Preface

INTRODUCTION

Enterprises today are linking their systems across enterprise-wide networks and VPNs as well as increasing their exposure to customers, competitors, browsers and hackers on the Internet. Each connection magnifies the vulnerability to attack. With the increased connectivity to the Internet and the wide availability of automated cracking tools, enterprises can no longer simply rely on operating system security to protect their valuable corporate data. Furthermore, the exploding use of Web technologies for enterprise intranets and Internet sites has escalated security risks to enterprise data and information systems. It is imperative that Web professionals are trained in techniques to effectively protect their sites from internal and external threats.

PURPOSE

The purpose of this book is to show globally how the Internet is paving the way for secure communications within enterprises and on the public Internet. In addition, the book will provide the fundamental knowledge you need to analyze risks to your system and implement a workable security policy that protects your information assets from potential intrusion, damage or theft. Through dozens of real life scenarios and/or examples, you will learn which countermeasures to deploy to thwart potential attacks. In this book, you will also gain extensive hands-on experience in securing Web communications and Web sites. You will learn the common vulnerabilities of Web sites; as well as, how to carry out secure communications across unsecured networks.

SCOPE

This book will illustrate the importance of Internet security as a method of protection for Internet and intranet based applications. In addition to commercial enterprises and governments, the book will also address, but not be limited to the following line items

as part of extensive hands-on examples that will provide you with practical experience in establishing Internet security:

- Maintaining strong authentication and authenticity.
- Preventing eavesdropping.
- Retaining integrity of information.
- Minimizing the effects of denial-of-service attacks.
- Selecting a firewall topology.
- Evaluating computer and hacker ethics.
- Installing and configuring Microsoft IIS, Netscape iPlanet or Apache.
- Securing your Web browser.
- Auditing and hardening your server operating system.
- Configuring user authentication.
- Implementing host-based access restrictions.
- Using SSL to encrypt Web traffic.
- Creating a certificate authority (CA).
- Implementing a client certificate.
- Configuring your Web server to require client certificates.
- Protecting browsers and servers with a proxy-based firewall.

This book will leave little doubt that a new world infrastructure in the area of Internet security is about to be constructed. No question, it will benefit enterprises and governments, as well as their advanced citizens. For the disadvantaged regions of the world, however, the coming Internet security revolution could be one of those rare technological events that enable traditional societies to leap ahead and long-dormant economies to flourish in security.

TARGET AUDIENCE

This book is primarily targeted toward domestic and international system administrators, government computer security officials, network administrators, senior managers, engineers, sales representatives, marketing staff, WWW Developers, military senior top brass, and other Internet users. This book is valuable for those who require the fundamental skills to develop and implement security policies designed to protect their enterprise's information from attacks, including managers, network and system administrators, technical staff and support personnel. This book is also valuable for those involved in securing Web sites, including Web developers, Webmasters, and systems, network and security administrators. Some experience with Web servers and technologies is required. Basically, the book is targeted for all types of people and organizations around the world that have Internet, extranet, and intranet security concerns. In addition, the targeted audience also includes the following:

- Scientists.
- Engineers.
- Educators.

- Top Level Executives.
- Computer and network security personnel and IT/IS directors.
- Information Technology (IT) and Department Managers.
- Programmers and Technical Staff.
- The massive target market of more than 600 million Internet and intranet users around the world.

ORGANIZATION OF THIS BOOK

The book is organized into fifteen parts as well as an extensive glossary of security, wireless network and Internet networking terms and acronyms at the back. It provides a step-by-step approach to everything you need to know about Internet security. The following detailed organization speaks for itself:

Part I: Introduction To Internet Security

Part One discusses Internet technologies and basic security issues.

Chapter 1, "Internet technologies," discusses securing dynamic content on a Web server. Topics include security considerations that apply to all dynamic content in general, Server Side Includes, Common Gateway Interface, and two ways to wrapper CGI content.

Chapter 2, "Basic Security Issues," is intended to help management successfully navigate a course, by providing an overview of security principles and the technologies which are appropriate for securing the Internet and networks today.

Part II: Establishing Your Organization's Security

Part Two discusses real threats that impact security and the security policy itself, which is the foundation for your protection.

Chapter 3, "Real Threats That Impact Security," discusses, what can you do about all of these real security threats.

Chapter 4, "A Security Policy: The Foundation Of Your Protection," provides technical professionals with the information they need to explain Internet policy issues to policy makers. It provides a construct for linking high-level policy to detailed technical decisions.

Part III: Developing Your Security Policy

The third part of this book discusses the steps you can take now and how to respond to attacks.

Chapter 5, "Steps To Take Now," provides a methodology for the steps you must take now to rapidly develop a risk profile for your enterprise; and, the enterprise requirements you must adhere to in developing an Internet security policy.

Chapter 6, "Responding To Attacks," contains hypothetical sample policy statements that address Internet-based security.

Part IV: Securing The Web Client

Part Four covers threats and vulnerabilities and how to protect your web browser.

Chapter 7, "Threats And Vulnerabilities," presents an overview of these vulnerabilities and threats, and is a marked deviation from the previous Top-20 lists. In addition to Windows and UNIX categories, SANS and NIPC have also included cross-platform applications and networking products.

Chapter 8, "Protecting Your Web Browser," focuses on the security aspects, particularly the risks involved with running any web browser and how to overcome some of these security shortcomings. Internet Explorer and Firefox will be used as examples, as these are the most commonly used, and therefore the most commonly exploited.

Part V: Network Interconnections: A Major Point Of Vulnerability

Part Five covers the basic operating system and TCP/IP concepts; as well as, early system security improvements.

Chapter 9, "Basic Operating System And TCP/IP Concepts," provides you with a much better understanding of the real-world risks of TCP/IP reset attacks. In other words, to better understand the reality of this threat, the aim of this chapter is to provide some background into the basic workings of operating systems and of TCP/IP concepts, and then to build upon this foundation to understand how resets attacks work.

Chapter 10, "Early System Security Improvements," focuses on early system security improvements like DES, shadow passwords and dialback/dialer passwords.

Part VI: Deterring Masqueraders And Ensuring Authenticity

Part six covers the impersonation of users, how masqueraders can iniltrate your system and how to hold your defensive line.

Chapter 11, "Impersonating Users" focuses on the impersonation of users by stolen passwords and the borrowing of IP addresses.

Chapter 12, "How Masqueraders Infiltrate A System," deals with a broad sweep of technologies and issues connected with policing, profiling and privacy as applicable to cyber surveillance and the infiltration of masqueraders.

Chapter 13, "Holding Your Defensive Line," shows you how to thwart blended threats, where a defense-in-depth strategy is the preferred approach. Defense-in-depth relies on the premise that multiple layers of security afford more comprehensive protection than any single mechanism.

Part VII: Preventing Eavesdropping To Protect Your Privacy

Part Seven covers unauthorized listening and looking and the countering or not countering the eavesdropper.

Chapter 14, "Unauthorized Listening And Looking," describes instant messaging and offers a brief overview of some of the security threats associated with the service. It covers the unauthorized listening and looking of IM: Yeah! Eavesdropping!

Chapter 15, “Countering Or Not Countering The Eavesdropper: That’s The Question?,” answers that question, and provides recommendations to counter or provide support for the eavesdropper either way.

Part VIII: Thwarting Counterfeiters And Forgery to Retain Integrity

Part Eight covers the forger’s arsenal and how to shield your asets.

Chapter 16, “The Forger’s Arsenal,” focuses on the forger’s arsenal (hacking e-mail messages; censoring system logs; and, scrambling the routing tables); as well as, the enhancement of the Internet Protocol (IP), called Path Enhanced IP (PEIP), which is designed to eliminate source forgery.

Chapter 17, “Shielding Your Assets,” focuses on how to shield your assets through patch management.

Part IX: Avoiding Disruption Of Service To Maintain Availability

Part Nine covers denial-of-service attacks, how to construct your bastions and the importance of firewalls.

Chapter 18, “Denial-Of-Service Attacks,” provides information and defenses against Denial of Service (DoS) attacks, which cause networked computers to disconnect from the network or just outright crash due to the delivery of viruses and bombs (nukes) via the Internet and data flooding.

Chapter 19, “Constructing Your Bastions,” discusses how to protect your site against the growing community of black-hat hackers, by thinking like they do and seeing the same information.

Chapter 20, “The Importance Of Firewalls,” focuses on the importance of firewalls, how they work and what kinds of threats they can protect you from, how to use a packet filter to shield against bombardment, and how to use application proxies to manage Internet communications.

Part X: Configuring Operating System And Network Security

Part Ten discusses operating systems that pose a security risk and network security.

Chapter 21, “Operating Systems That Pose A Security Risk,” discusses the problem of operating system security and the social and economic implications for risk management and policy.

Chapter 22, “Network Security,” covers network security abuses.

Part XI: Enhancing Web Server Security

Part Eleven discusses how to control access, extend web site security functionality and how to secure web communications with SSL VPNs.

Chapter 23, “Controlling Access,” explores how a comprehensive approach simplifies network access management, creates a secure, intelligent wired and wireless environment

and provides affordable network security that detects all users and enforces all enterprise policies at every access point.

Chapter 24, "Extended Web Site Security Functionality," investigates spoofing and phishing attacks and present countermeasures, with regards to extended web site security functionality, while focusing on solutions that protect naïve as well as expert users.

Chapter 25, "Securing Web Communications With SSL VPNs," examines the security risks that arise from securing web communications with SSL VPNs and proposes strategies for remediation.

Part XII: Issuing And Managing Certificates

Part Twelve discusses why digital certificates are used; as well as, certificate authorities and trusting CAs in servers and browsers.

Chapter 26, "Why Digital Certificates Are Used," takes a look at digital certificates (past, present and future) and their potential for deterring phishing attacks and online fraud. It demonstrates the severe pitfalls from First Generation manual vetting of certificate holders and the inherent unreliability of the identity information they contain (which can easily be faked).

Chapter 27, "Certificate Authorities," discusses the use of CAs to verify that the site is who it claims to be.

Chapter 28, "Trusting Cas In Servers And Browsers," briefly touches on some common shared certificate configurations.

Part XIII: Firewalls And Firewall Topologies

Part Thirteen discusses how to provide protecting servers and clients with firewalls, how to choose the right firewall, firewall topologies and how to select the right firewall security topology policy.

Chapter 29, "Protecting Servers And Clients With Firewalls," presents a brief overview of firewall components, types available, and the relative advantages and disadvantages of each. It is intended to lay out a general road map for administrators who wish to publish information for public consumption with regards to protecting servers and clients, while preventing unauthorized access to their private or confidential network.

Chapter 30, "Choosing The Right Firewall," explores, in depth, the aspects of security and exemplifies several existing solutions.

Chapter 31, "Firewall Topologies," focuses on independent utilities that may be assembled to provide an in depth defense against intrusion, extrusion, and collusion.

Chapter 32, "Selecting Firewall Security Topology Policy," helps the responsible manager and firewall administrator create useful policy for the firewall.

Part XIV: Security Management Solutions And Future Directions

Part Fourteen discusses how to identify and respond to security violations; conduct real-time monitoring and auditing; how to limit damage; keep up to date on new threats and

emerging technologies; and, finally the summary, conclusions, and recommendations for the book.

Chapter 33, "Identifying And Responding To Security Violations," describes Internet security tool technology (as part of Internet security management solutions and future directions); and demonstrates how it can help administrators identify potential problems; as well as, make well-informed security decisions that strengthen the Internet's security posture.

Chapter 34, "Real-Time Monitoring And Auditing," focuses on "theoretical best-practices" combined with "real-world practicality" to define a usable policy for the real-time auditing and monitoring of databases. By following the policies outlined in this chapter, you can properly implement a database system that will work well, and provide adequate security for the data it houses.

Chapter 35, "Limiting Damage," focuses on how to limit damage to your computer.

Chapter 36, "Keeping Up ToDate On New Threats," examines components of a comprehensive framework that enables enterprises to enhance their threat-mitigation capabilities, while increasing the return on investment of existing information technology infrastructures. This chapter also looks at the role of a multilayered approach to building and maintaining an effective security ecosystem for enterprises.

Chapter 37, "Emerging Technologies," examines differing views on how to deal with weaknesses in the Internet (specifically Internet security).

Chapter 38, "Summary, Conclusions And Recommendations," focuses on these security principles and presents a summary, conclusion and recommendation for each.

Part XV: Appendices

Seven appendices provide additional resources that are available for Internet security. Appendix A shows how to configure Internet authentication service on Microsoft Windows 2003 server windows 2003 / enhanced. Appendix B discusses Internet security management, resiliency and security. Appendix C contains a list of top Internet security implementation and deployment companies. Appendix D contains a list of Internet security products. Appendix E contains a list of Internet security standards. Appendix F contains a list of miscellaneous Internet security resources. The book ends with Appendix G – a glossary of Internet security related terms and acronyms.

CONVENTIONS

This book uses several conventions to help you find your way around, and to help you find important sidebars, facts, tips, notes, cautions, disclaimers and warnings. They alert you to critical information and warn you about problems.

John R. Vacca
Author and IT Consultant
e-mail: jvacca@hti.net
visit us at http://www.johnvacca.com/

Chapter 2

BASIC SECURITY ISSUES

INTRODUCTION

Internet security is a contradiction in terms, like the classic references to Alaskan Crab and the National Security Agency. True security can only be achieved when the information is isolated, locked in a safe, surrounded by guards, dogs and fences, and rendered inaccessible. Some would argue that even then, there is not absolute security. It simply is not possible, therefore, to render a network system completely secure, and anyone who wishes to understand and apply the principles of security to the Internet or any other network, must first understand and accept this basic tenet in order to be successful. In spite of this, managers of network systems must strive to attain this unreachable goal simultaneously [1].

The reason behind this often frustrating dilemma lies in the motivations for the development of networks. Networks were created as a remedy to the problem of data isolation in the early days of computing. "Islands of Automation" were a hindrance to conducting business successfully because critical information required by one "island" could not be accessed by others. Networks became the communication bridges by which these islands could be integrated. Since security and privacy [2] are the antithesis of sharing and distribution, Internet security must become a balance between providing appropriate access to those who need the information and safeguarding that information by denying access to those not authorized. This is all done while assuming some level of risk, which is appropriate to the sensitivity of the information that is to be guarded [1].

This is not intended to imply that Internet security is not necessary, nor that management should not strive for it. On the contrary, the explosion of information across the networks in this country and in the world has raised the specter of corporate espionage to new heights. Corporations today know that in the information age, information is power; and, those organizations which control their information appropriately, can gain a competitive advantage: those who do not are vulnerable to losing valuable trade secrets to competitive spies [1].

Equally dangerous is the possibility of loss of information or compromising that information due to acts of sabotage, such as from disgruntled employees. As employees become more mobile, and as they demand more information while they are on the road, the vulnerabilities of compromised information become more severe by an enterprise's own employees [1].

Within this perplexing situation, managers must navigate between the risks of losing information so necessary to the enterprise's operation and the costs and constraints associated with an overly aggressive security solution. This chapter is intended to help management successfully navigate this course by providing an overview of security principles and the technologies which are appropriate for securing the Internet and networks today [1].

INTERNET AND NETWORK SECURITY ISSUES: BASIC SECURITY CONCEPTS

A good place to begin is by defining the basic concepts involved in securing any object. The key words in the security lexicon are vulnerability, threat, attack, and countermeasure. An examination of each follows [1].

Vulnerability is the susceptibility of a situation to being compromised. It is a potential, a possibility, a weakness, an opening. A vulnerability in and of itself may or may not pose a serious problem, depending on what tools are available to exploit that weakness. The classic definition of vulnerability comes from Greek Mythology, with the story of Achilles, whose heel represented his greatest vulnerability [1].

A threat is an action or tool which can exploit and expose a vulnerability and therefore compromise the integrity of a given system. Not all threats are equal in terms of their ability to expose and exploit the vulnerability. For example, the Microsoft Concept virus exploits a vulnerability in Word Macros allowing access to the users' file system, but the virus itself is relatively benign. Other similar viruses could do a lot more damage [1].

An attack defines the details of how a particular threat could be used to exploit a vulnerability. It is entirely possible that situations could exist where vulnerabilities are known and threats are developed, but no reasonable attack can be conceived to use the specific threat upon a vulnerability of the system. An example of an attack is a Trojan Horse attack, where a destructive tool such as a virus is packaged within a seemingly desirable object, like a piece of free software [1].

Countermeasures are those actions taken to protect systems from attacks which threaten specific vulnerabilities. Achilles covered his heel with a protective metal plate as a countermeasure to potential attacks to his one vulnerability. In the Internet security world, countermeasures consist of tools such as virus detection and cleansing, packet filtering, password authentication, and encryption [1].

Any security scheme must identify vulnerabilities and threats, anticipate potential attacks, assess whether they are likely to succeed or not, assess what the potential damage might be from successful attacks, and then implement countermeasures against those defined attacks which are deemed to be significant enough to counter. Therefore, you can see that security is all about identifying and managing risk, and that security is a very relative

concept which must be tailored to the needs, budget, and culture of each organization. For example, a Trojan Horse attack on one organization could succeed easily and compromise extremely important information. The same attack on another organization would only result in minimal damage, perhaps because there is no sensitive data available on that particular system. Furthermore, companies have personalities just as people do, and therefore, some companies are willing to live with more risk than others. In each of these organizations, different security schemes will be employed with different countermeasures to suit their specific situations [1].

As will be discussed later, management must consider all of these factors in defining a security strategy. Management must also consider the cost of protecting against all possible attacks. Security costs money, and each organization must determine how much it will cost to institute appropriate countermeasures. Only then can an organization truly determine which of the possible spectrum of attacks should be defended, and which should be ignored [1].

Generic Internet Security Threats

In any organization, there are a number of generic security threats which must be dealt with. These include the theft of information, the compromising or corruption of information, loss of confidentiality, and the disruption of service [1].

One of the major threats which companies are dealing with is the introduction of malicious programs over the network. The term "computer virus" has been used loosely to categorize these attacks which come in Trojan Horses, worms, and logic bombs as well as true viruses [1].

A Trojan Horse is a program that conceals harmful code. It usually disguises itself as an attractive or useful program which lures users to execute it, and in doing so, damages the user's system. For example, a posting in the US Department of Energy Computer Advisory Capability page lists a known Trojan Horse in a program called AOL4FREE. While the title suggests that this program will allow you to participate in AOL without any costs, running the program will delete all of the files on your hard disk. The program hidden in the Trojan Horse can be one which causes malicious damage, or one which performs some espionage for the attacker, such as stealing the password file from the computer it invades [1].

A logic bomb is code that checks for certain conditions and when these conditions are met, it "detonates" to do its damage. Sometimes, like the Magellan virus, the trigger logic is a date, but it can be any given set of parameters, including a person's name, a bank account number, or some combination of events and parameters [1].

A worm is a self contained program which replicates itself across the network. Therefore, it multiplies its damage by infecting many different nodes [1].

A virus is code which plants a version of itself in any program it can modify. The Microsoft Concept virus is a good example: once it has "infected" Microsoft Word, all subsequent documents which are opened by the user may only be saved as template files. In all other respects, Microsoft Word continues to operate normally [1].

> **Note:** These are not mutually exclusive threats. A logic bomb could plant a virus under the specified conditions, as could a Trojan Horse deliver a worm.

Furthermore, each of these threats could have different or multiple missions. These could be the theft of data, the compromising of confidentiality, integrity or availability, or the disruption of service to the organization [1].

In addition to planting computer programs which could create these effects, there are also threats which involve the theft or compromise of information while it is in transit between endpoints of a network. One such example is called Snooping, in which an attacker simply eavesdrops on electronic communications [1].

These are the classes of threats that today's network managers must deal with, and that senior management must be aware of, since they will play a major part in determining the appropriate and tolerable cost of security to counteract these potential threats [1].

Internet Security Countermeasures

Given the preceding scenario, a reasonable question at this point might be: "What tools are available today to help mitigate the consequences of these security threats on the network?" The good news is that there are multiple technologies which can be brought to bear on the issues, and they are impressively effective [1].

Internet Security Policy

The bad news is that no amount of technology can overcome a poorly planned, poorly implemented or nonexistent Internet security policy. Consider the following story witnessed by a poster on a security newsgroup on the Internet: A customer being waited on at a public service agency (say a Registry of Motor Vehicles) requires some information from the clerk – who in turn, needs to access that information from a workstation centrally located in the area behind the window. Sitting at the workstation, the clerk yells to a co-worker "Dee, is the password still ...? [1]"

Again, the security of any information in any organization today is primarily dependent on the quality of the Internet security policy and the processes by which that organization imposes on itself. If the security procedures are lax, are not enforced uniformly, and allow gaping security holes to exist, no amount of technology will restore the security breaches. Organizations that are concerned about security on the Internet should ask themselves a few of the following questions before worrying about encryption, packet filtering, proxy servers, and other related technology solutions:

- Does the corporate policy allow passwords such as "password", employee initials, or names or initials of employees' immediate family members?
- Is there a process in place to change passwords periodically?
- Do employees keep their password written on paper under their mousepads, keyboards, monitors, etc.?
- Is there a program in place to make employees aware of the need for security and to disseminate security procedures to the employees to facilitate its implementation?
- Do employees understand the different levels of security of information and what techniques to apply to each to ensure an appropriate level of protection?

- Is the responsibility for information security assigned to a senior member of the management team, who is held accountable for maintaining appropriate security?
- Is there a set of guidelines to identify the security classification of different documents and information generated by the employees?
- Is there a process in place to classify or categorize these documents and information and secure them appropriately [1]?

It should be self evident at this point that the primary need for any organization is to get its own house in order, identify its security needs based on the types of information with which it deals and develop a security policy and plan before committing to technology. The following are some elements of a good security plan:

- Develop security requirements based on an analysis of the organization's mission, the information at risk, the threats to that information and the implications of any successful attacks.
- Appoint a security officer and delineate clearly the required job responsibilities and skills.
- Define appropriate security services and mechanisms and allocate them to components of the company's IT systems.
- Identify different measures of security appropriate for each level.
- Remember that security is not only technology; physical security and procedural security are as important as the technology used.
- Identify users who should have access to each level of security [1].

Authentication

A primary tool in securing any computer system is the ability to recognize and verify the identity of users. This security feature is known as authentication. Traditionally, special names and secret passwords have been used to authenticate users, but as the anecdote in the preceding demonstrates, the password is only as good as the users' ability to keep it secret and protect it from being abused by unauthorized users [1]. There are three generally accepted techniques for authenticating users to host machines:

1. Authentication by something the user knows
2. Authentication by something the user has
3. Authentication by physical characteristics [1]

Authentication By Something The User Knows

Authentication by something the user knows is the password/username concept described in the preceding. There are two common approaches to password authentication, known as PAP and CHAP. PAP, which stands for Password Authentication Protocol, simply asks the requester to provide a "secret" password, and if the password provided is included in the user profiles, the requester is given access. CHAP (Challenge Handshake Authentication Protocol) takes the concept one step further by challenging the requester to encrypt a response to the challenge message. This, in effect, acts as a different password for each entry. Often, the CHAP mechanism is combined with an encrypting smart card, which uses

an encryption key to encode the challenge message. Only if the challenge message is correct will the requester be granted access to the system [1].

Authentication By Something The User Has

In the authentication by something the user has technique, the user is given some kind of token, such as a magnetic stripe card, key. In other sophisticated cases such as the remote access standard RADIUS (which will be discussed later), the user has a smart card equipped with a computer chip which can generate an encrypted code back to the computer system [1].

Authentication By Physical Characteristics

Here, the mechanism is to recognize some measure of the individual which ostensibly cannot be duplicated. Biometric techniques such as fingerprint ID, palm print ID, retinal scan, manual and digital signature, or voice recognition are used to validate the identity of the potential user.

Authentication is also necessary when two computers communicate with each other. For example, what should your host computer do when another computer asks to have a disk mounted which contains all of your organization's personnel data? How do you know that the requesting computer has a legitimate reason to access that information, and that it is not some external network hacker trying to steal information from your organization? In order to prevent such events, the Internet Engineering Task Force (IETF) has formed a working group by the name of IPSec (Internet Protocol Security). Additionally, there are a number of de facto standards – those which are developed by companies rather than by official committees, but which enjoy widespread acceptance. While many of these standards are under review and take some time to work their way through the approval process, two are worthy of mention here, IPSec's SKIP (Simple Key Management for Internet Protocol) and Livingston's RADIUS (Remote Authentication Dial In User Service) [1].

SKIP is a technique for providing authentication and encryption security at the IP layer of the Internet architecture. It relies on the existence of an authority in the network which can issue a certificate [3] to known trusted entities within the system. If an entity claiming to be a member of the system requests an action, the receiving computer system can have the requester present an encrypted certification that they are who they say they are. The certificate conforms to one of the methods of authentication, namely, a secret encoding technique and a secret key which are only available to trusted members of the system. The fact that SKIP operates at the very lowest protocol layers of the architecture, it has the advantage of protecting all upstream applications as well, by preventing connections between systems which are not authorized. Since potential intruders cannot even establish connections, their ability to do malicious damage is severely restricted [1].

In Fig. 2-1, the Requesting Entity first gains a certificate by requesting one from the trusted certification authority (1), who validates the trustworthiness of the Requester by granting a certificate (2) [1]. Armed with this certificate, the Requester can now petition the host and presents the certificate along with the request of the host (3). The host, upon seeing the certificate will grant the information to the requester (4).

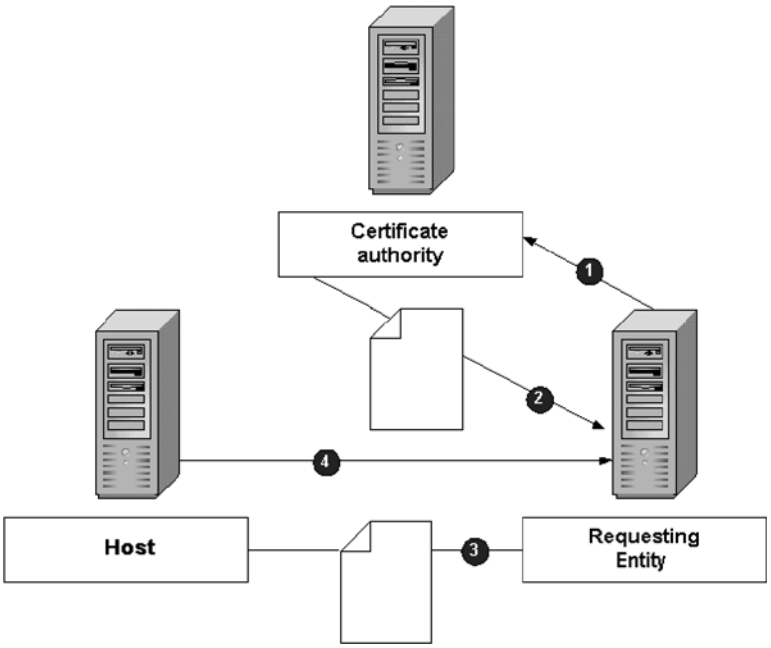

Figure 2-1. How to gain a certificate.

RADIUS is one of the more popular public network authentication protocols. The primary purpose of RADIUS is to offer centralized access control for remote dial-in users. RADIUS simplifies the administration of passwords, user names, profiles for remote users, and other security and accounting related information by placing all of the security in a central server, and issuing challenges to the user [1].

Privacy

A perpetrator may observe confidential data as it traverses the Internet. This ability is probably the largest inhibitor of business-to-business communications today. Without encryption, every message sent may be read by an unauthorized party.

Today, intruders continue to install packet sniffers on root-compromised systems. These sniffers are used to collect account names and passwords, and are frequently installed as part of a widely available kit that also replaces common system files with Trojan horse programs. These kits provide cookbook directions that even a novice or unskilled intruder could use to compromise systems.

Virtual Private Networks

The Internet Community is constantly seeking new and better mechanisms to secure the Internet. Today, there are several other relevant proposals for standards which are under review by the Internet Engineering Task Force (IETF). One proposal which is generating some potential interest is the Level 2 Tunneling Protocol (L2TP), which is under review as

part of the IPSec group within the IETF. This proposal would establish a set of protocols by which compliant Internet components could create their own channel inside the Internet. This channel would be protected by authentication and encryption countermeasures. These would ensure that even though the traffic is being transmitted over the public Internet, individual sessions can be established which are private to those members allowed to work within that channel. The technology is known as tunneling because the correspondents are creating a tunnel of sorts through the public packets inhabiting the Internet, and exchanging very private communications within them. The concept comes from medieval times, where tunnels were built between fortified towns and castles to allow their inhabitants to move safely between them away from the dangers of the bands of marauders outside their gates [1].

The use of tunneling technology allows another concept to be implemented: the concept of a Virtual Private Network, or VPN. Companies who want a less expensive alternative to private Wide Area Networks can utilize tunneling within the Internet and develop their own virtual WANs, safe from unwanted intrusions, yet riding on the cost benefits of the Internet mass volumes [1].

Non Repudiation

This security concept protects against the sender or receiver denying that they sent or received certain communications. For example, when a person sends a certified or registered letter via the United States Postal Service (USPS), the recipient is supposed to prove his or her identity to the delivery person, and then confirm their receipt by signing a form. The signed form is then returned to the sender, which proves to the sender that their correspondence was delivered. This prevents the recipient (for example a debtor) from claiming that they never received the correspondence (for example a demand note) and therefore using that as an excuse for their actions (not paying the debt). In computer networks, these kinds of services are also available, and are becoming increasingly valuable as commerce on the Internet continues to gain in popularity [1]. There are three different types of non-repudiation services that are applicable in computer network messaging:

1. Non-repudiation of Delivery Service.
2. Non-repudiation of Origin Service.
3. Non-repudiation of Submission Service [1].

Non-repudiation of Delivery Service is similar to the US Post office certified mail example in the preceding. This provides the sender with proof that a message was successfully delivered to the intended recipient. Many e-mail packages offer senders the option to request a return receipt. This return receipt provides the sender with a non-repudiation of delivery service feature – the recipient can't legitimately claim they did not receive the message [1].

Non-repudiation of Origin of Service provides the recipient with proof of who originated the message and what it contains. For example, according to a usenet posting, America Online (AOL) was victimized by crackers pretending to be AOL employees and requesting passwords and credit card information from subscribers. In other words, a particular cracker armed with an AOL hacker program created a fake screen to pass himself off as an AOL employee and steal the AOL user's password. Non Repudiation of Origin of Service could

have foiled this kind of attack if it had been available to AOL subscribers. If it had been available, users could have verified that the crackers were not genuinely AOL employees, and therefore would not have given away their passwords [1].

Non-repudiation of Submission Service is similar to the concept of non repudiation of delivery. This service offers proof that a given message was in fact sent from a particular sender. If you go back to the US Post Office example, when you mail important papers such as legal documents, it is considered prudent to send them via registered mail. When you do so, you get a receipt from the Postal Service and a special identification number is affixed to the return. Thus, if the recipient does not receive the documents, or contends that it was not sent on time, you have evidence that your submission did occur at a particular time [1].

Integrity

Integrity refers to the completeness and fidelity of the message as it passes through the network. The key here is making sure that the data passes from the source to the destination without undetected alteration [1].

> **Note:** The use of the word "undetected" is important here. You may not be able to thwart someone from tapping out messages and attempting to modify them as they move through the network, but you will be able to detect any attempt at modification and therefore reject the message if such a modification attempt is detectable.

If the order of transmitted data also is ensured, the service is termed connection-oriented integrity. The term anti-replay refers to a minimal form of connection-oriented integrity designed to detect and reject duplicated or very old data units [1].

Confidentiality

Confidentiality is a security property that ensures that data is disclosed only to those authorized to use it, and that it is not disclosed to unauthorized parties. The key point behind ensuring the confidentiality of information on the network is to deny information to anyone who is not specifically authorized to see it or use it. Encryption is a frequently used mechanism for guaranteeing confidentiality, since only those recipients who have access to the decrypting key are able to decode the messages. Confidentiality therefore equates to privacy [1].

Access Control

Finally, the access control concept relates to the accepting or rejecting of a particular requester to have access to some service or data in any given system. A service could be a program, a device such as a printer or a file system, and data could be a text file, an image, a collection of files, or any combination of the above. The real question is, what are the risks involved in allowing access to any of the system's services or information to individuals requesting such access? In some cases, such as the advertising Web page of an organization, the answer is that no damage could occur. The objective of such a page is precisely to spread the word about the organization, and therefore access control is not an issue. On the other

hand, access control is a major issue if someone requests access to the file which contains the passwords for all of the users of the system. It is therefore necessary to define a set of access rights, privileges, and authorizations, and assign these to appropriate people within the domain of the system under analysis [1].

SUMMARY AND CONCLUSIONS

Okay, so now you've covered all of the building blocks and some examples of how they might go together. The question still might be on your mind: What should the organization do to be secure. The answer is "it depends." It depends on specific security needs and budget limitations of your organization. Very few enterprises, not even the Federal Government and the Military, can afford "security at any price." Eventually, you will be forced to stop building security features and learn to live with the residual risks of your system. Where you stop depends on how much you are willing to pay to get the amount of security appropriate to your application [1].

One typical and common sense approach is to develop a security infrastructure incrementally. Start inexpensively with packet filtering and authenticating routers as the beginning firewall [4]. Many industry analysts contend that over 90% of attacks can be successfully defended by integrated routers and firewalls. Later, if you still need more, you can add encryption and key management for further enhancements. At each point, determine where your vulnerabilities are, what the potential attacks might be, and what consequences would ensue from a successful attack. Many people find that the use of simple and inexpensive packet filtering and authentication, "move their dots" into the lower left hand quadrant of the likelihood/consequence space, and they have no further need to add more sophisticated measures. Certainly, if more is required, and the cost implications are warranted, customers can move into application coupled systems to further enhance the security. The ultimate move, of course, is to go to private networks, where one eliminates the physical connection to the network from potential hackers. Finally, use the services of agencies such as the National Computer Security Agency (NCSA) and ISS, which offer security audits of sites to help you determine vulnerabilities and countermeasures, and help you decide whether the risks facing your operations warrant further expenditures of time and money [1].

REFERENCES

[1] "Internet Security Primer," copyright 2003/2004 ZZZ Online, ZZZ Online, 2004.

[2] John R. Vacca, Net Privacy: A Guide to Developing and Implementing an Ironclad ebusiness Privacy Plan, McGraw-Hill, 2001.

[3] John R. Vacca, Public Key Infrastructure: Building Trusted Applications and Web Servicess, Auerbach Publications, 2004.

[4] John R. Vacca, Firewalls: Jumpstart for Network and Systems Administrators, Digital Press, 2004.