by its employees, partners and stakeholders. Such inputs render an information security policy legitimate.

According to security policy experts Carol Kramer of the SANS Institute and Stephen Northcutt at the Global Incident Analysis Center, it is important that a cyber information protection policy cover the areas of password management, anti-virus solutions, incident handling, data backups and the protection of proprietary information[4].

Password Management

Passwords are a first line of defense when it comes to controlling access to protected systems and information. It is important to know the idiosyncrasies and limitations of account administration when it comes to your operating systems, database servers and applications. The following should be researched and analyzed thoroughly before establishing policy in a formal way:

- Procedures for protecting password files and administrator accounts
- Random password generation, one-time passwords and two-factor authentication
- Length of a password's life
- Password expiration and renewal
- Procedures for cleansing ex-employee access
- Length and qualities of acceptable passwords

[3] "CERT/CC Statistics: 1988-2001", Carnegie Mellon Software Engineering Institute, CERT Coordination Center www.cert.org/stats/cert_stats.html

[4] Kramer, Carol, Northcutt, Stephen and Kerby, Fred editors, "Basic Security Policy: Version 1.6- May 8, 2001", SANS GIAC, 2001

Anti-Virus

An effective cyber security management policy considers where vulnerabilities exist for an organization's resources before formalizing processes and procedures. This is especially true for exposures to the outside, i.e. Internet, community. Once weaknesses are identified, the policy will specify both commercial and internally developed solutions to prevent the introduction of malicious code on the company's perimeter defense systems, servers and desktops, how deployment is to unfold, and who is responsible for deployment.

It is not enough, however, to merely understand the weaknesses and adopted solutions. It is important also to analyze what will transpire once a virus is detected, and the sequence of measures to be taken during the handling of an incident. All employees should feel responsible for reporting evidence of an intrusion or attack. An effective, formal anti-virus policy clearly states the simple steps required to report an incident.

Incident Handling

Policy should cover the very practical steps that an organization needs to take when a cyber security incident occurs. Documented incident handling tasks are aimed first at securing information assets – minimizing damage -- as quickly as possible. Beyond providing immediate, on-the-scene protection, written incident-handling tasks will strengthen organizational learning and may assist the cyber security professional in the pursuit and prosecution of criminals. It is always a good idea to practice incident handling and continually update procedures so that when these are needed in live situations they will be proven and reliable.

Backup and Recovery

With so much having been written and so many nightmares having been documented in the information age regarding the loss of valuable corporate data, it is perplexing that some outfits still do not have a formal policy for creating and recovering from backups. Policy needs to emphasize the fundamental importance of backup and recovery processes for desktops, file servers and mainframes. Again, responsibilities should be clearly documented. Batch processing and storage capacity planning need to be integral parts of the operational planning process. A plan for disaster recovery from offsite backups should be considered. In addition to adequately protecting backup media in limited-access facilities, enlightened organizations will recover from backups in simulated environments as a matter of practice, with an eye toward perfecting the procedures.

Proprietary Information

Every organization has sensitive information that it does not want exposed to certain others – product designs, promotional plans, human resource strategies, financial forecasts, staff medical records etc. Cyber security management policy should reinforce a company's formal information classifications and specify the rules, guidelines and procedures for the protection of each. It should be clear to employees what are the consequences of not adequately following these. Proprietary information needs to be

regularly audited in terms of how it is handled, who has access to it, and the level at which it is protected.

Incorporating the areas of password management, anti-virus, backups and proprietary information protection into an organization's cyber security policy can help to establish some common best practices. Newmediary Inc. provides a succinct list of best practices in the publication entitled "Security for Today's Enterprise". Included in the list are the following sensible guidelines:

- Disable default accounts and change their passwords;
- Close vulnerable services and unnecessary ports;
- Assure strong backup procedures;
- Secure system files;
- Use computer security professionals and consortia;
- Simplify the policy for practical application[5].

Valuable policy is always written down in clear, concise, realistic and specific language. As a fundamental element of the cyber security management process, policy also requires ongoing evaluation to ensure that it keeps pace with changes in the global information environment, and with changes in the organization itself. Again, policy supports the goal of protecting the confidentiality, integrity and availability of an organization's valuable information.

Technology

A number of technologies are available today that, when selected and applied as coordinated elements within the cyber security management system, can offer insurance against unauthorized access, data loss and DoS attacks, such as those depicted in Figure 2 below. A few of these technologies are depicted in Figure 1 above – perimeter defense, backup and recovery, encryption and digital signature. It is important, however, to understand that technology alone does little to achieve the cyber security management system's objectives. Rather, it is the synergistic interplay of technology, policy and planning that maximizes the protection of information assets.

[5] "Security for Today's Enterprise", Newmediary Inc., 2001 http://www.techguide.com/html/security.pdf

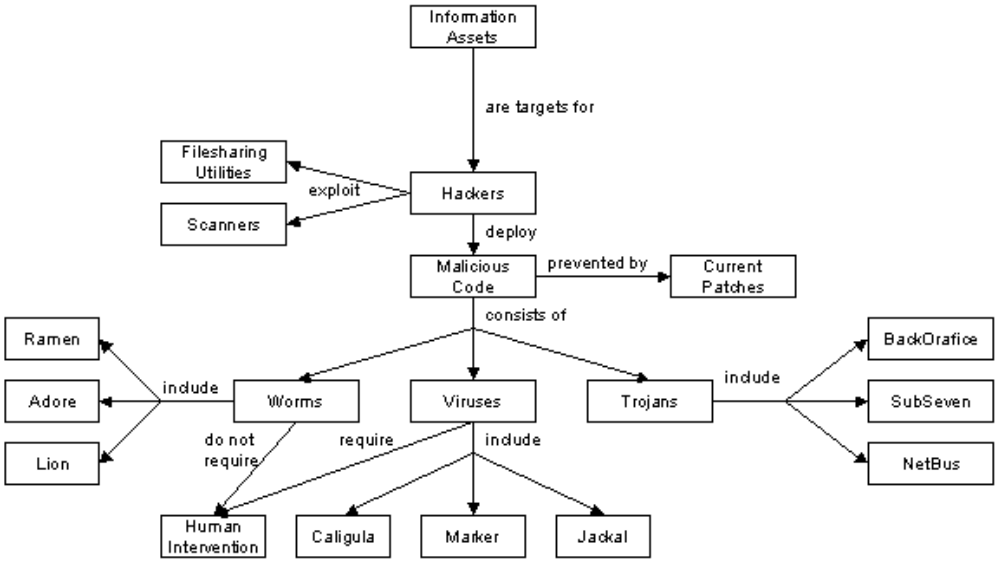

Figure 2

Perimeter Defense

Perimeter defense mechanisms guard against and detect unauthorized access to information resources. They appear at the bounds of the asset being protected, whether the resource is a network, a host system tied to a network, or merely a standalone machine. These solutions include routers, firewalls, virtual private networks (VPN) and intrusion detection systems (IDS). Their application comes in the form of hardware, software, or a combination of the two. Also, it is possible for a solution provider to combine these technologies, e.g. some routers include firewall capabilities.

Perimeter defense solutions make use of standards-based technologies such as the popular Internet Protocol Security (IPSec). IPSec is the standard for authentication, encryption and tunneling on the Internet. It ensures the integrity of IP packets flowing across local area networks (LANs) using "transport" mode and wide area networks (WANs) using "tunnel" mode[6]. Because there is little need within the confines of a LAN to hide address information, transport mode protects only the packet "payload" – the part of the packet that contains sensitive userid, password and business data. On the other hand, in order to provide secure packet exchange across a public WAN where addresses are vulnerable to outsiders, IPSec applies tunnel mode to hide both the packet's address information and the payload. Tunnel mode is generally slower than transport mode because of this added overhead. Figure 3 below shows two perimeter defense deployments at the bounds of a protected network -- a

[6] Ryan, Jerry, "How to Build Secure LANs with IPSec", Applied Technologies Group Inc., 2001 http://www.techguide.com/html/ipsec.pdf

VPN and a corporate firewall. Within the protected network, host-based IDS implementations could also be directly tied to the servers.

Firewalls

A firewall is a device that blocks Internet communications access to a private resource. The private resource can be a network, a server or a personal computer. A firewall allows unfettered outbound packets from, say, a protected network to the Internet world, but allows only appropriate inbound packets. Firewalls are popular and effective, but can be subverted if the protected resource has a modem configured for auto-answer.

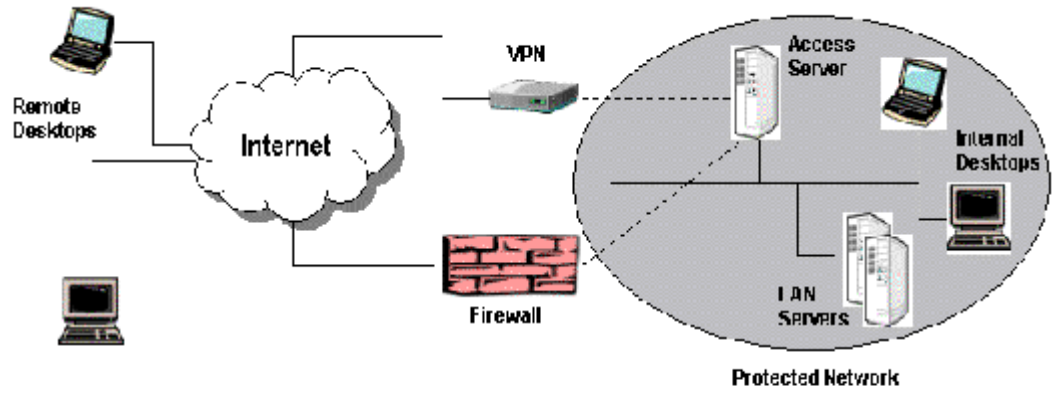

Figure 3

There are two types of firewalls – protocol-level firewalls and application-level firewalls (see the concept map represented by Figure 4 below). Packet filtering firewalls use a packet's header to determine whether the incoming packet is allowable. This approach to traffic management is fast and simple, but less secure because it provides no means of determining whether or not the packet header has been spoofed. Dynamic packet filtering firewalls offer improved protection against spoofing by changing the outbound packet header information on the fly upon exit from the private resource. "Stateful" inspection firewalls offer an intelligence-based approach that compares the activity on a port to what is considered normal for that port. Stateful inspection overhead, however, has an adverse impact on performance.

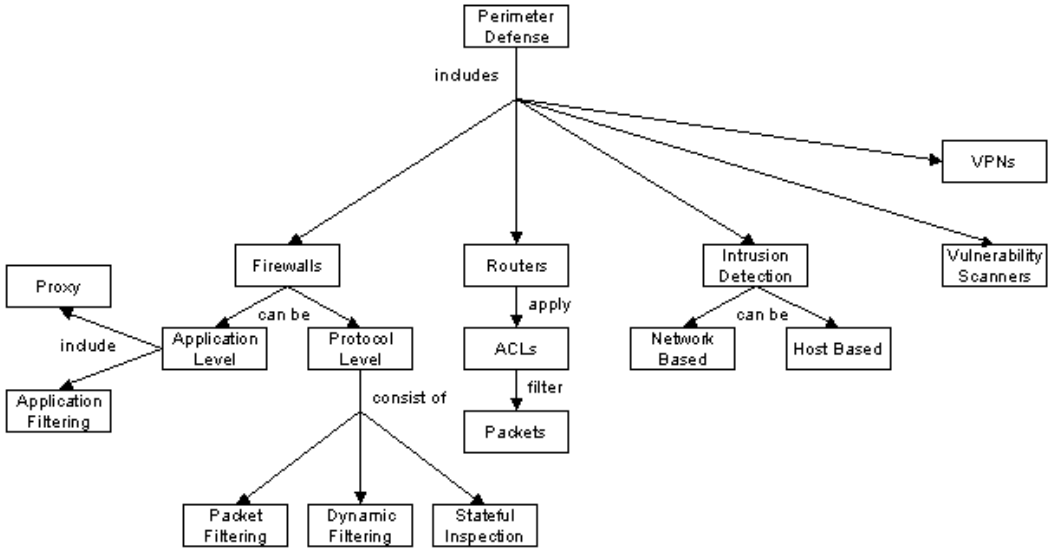

Figure 4

Application-level firewalls are slower still. However, they offer high levels of protection because they understand in depth what the application expects and how it performs communication. Proxies are a very effective type of application-level firewall. Under a proxy configuration, the user of an application inside a protected network never communicates directly with the outside world, rather only with the application's proxy. The proxy then communicates on behalf of the insider to the outside resource, and vice-versa. In some ways, today's proxy servers can be compared to the Pony Express riders of the untamed West who carried messages back and forth from outpost to outpost!

Intrusion Detection Systems

Another way to fortify perimeter defense is to install an IDS, especially on core systems like e-mail, web and domain name servers. Intrusion detection systems supplement firewall technology with strong monitoring and record keeping at both the network and host levels. IDS technologies monitor network traffic and system logs to compare what's going on in real-time to the known methods of hackers. When a suspicious event is detected, an alarm is kicked off immediately. Often the IDS will take action to suspend or drop the offending connection, all the while recording as much information as it can to assist the system administrator in later identification and apprehension. It takes a skilled administrator, however, to configure IDS such that normal activity does not trigger an alarm, i.e. to avoid "false positives".

IDS solutions, though an integral component of multi-level protection, can be resource intensive. It takes a large measure of resources to intercept packets, analyze them against known profiles of malicious code, and either deflect or pass on the results. This can be problematic when IDS processes are bundled with firewalls or routers. Today, the concept of providing high-powered security

"appliances" addresses this performance issue. The idea is to enable a hardware-based solution for very speedy analysis and disposition of incoming packets to a protected network flowing in high traffic[7]. Through the use of application specific integrated circuit (ASIC) technology, security appliances hold the promise of, perhaps, gigabit speed intrusion detection.

Appliance capability will fortify defenses against today's DoS attacks, e.g. Ping Floods and SYN Floods and even distributed DoS (DDoS) attacks like Tribe Floods and Stacheldraht. However, hackers have shown firm resolve to break new defenses when the bar is raised. This fact argues for creativity and continual improvement of a multi-level defense system to meet the goal of protecting an organization's information assets.

Virtual Private Networks

VPNs provide a secure, dynamic tunnel capability that allows users to make use of both the Internet and a protected LAN simultaneously without the worry of exposing sensitive information to cyber criminals. Using IPSec's tunnel mode, VPNs encrypt the source and destination addresses of a packet so that these are not exposed to Internet hackers as clear text but are still usable for routing purposes. This is accomplished through a mechanism called ecapsulation. Encapsulation is a method whereby the IPSec tunnel capability encrypts the sensitive IP Header and wraps a protective outer header around it. A VPN also provides encryption of the packet's user data payload. Typically, today's solutions apply the Data Encryption Standard (DES) algorithm or extended 3DES scheme to maximize the length of keys used to scramble and unscramble data, although newer standards are emerging, e.g. Advanced Encryption Standard (AES). AES specifies key lengths of 128-bits, 192-bits and 256-bits[8].

Encryption

Encryption is a technique for transforming text into something visually meaningless and is a fundamental cyber security management system technology. Objects of encryption include those pieces of information that, if compromised, could result in adverse effects on an organization's valued information assets – userids, passwords, business data, names and addresses of servers and workstations, etc. In-depth, multi-level cyber security management applies encryption together with other technologies like perimeter defense solutions, backup and recovery, and digital signature, as indicated in the Figure 1 concept map. Indeed, encryption is often built into perimeter defense mechanisms like firewalls and VPNs.

Encryption is what results from applied cryptographic algorithms. A clear overview of cryptographic algorithms is presented in industry analyst Tom Austin's book titled PKI: A Wiley Tech Brief. There are two types of cryptographic algorithms – symmetric algorithms and asymmetric algorithms (see the

[7] "Stopping Attacks: The Importance of Denial of Service (DoS) Security Appliances", Newmediary Inc., 2002 http://www.techguide.com/html/netsec.pdf

[8] "ADVANCED ENCRYPTION STANDARDS (AES): Questions and Answers", http://csrc.nist.gov/encryption/aes/aesfact.html

Figure 5 concept map below). The latter of these is practically synonymous with the conception of Public Key Infrastructure (PKI). Both support the notion of keys that are used as input to the algorithm to create scrambled cipher text from plain (clear) text or to create plain text from cipher text. When all other factors are equal, key length is an important factor in determining the strength of an algorithm because the longer the key, the longer it will take a hacker to decipher (and thereby use) the key illicitly[9].

Symmetric systems are based on the sharing of one secret key between two persons across a secure channel. One problem with this approach is that, with enough time and computing power, hackers can bust the shared key. Another problem is that the management and distribution of symmetric keys is costly. DES uses 56-bit, symmetric keys and encrypts data by the 8-byte block[10]. Kerberos is an example of a symmetric key system that strengthens DES with a trusted Key Distribution Center (KDC) to manage the secret keys between sites and between the KDC and client sites.

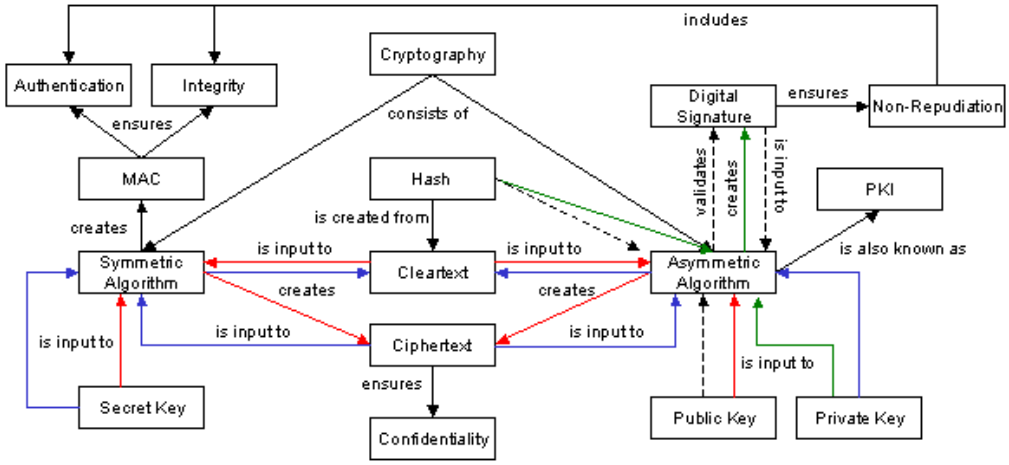

Figure 5

Asymmetric key encryption systems operate on the notion that two, mathematically related keys are better than one. The underlying asymmetric algorithms are founded in extremely difficult mathematical problems, with key lengths long enough to support combinations in the many trillions! One example of an extremely complex mathematical problem used in asymmetric cryptography is the RSA algorithm. RSA is based on factoring very large integers into prime factors. Other cryptosystems are based on solving the discrete logarithm problem, e.g. elliptic curve systems.

[9] Austin, Tom, PKI: A Wiley Tech Brief, New York, NY, USA, Wiley Computer Publishing, John Wiley & Sons, Inc., 2001, pp. 46-48

[10] Ryan, Jerry, "Designing and Implementing a Virtual Private Network (VPN)", Applied Technologies Group Inc., 1999 http://www.techguide.com/html/vpnet.pdf

Under a symmetric key setup, if Bob and Alice want to exchange a message, each of them must know the secret key. Asymmetric key management systems allow Bob and Alice to have their own private keys that nobody else knows about. In addition, both Bob and Alice have a public key that they share with each other, and anyone else. Alice and Bob can use each other's public key to encrypt a message that is decipherable by the other using the other's private key. Likewise, the two can use the other's public key to decrypt a message that the other had encrypted with their own private key.

Figure 5 shows the encryption and decryption processes in red and blue, respectively. Aside from the algorithms themselves, the substantive difference between symmetric encryption/decryption and asymmetric encryption/decryption is inherent in the number and nature of keys used. Regardless, the result guarantees confidentiality through the use of cipher text. However, the objectives of authenticity and integrity are achieved differently by the two approaches. The symmetric approach is to create a Message Authentication Code (MAC) for such purposes, while the asymmetric approach is to create a digital signature.

MACs are generated at the sending location when plain text is input to a symmetric algorithm. The plain text message and its associated MAC are then sent to a recipient who, having the same symmetric algorithm as the sender, creates another MAC of the plain text and compares it with the MAC sent. If the two MACs are identical, the message received has integrity, i.e. it has not been altered. Conversely, asymmetric algorithms use the concept of digital signature to ensure authenticity and integrity. The creation and verification processes for digital signature are shown in Figure 5 using green and dashed arrows, respectively. Asymmetric systems also provide a good, though not perfect, measure of non-repudiation, i.e. insurance against denial on the part of Alice or Bob that they "signed" the message.

Summary

The goal of a cyber security management system is to protect the confidentiality, integrity and availability of information assets. Two relevant cyber security management system technology categories have been described here – perimeter defense and encryption. These concepts and solutions are interrelated and often bundled together in practical application. Again, a thoroughly conceived and equivalently rendered cyber security management policy helps to move the application of these technologies forward. The concepts of policy and technology are primary to an effective cyber security management system. They are intertwined with each other as well as with other concepts such as planning and configuration management. All of these concepts must be active in an organization's cyber security management system in order to sustain desired levels of information asset protection.

REFERENCES

Adams, Carlisle and Lloyd, Steve, Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations, Indianapolis, IN, USA, Macmillan Technical Publishing, 1999

Austin, Tom, PKI: A Wiley Tech Brief, New York, NY, USA, Wiley Computer Publishing, John Wiley & Sons, Inc., 2001, pp. 46-48

Dumbill, Edd, "Jargon Lexicon", AmigaGuide, 1994
http://star.informatik.rwth-aachen.de/jargon300/Trojanhorse.html

Kramer, Carol, Northcutt, Stephen and Kerby, Fred editors, "Basic Security Policy: Version 1.6- May 8, 2001", SANS GIAC, 2001

Krawczyk, H. (IBM), Canetti, R. (IBM), Bellare, M. (UC San Diego), "HMAC: Keyed-Hashing for Message Authentication", June 1997 www-cse.ucsd.edu/users/mihir/papers/rfc2104.txt

Lo, Joseph, "Trojan Horse Attacks", 2002 http://www.irchelp.org/irchelp/security/trojan.html

Novak, Joseph D., "The Theory Underlying Concept Maps and How to Construct Them", Cornell University, May 2001 http://cmap.coginst.uwf.edu/info/

Rogaway, Phillip, "PMAC: Background", UC Davis, May 2001
www.cs.ucdavis.edu/~rogaway/ocb/pmac-bak.htm

Ryan, Jerry, "A Practical Guide to the Right VPN Solution", Applied Technologies Group Inc., 2001
http://www.techguide.com/html/vpnsolu.pdf

Ryan, Jerry, "Designing and Implementing a Virtual Private Network (VPN)", Applied Technologies Group Inc., 1999 www.techguide.com/html/vpnet.pdf

Ryan, Jerry, "How to Build Secure LANs with IPSec", Applied Technologies Group Inc., 2001
www.techguide.com/html/ipsec.pdf

Semjanov, Pavel, "Password Cracking FAQ", 2001
http://www.password-crackers.com/pwdcrackfaq.html#I

"ADVANCED ENCRYPTION STANDARDS (AES): Questions and Answers",
http://csrc.nist.gov/encryption/aes/aesfact.html

"CERT/CC Statistics: 1988-2001", Carnegie Mellon Software Engineering Institute, CERT Coordination Center www.cert.org/stats/cert_stats.html

"Implementing a Secure Virtual Private Network", RSA Security Inc., June 2001
http://www.rsasecurity.com/solutions/vpn/whitepapers/ISVPN_WP_0501.pdf

"Security for Today's Enterprise", Newmediary Inc., 2001
http://www.techguide.com/html/security.pdf

"Stopping Attacks: The Importance of Denial of Service (DoS) Security Appliances", Newmediary Inc., 2002 http://www.techguide.com/html/netsec.pdf

Last Updated: October 23rd, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
GridEx IV 2017	Online,	Nov 15, 2017 - Nov 16, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CAUS	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, GB	Nov 27, 2017 - Dec 02, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZUS	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Khobar 2017	Khobar, SA	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TXUS	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, DE	Dec 04, 2017 - Dec 09, 2017	Live Event
European Security Awareness Summit & Training 2017	London, GB	Dec 04, 2017 - Dec 07, 2017	Live Event
SANS Bangalore 2017	Bangalore, IN	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, DE	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS San Diego 2017	OnlineCAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced