

A Guide to Security Technologies

A Primer for IT Professionals



Table of Contents

Introduction	1
Information Security: Sizing Up the Risks	2
Information Crime Statistics	2
Why Computer and Information Crimes Are on the Rise	3
Hacker Tools and Tricks: What You're Up Against	4
The Costs to the Enterprise	6
Fundamental Information Security Concepts	7
Security Policy and the Continuum of Risk	7
Defending the Network Perimeter	8
The Conceptual Building Blocks of Information Security Systems	8
Security Assessment, Management and Monitoring	11
An Overview of Security Technologies	12
User Authentication	12
Implementing Strong Authentication	16
Firewall Systems and Authentication	16
User Identification: Providing Access Credentials	17
Data Privacy	20
Data Integrity	21
Non-Repudiation	22
Technologies for Managing Security	23
Standards in Security Technology	24
SSL: Making online commerce secure	24
IPSec: Building security into Internet connections	24
S/MIME: Secure messaging	25
PKIX: The IETF defines interoperable Public Key Infrastructure	25
Other standards in information security	25
Summary	27
About RSA Security Inc.	27
Glossary	28
Additional Information Resources	43

INTRODUCTION

Information security has emerged as one of the most important segments of the computing industry. Organizations the world over are adopting new, Internet-based approaches to enhance communication, increase customer satisfaction and reduce costs. Security is the enabler that makes these new approaches suitable for commercial use. Technologies such as firewalls, Virtual Private Network (VPN) connections, session encryption, digital certificates and others are now entering the mainstream of business computing; each offers, in its own way, an important stepping stone for companies looking to advance further into the next generation of open computing and electronic commerce.

Yet it is not a straightforward path. There is no one solution or approach that solves all information security problems. Making matters worse, the technologies and protocols that are the foundation of security approaches can be abstract, complex and difficult to grasp. And practically every day it seems a new protocol, technology or strategic alliance is announced that promises to change the complexion of the information security marketplace.

As a result, network managers and IT professionals are left on their own, to piece together a patchwork of systems that may or may not adequately address the real security risks confronting their organizations. *A Guide to Security Technologies* was created for this audience, and is intended to be a primer, to make the complicated issues behind security technology easier to understand, and thereby easier to apply as enablers of strategic business initiatives.

This Guide provides information on:

- 1) the major threats to information security;
- 2) the key concepts which are the foundation of information security measures;
- 3) the leading security technology implementations;
- 4) related industry standards.

With this information in hand, it is hoped that security managers and IT professionals can make better-informed decisions about today's security options, and also have the necessary context for understanding continuing advances in security technology.

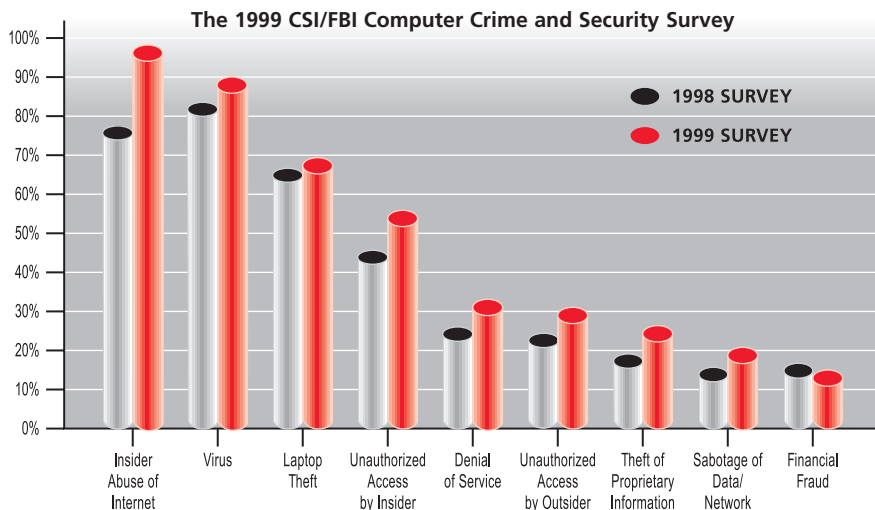
INFORMATION SECURITY: SIZING UP THE RISKS

The issue of information security has grown in prominence in recent years, especially as the Internet has come into widespread commercial use. In this section we examine the phenomenon of hacking and computer crime: How extensive is it? What factors are behind its growth? What are hackers actually doing, and how are they doing it? And what are the real threats to businesses and their computer systems?

Information Crime Statistics

Each year since 1996, the Federal Bureau of Investigation (FBI) and Computer Security Institute (CSI) have jointly surveyed security managers at a wide range of U.S. corporations, government agencies, financial institutions and universities to uncover trends in computer crime. Some of the key findings from the 1999 CSI/FBI Computer Crime and Security Survey include:

- > **Most organizations reported being victimized by computer crime.** 62% of respondents admitted that they had been victimized by computer security breaches in the previous 12 months. When considered in light of the fact that many, if not most computer crimes go undetected, it is clear that the issue of security breaches should be of concern to every organization.
- > **The damages resulting from computer crime are significant.** Not all organizations that were victimized by computer security breaches were able to quantify their losses. However, the losses of those survey respondents that could totaled more than \$100,000,000. Notably, the theft of proprietary information resulted in the highest financial losses, continuing a rising trend.
- > **Insider and outsider attacks continue to increase.** Unauthorized access by malicious employees still remains one of the most serious security threats; in the 1999 survey it was reported by 55% of respondents. System penetration by outsiders increased as well, with 30% of respondents reporting intrusions.



But the problem of information security is not limited to the United States; in fact, many of the crimes reported in the CSI/FBI research originated outside the United States. A quick review of press reports shows that information security is a problem for organizations the world over — Japan, China, India, Russia, Europe and Latin America. Simply put, as the use of computing increases in a society, so grows the risk of information crime.

Why Computer and Information Crimes Are on the Rise

All parties involved in information security agree that the threat from computer crime is more serious today than ever before. A number of trends have worked together to make this the case; and because these trends are likely to continue in the foreseeable future, the threat to organizations will only become more serious. The trends driving this increase in computer crime include:

- > **The rise of distributed computing.** The migration of computing power from the centralized datacenters of the past to today's distributed networks of desktop systems has made information security much more problematic. To use a metaphor, it is easier to guard a bank vault than to guard every house in town.
- > **The trend toward mobile computing.** As working from home and logging on from the road have become more widespread, the number of remote access ports has skyrocketed. This means more network openings, and therefore, more opportunities for criminals.
- > **The emergence of the Internet for business communications.** While a few years ago, use of the Internet was limited to the information elite, it has now entered the mainstream of computing and will continue to ingrain itself as the infrastructure medium of choice. As that evolution continues, we are seeing the nature of Internet communications changing, from one-way information exchange, to transactions. The security problems the Internet introduces are many:

The ultimate connection medium — In a sense, the Internet connects any and all networked computers into a single network. This is a fact that works to the advantage of hackers, offering them a kind of direct "exit ramp" from the Internet to practically any network or company they choose to target.

A public space — A second critical fact of Internet life is that it is inherently a public network — a conglomeration of hundreds of thousands of server connections, managed by tens of thousands of individuals and organizations, used by tens of millions of people worldwide. Yet it was created without inherent security protocols. Important technologies such as browser-based session encryption and VPNs are therefore being introduced to protect the privacy of transactions traveling through this vulnerable public space.

A worldwide club — With thousands of hacker Web sites and numerous news-groups available, anyone can have access to the latest hacker tricks, tips and tools. The anonymity of Internet discourse also enables the interaction of curious adolescents with international felons, in the comfort and safety of their own living rooms. The Internet has helped break down the barriers of entry to this club.

While it is wrong to point to the Internet as the primary driver of increased information crime, it has clearly and dramatically increased the challenges facing security managers.

- > **Better hacker tools.** The fact that the Internet is an efficient delivery vehicle is only part of the problem. Just as important is that hacker software tools abound and are continually being improved. A quick survey of the wares available on hacker Web sites shows that many are in versions 3, 4 or higher — often revised to make them faster or simpler to use, or to overcome advances in security measures. The sites even offer product datasheets, FAQs and user profiles. The net result is that today, someone with less technical skill and less motivation can do more damage than ever before.
- > **Widespread computer literacy.** When mainframes were the only computers available, only a limited number of people had the requisite technical skill to threaten a company's information security. That situation is now totally reversed, as the use of computers or computer-like devices has become part of everyday life. It is now typical of both white-collar and blue-collar workers to use computers on the job, while half of all homes in the U.S. have at least one computer. Today, virtually anyone can have enough computer experience to pose a threat.

Hacker Tools and Tricks: What You're Up Against

In general, hackers seem to have four motivations: *Challenge*, the desire to outwit a particular security approach, much like solving a puzzle; *Workarounds*, the desire to get around bugs or blocks in a software system; *Mischief*, the desire to inflict some kind of distress on a person or organization; and finally, *Theft*, the stealing of funds or information. The last two reflect the motivations of a malicious hacker, who may resort to electronic terrorism in the extreme. While their motivations may be few, the techniques that hackers will use to gain access to networks and resources are numerous:

- > **Social engineering.** A fancy term for "con artistry", this involves tricking someone into giving you their password or other private information. A typical scam is calling an employee, posing as a network administrator or a fellow employee with an urgent problem which requires the employee's information to solve. Workers have also been known to share private information unreservedly with someone who has no credentials other than a fake business card, or who claims to be a new employee trying to get up to speed. This is the easiest, and thus most common technique used to obtain a password and access to a network.
- > **Password cracking.** Beating password protection is easier than most people think. For one thing, many users will enter no password at all; another sizable percentage will use "secret", or the word "password" itself. Also common are children's names, sports teams, and dates such as birthdays and anniversaries. Because it is cumbersome to manually retry dozens of alternatives, software tools are available which automatically try every theoretical alphanumeric combination of user name and password at high speed — an approach known as "brute force" — often aided by a dictionary of commonly used passwords. The hacker who is lucky enough to locate the encrypted password list on the security server also has the aid of other software tools to decrypt the file.

- > **Network monitoring.** Also known as “sniffing”, this is a deliberate attack that involves deploying a piece of code on the network that monitors all traffic, looking for passwords or other specified information. Often, network traffic travels “in the clear” (meaning unencrypted), making it simple to locate specific information, which can be written into a file on the hacker’s desktop.
- > **Abuse of administrative tools.** Software designed to simplify management of a network can also be misused by malicious parties. For example, a program known as SATAN — an acronym for System Administrator’s Tool for Analyzing Networks — was quickly adopted by hackers as a means for uncovering network weak points.
- > **Man in the middle.** This kind of attack occurs when an unauthorized party successfully plants himself, undetected, between the two parties actively involved in a private communication or transaction, either on a LAN or unsecured Internet session. The third party intercepts and replaces components of the communication with their own, acquiring a password or even taking over the session itself. A hacker will often use “denial of service” attacks (below) to freeze out one of the valid members of the communication session.
- > **Denial of service.** This attack puts an organization out of business for a time by freezing their systems. This means flooding a Web server or any important server with useless hits, so that legitimate traffic is locked out, and important services are no longer available on the network.
- > **Trojan horse.** Hackers have been known to create programs which on the surface appear to be a helpful utility, but which, in reality, are designed to secretly inflict damage. Some actually attempt to open up holes in network security systems.
- > **Virus.** Like the Trojan Horse, a virus is a software-based hack that runs without your permission. Unlike the Trojan Horse, however, it is introduced to your computer without your knowledge, usually via e-mail. What makes the term “virus” apt is that these kinds of code are usually self-replicating, often designed to be spread by one person to another automatically. A type of virus known as a “worm” systematically eats through and destroys stored files.
- > **IP and Web spoofing.** Some security systems use the Internet (IP) address of an incoming session as a means of validating access. IP spoofing, then, is the means of gaining illicit access by masquerading as a valid IP address. Another hack known as Web spoofing works in the opposite direction: the criminal redirects traffic designated to a valid Web or IP address to his own fraudulent, look-alike Web site, where typically credit card information is captured for later use.

The Costs to the Enterprise

Clearly, businesses face a myriad of problems and experience a number of costs as a result of the dirty tricks listed above. They include:

- > **Financial loss.** In addition to direct costs, such as of monies actually stolen due to fraudulent access, there are often huge indirect costs inflicted on victims of information crime. Downtime is a significant cost, in addition to that of recreating files and systems which have been corrupted or destroyed, the legal costs of investigating and prosecuting the crime, the administrative costs to review and enhance security policies, systems and equipment, and many more.
- > **Competitive compromise.** The damages inflicted by information crime on an organization's effectiveness and competitiveness can be substantial. At the extreme, actual trade secrets and business plans may be stolen. But even lesser crimes can hamstring the company with unnecessary costs and force management attention away from the core business.
- > **Lost sales.** Hacking can impact an organization's sales revenues in multiple ways. In addition to directly interrupting the sales process through flooding, spoofing or other mischief, sometimes hackers will try to inflict damage at a more profound level. Successful companies often have a unique way of doing business that their name and reputation embody. Information crimes can undermine a company's reputation and brand essence — making a solid bank seem risky, a clever technology company seem hapless, or a slick consumer products company seem disarrayed.
- > **Legal problems.** In many industries such as banking, finance and health care, companies are bound by a legal or fiduciary duty to safeguard the confidentiality of their customers' records or assets. Organizations that fail to do so can be subject to lawsuits and significant fines — not to mention the loss of customers as a result of negative publicity.

Information security, then, is a two-edged sword. On the one hand, it is incumbent upon organizations to provide appropriate information security to protect both themselves and their customers or constituents. On the other, solid information security is also an *enabler* — allowing organizations to take full advantage of new approaches such as e-commerce, and to gain the resulting benefits.

FUNDAMENTAL INFORMATION SECURITY CONCEPTS

Clearly, the challenges to an organization's information security are many, and inherently unpredictable. The nature of information crime is in constant evolution, devising new approaches and techniques in response to advances in system and security technology, always with the purpose of avoiding detection. For security managers it can be much like fighting an unseen assailant — one who may not even be detected until a potentially lethal blow has been struck.

Yet, this is not to say that the security manager is helpless in the fight. In this section, we will discuss the principles that are the underpinnings of information security systems; in later sections, we discuss how these principles are applied in security technologies.

Security Policy and the Continuum of Risk

One axiom of information security is that you can't have both access to information and airtight security at the same time. Just as living life fully involves accepting some degree of risk, so we find that operating an organization, attuning it to the needs of its customers and partners and improving its performance naturally involves accepting some level of risk. Somewhere, some time, there will be security breaches; even if computer system security *could* be made airtight, there would still be risks introduced by the human factor, such as deceitful employees and "dumpster divers" scouring for private information.

Factors such as today's reliance on unimpeded information flow, complex Internet-worked systems, the emergence of virtual, partner-based alliances and broad computer usage across contemporary society together suggest that:

- > It is no longer feasible or appropriate to define information security in the simple terms of "Inside the Network = Good; Outside the Network = Bad" as was the case in the past;
- > There are tradeoffs between absolute information security and the efficiency of information flow;
- > Managing the human dimension of information security — both user and administrator — is just as important as implementing physical and software systems; and
- > Security decisions are being influenced by business line managers, with implications that affect revenue generation.

In this landscape, the issue of security policy takes on greater importance. Recognizing that completely airtight information security is unattainable and also perhaps contrary to organizational objectives, security managers need to craft policies that prioritize the organization's risks, placing the strongest security measures against the most dire threats. This approach is essentially optimizing information security decisions, balancing the cost of security measures against accurate assessments of the probability of damages resulting from security breaches.

Defending the Network Perimeter

The concept of the “network perimeter” has been commonly used in the field of information security. It refers to the boundary between access and non-access, the implementation of the trust relationships defined by security policies. Historically, the network perimeter was clearly defined by hardware (i.e., modems and RAS ports). Inside the perimeter was a trusted space where information and resources are made available; anything outside the perimeter was assumed not-trusted, until proven otherwise.

In recent years, however, the emergence of broad connectivity and the Internet have tended to erode this physical description of the perimeter. Business partners have access to a company’s private information via an extranet, customers access their accounts and place orders via a secure Web site, and in fact, *anyone* can interact with the company’s computers via the public Web site. While in the past it may have been reasonable to assume that anyone who had successfully logged onto the network was a trusted party, today, most would agree that assumption is no longer valid. Security technology is evolving to reflect this change, moving from a whole-network perspective, to application-oriented security, where each sensitive resource or application on the network can enforce security policies. This is akin to posting security guards next to every valuable item in a museum, rather than just at the front door, in recognition of the fact that now, the avenues of access are more diffuse than ever before.

The Conceptual Building Blocks of Information Security Systems

Providing information security for an enterprise can be reduced to solving four basic problems:

- > Verifying the authenticity of users;
- > Establishing some means of user identification for purposes of access control;
- > Protecting the privacy and integrity of information on and beyond the network; and
- > Preventing validated parties in a transaction or exchange from denying the actions they have taken.

User Authentication

One of the most fundamental steps in information security is that of recognizing which individuals should be trusted with private information, and then establishing systems which allow only these trusted parties to gain access. Thus, a necessary step is to validate the user who attempts to access any sensitive material, a process known as *authentication*. How does a user prove his or her authenticity in the context of a computer-based interaction? In general, there are three different approaches.

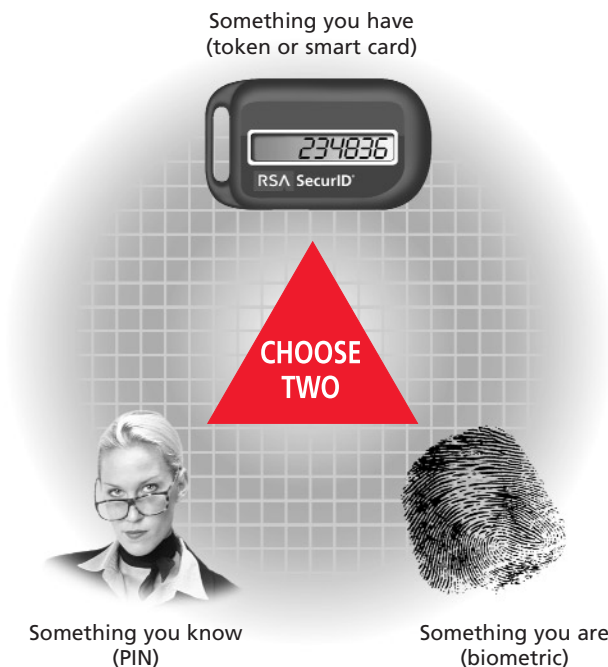
One is where the user provides information that seemingly only he or she would *know*. The password is an example of this form of authentication; it is perhaps the most common way of limiting access in use today. Other familiar examples of this form of authentication include providing a mother’s maiden name, or the date of your last transaction, as often used in customer service situations.

A second approach is to require the user to present proof via something unique that only he or she *has*. This is the approach used when the bank asks for obscure information off of your monthly statement, or a control number printed on the surface of your credit card. For ongoing access to computer networks however, it is common to provide a token of some sort to valid users, which can take a range of forms. These can include dedicated authenticators which generate access codes; general purpose “smart cards”; special authentication software for use on PCs or PDAs; and finally, digital certificates — difficult-to-fake files issued by a trusted party which attest to the individual’s validity, like a passport.

A third authentication approach is to test something that represents what the user physically is. Known as *biometrics*, these forms of authentication can include fingerprints, voice prints, retinal scans or a number of other physical tests.

Each of these three main authentication approaches has its own strengths and weaknesses. The simplest to implement is generally the password, which accounts for its broad use. However, passwords can be vulnerable in many ways, ranging from guessing, to interception off the network, to outright theft or “social engineering” methods, in which users are tricked into providing their passwords to hackers. For this reason, authentication via password does not offer a suitable level of protection for more sensitive data and applications.

By combining approaches — as in password plus token authentication, or biometric plus password — a much stronger level of security can be obtained. This is the approach known as *two-factor authentication*, and is currently used to protect millions of users in organizations around the world.



User Identification

An issue closely related to authentication is *user identification*, which in information security relates to the issuing and verification of appropriate access privileges to the authenticated individual. This is much like the process of issuing a driver's license: the individual must first prove his or her authenticity to the issuing agency. Once that step has been achieved, the issued license itself then becomes a public proof of identity for that person, while also providing evidence of his or her privileges (i.e., licensed to drive an automobile vs. a truck or bus). Likewise in information security, once the individual is authenticated, electronic credentials can be issued which are validated as the person seeks to access various resources on the network. The credentials grant access to certain protected files, but not others.

There are various systems and approaches for access control in a networked or Internet environment. However, as organizations are moving toward application-level security, a greater burden is placed on their users to authenticate themselves repeatedly as they access multiple protected systems. The term *single (or reduced) sign-on* refers to technology which simplifies an authorized user's repeated access to protected files and applications, without requiring multiple authentication sessions.

Data Privacy and Integrity

When the properly authorized individual begins working, it is important that sensitive or privileged content be protected from eavesdropping or other tampering. This is particularly important if the Internet is the communications medium, since Internet traffic travels through a public space that offers many opportunities for interception and alteration.

The most common method for keeping communications private is by employing *encryption*: rendering meaningful data into apparently random bits, which can only be understood by the intended receiver who knows the secret necessary to decrypt the data or message. Cryptography can also be applied to solve other information security problems: for example, a *digital signature* uses encryption to assure *data integrity* — proof that the original file has not been altered since it was transmitted — as well as *non-repudiation*.

Non-repudiation

When two trusted parties are involved in a transaction — whether a sale, or communication of sensitive information — it is in the interest of both parties that neither one later denies that the transaction occurred. Systems designed to provide non-repudiation services can issue proof both that a particular communication was actually sent by the originating party and not an impostor, and also that the intended addressee actually received the message.

These topics — authentication, identification, data privacy, data integrity and non-repudiation — form the pillars of today's security technologies. In the next section, various implementations of these concepts into security technology will be explored in more detail.

Security Assessment, Management and Monitoring

In addition to the creation of security policy and the implementation of security systems is the task of administering the security system. This administrative role primarily involves three tasks:

- > Assessing security to uncover weaknesses in current security methods. Software systems are available to perform this task. Also, many companies choose to hire outside firms to provide audits of their security systems. In this process, the differences between planned security policy and actual settings are identified;
- > User and system management, which involves keeping files of authorized users and privileges, and of system resources, applications and files, accurate and up-to-date; and
- > Monitoring patterns of suspicious activity in real time to detect attempts at unauthorized access, and creating audit records that may be necessary to bring action against an employee or outside criminals.

In practice, the features built into security solutions to provide management and monitoring services can be among the most important determinants in the final selection between competing alternatives.

AN OVERVIEW OF SECURITY TECHNOLOGIES

A detailed discussion of all current and emerging security technologies is beyond the scope of this Guide. Rather, our goal here is to cover the main principles that underlie today's commercial security solutions, based on the problems of user authentication, identification, data privacy, data integrity and non-repudiation, as described in the previous chapter. A section on security management, including security assessment and intrusion detection, is also included.

User Authentication

The most fundamental information security task is user authentication — assuring that the user has valid rights to access system resources. Performing user authentication in a reliable way is perhaps the most important step towards reducing an organization's exposure to information crime.

- > Popular technologies for authenticating users include: **password systems, authentication devices** (tokens, software tokens and smart cards), **biometrics and digital certificates**.

- > Each approach has its strengths and weaknesses; no one authentication is right for every purpose. Combining approaches into **two-factor** systems can provide a much **higher degree of protection** than single-factor implementations.
For information security managers, the job is to pick and choose, **protecting resources** based on their sensitivity and risk.

Password systems. Among the most familiar techniques for providing proof of user authenticity are passwords. On the surface, they would seem an ideal solution, since the range of possible passwords is virtually unlimited; what better proof of authenticity could there possibly be than a unique word or combination of random characters specially chosen by an individual?

The reality of password security, however, does not live up to this promise. There are a multitude of approaches for beating password protection, including automated guessing programs, network monitoring tools, and “social engineering” tricks.

Because of this “porosity”, password-only protection is best suited to protecting information and systems that are not highly sensitive.

The most popular protocols for handling password authentication are TACACS+ (Terminal Access Controller Access Control System), developed by Cisco Systems, and RADIUS (Remote Authentication Dial-In User Service), now an IETF (Internet Engineering Task Force) standard. Both of these protocols are designed to go beyond simply processing a password session, to provide “AAA” services: authentication, authorization and accounting. RADIUS in particular has shown strong acceptance among companies that provide Internet services. Both can be used in conjunction with strong authentication systems.

Both RADIUS and TACACS+ use the PPP mechanisms of PAP (Password Authentication Protocol) and CHAP (Challenge Authentication Protocol) to actually process authentication requests. PAP is a simple password-lookup, with the option of encrypting the password in transit to prevent eavesdropping. The stronger CHAP issues a randomly-generated “challenge code” to the user at login; this code is combined with the user password and then encrypted into a hash code which is returned to the server for verification. In this way, CHAP protects against capture and replay of a password. Both TACACS and RADIUS will attempt CHAP authentication first, then PAP authentication before rejecting a user as invalid.

An alternative approach to strengthening password security is the *one-time password*. Here, when establishing the account, both the client and the server agree to a *series* of valid passwords; each time the user connects, the next password in the series is used. The purpose again is to protect against replay of an intercepted password session. One-time password systems, however, have not achieved widespread commercial success.

Token-based authentication. A stronger approach to user authentication involves distributing a device to authorized users, often called a “token”, which generates a code which must be used to log on. This token can be either a hardware device or a software utility. Importantly, the token must do more than simply communicate an unchanging account number, which could be reused if intercepted during transmission. Instead, authentication devices use a number of technologies to outwit hackers through constantly changing access codes: shared secrets, one-time passwords, time-code synchronization between client and server, and sometimes, challenge-response. Often multiple approaches are combined, along with encryption or hash algorithms to further protect communications.

Because token systems also use PIN numbers to limit access to the code-generating device or software, they are known as “two-factor authentication” — the two factors being the PIN (something the user knows) and the token (something the user possesses, as evidenced by the code it generates). This is analogous to a bank ATM card and PIN. Because capturing both the physical token and the PIN is exceedingly difficult, this approach provides much stronger authentication than passwords; yet it imposes this strong security with less user burden and greater scalability than biometric systems.

The most popular strong authenticators in use today are small handheld devices which generate a changing numeric authentication code each minute; to gain access, the user simply enters this code together with their PIN or password. This changing authentication code is based on a secret “seed value” known only to the authentication device and the security server that issued it. By combining the secret value with the current time, and then scrambling that resulting value with an algorithm, the authentication code both preserves the secrecy of the shared value, and provides a changing value that is only valid at the time of issuance. The security server authenticates

the user by generating its own version of the currently-valid code, based on the secret value in its records, and comparing it against the code supplied by the user. A valid code supplied with the correct user name and PIN at the time of logon is considered proof of the presence of both factors — the person and the physical token — and therefore the user is considered authentic.

An alternative two-factor system uses a similar device, but employs a challenge-response approach to avoid transmitting a password. At logon, the server issues a challenge code, which the user manually enters into their authenticator; via an algorithm, a response code is generated by the device which is then entered and sent back to the authentication server for validation. The fact that the secret response-generating algorithm is embedded in the authentication device is proof of the physical presence of the token. This system is considered more cumbersome by many end users because of the extra steps required.

Token-based two-factor authentication can create a prodigiously high barrier for hackers attempting to gain unauthorized access. Millions of users around the world are currently protected by two-factor authentication systems. The primary drawback is the cost of providing the authenticators to authorized users; this is becoming less of an issue as the technology matures, and production costs are lowered. Also, as smart card technology is becoming more widely adopted, companies can choose to deploy two-factor authentication through their smart card system.

Smart cards. Almost a billion smart cards are in use around the world. While new to the United States, smart cards are in common use in Europe and Asia for banking and payments (e.g., pay telephones, public transit, pay television services), for storing personal information such as medical records, and are now being looked at for authentication purposes.

Smart cards can be considered an enhancement of familiar credit card or bank ATM cards. In contrast to the credit card's simple magnetic stripe, which carries some form of static information such as an account number, the smart card has both dynamic memory and a chip built into it, which allow it to process and update stored information — hence the term “smart”. While the credit card's magnetic stripe is external and thus readily available for reading, the smart card's on-board processor prevents access to stored information. So, for example, rather than carrying a large amount of cash, the smart card user can do an electronic transaction which deposits a certain amount of cash credit onto the smart card; now the user doesn't have to worry about the money being lost or stolen, since only he or she has access to the PIN-protected smart card.

Smart cards are available with the features of a two-factor authentication token applied; some also have the ability to interact with public key infrastructure systems, providing a wide range of information security services described later in this section. To use the smart card for authentication, the user activates the smart card's token code-generating application using a PIN. Because this PIN number is never communicated outside the card, smart cards can provide a very secure platform for authentication.

Smart cards can also include photo IDs and magnetic stripes for physical access privileges, as well as memory space for bank credit data. This makes smart cards an attractive, multiple-purpose option. The drawbacks for authentication use are the cost of supplying card readers to all protected PC users, and the fact that no single standard has yet emerged as the clear winner in the smart card space.


Biometrics. Systems which base user authentication on measurements of unique physical features — fingerprints, retinal scans, voice recognition or others — are popularly considered the ultimate in strong authentication. And in fact, biometric systems can provide very strong authentication; however, a number of factors have kept biometrics from achieving widespread acceptance for network access application, including high cost and intrusiveness.

A number of logical problems must also be resolved before biometrics will be the authentication approach of choice. For example, say a company uses thumbprint recognition as its form of authentication. Every time a user touches a drinking glass, doorknob or keyboard, he is literally leaving a copy of his password out in public. To provide verification, the biometric system must deliver some reliable proof that the user actually provided the biometric reading at the time of authentication: how can this be done when a user is logging on via a remote access device? Also, passwords, token codes and digital certificates are easily changed; however, changing the user's retinal pattern or voiceprint is not practical should the data be compromised.

Therefore, while appropriate for some authentication scenarios — and holding much promise for the future — today's biometric systems are generally not considered suitable for protecting a broad range of information resources, across various forms of access media, on the typical enterprise network.

Digital certificates. For some user authentication applications, *digital certificates* can serve as proof of identity. The digital certificate is a special file, issued by a public key system, that binds an individual to an encryption key; anything of a private nature that is meant for that individual should be encrypted using this "public" encryption key. Only the valid user has the ability to decrypt the information via a second key, which is held in absolute secrecy — for all others, the information will be unintelligible. The strength of encryption used prevents hackers from unlocking the information.

A Digital Certificate Issued by the RSA Keon Certificate Server



SERIAL NUMBER: AcbOda0137a5fa78568f
VALIDITY: Nov. 03, 1999 - Nov. 03, 2000

SUBJECT/NAME/ORGANIZATION
 Locality - Internet
 Organization - ABCZZZ Company
 Organizational Unit - Finance - Individual Subscriber
 Organizational Unit - www.abczzz.com/rapesidiary/CPS
 Incorp. by Red, XOYJK
 Organization Unit - Digital ID
 Common Name - John Doe
 Email Address - jdoe@abczzz.com
 Unstructured Address - 10 Main Street Bedford

PUBLIC KEY:
 kdkjfkmsaigmkepelmkdljduoe
 jeijfgkoeksjkdjgfiloadjg

SIGNED BY: ABCZZZ Company:
 kdkjfkmsaigmkepelmkdljduoe
 jeijfgkoeksjkdjgfiloadjg

Status: Valid

Digital certificates can provide **important value** for user authentication, and are often used in conjunction with smart cards. **Public key systems**, which are described in more detail in the following sections, also address a wide range of other information security services, and thus are one of the most important **information security technologies**.

Implementing Strong Authentication

User authentication can be implemented in a number of ways. Most people are familiar with the idea of authenticating when accessing a network or service from a physically remote location — for example, when logging onto an online service provider, or dialing up a remote access server on the company's network from a hotel room. However, depending on the needs of the organization, user authentication can be implemented in a variety of other ways as well:

- > *To validate all logons* to local area networks, providing user accountability and protecting against internal information crimes;
- > *To protect physical access to individual desktop systems* and network hosts, thus assuring that only valid users can gain access to files and network services, and eliminating the exposure resulting from stolen laptop systems;
- > *To augment a third party service provider's offering*, such as a VPN service;
- > *To enforce strong authentication to firewall systems* before allowing any external access to a protected IP network;
- > *To control access to individual Web pages or Web-based applications* or directories on an intranet/extranet server.

Firewall Systems and Authentication

Firewall is the term given to a hardware or software system that controls access between two networks. Typically, a firewall acts as a barrier between the Internet and a private corporate network, allowing only authorized parties to cross the barrier. Today, firewalls are one of the most popular alternatives for enforcing access control, and can support both password authentication and two-factor authentication, generally using TACACS+ or RADIUS protocols for centralized management of authentication, authorization and accounting.

Firewalls are typically implemented on a router — a hardware device that serves as a connection between two networks — and primarily implement two strategies for access control. *Packet filtering*, which operates on the network level, is used to block out all “illegal” traffic, as defined by security policy; for example, allowing incoming access only to known trusted parties based on the source IP address. An alternative approach used by other firewalls is the *proxy server* (also known as an *application gateway*), which disallows connections directly between the Internet and private network, instead serving as a middleman between the two. Often used to mask the addresses of the resources on the private network, the proxy server is more aware of the content of the transactions it is processing than the packet filtering firewall (and

thus, is slower than the packet filtering firewall). However, application gateways offer more opportunity for access control, authentication and logging of suspect incidents. To gain the best features of each approach, some vendors now offer hybrid firewalls with “stateful inspection” — offering both the ability to filter the header information and look deeper into the packet as needed.

While firewalls can provide important security services to enterprise networks, they have some known shortcomings. Because they enforce *security policy* — a foreign notion to many organizations — firewalls are often implemented ineffectively, therefore providing a sense of invulnerability that is unwarranted. The hacker technique known as “IP spoofing” — an invalid user masquerading behind a false IP address — can be used to bypass packet filtering firewalls; strong authentication services can prevent this hack. Also, firewalls control access but typically do not control content, and thus won’t prevent a user from receiving an attachment that contains a virus, one of the most commonly encountered information security problems.

User Identification: Providing Access Credentials

Earlier, we used the analogy of issuing a driver’s license to illustrate the difference between *authentication* and the ongoing *identification* of the user. In terms of information security, a user ideally authenticates to the network once, and then a rights-based system provides reliable access to the information resources for which he or she has been approved.

This issue of enforcing personal access rights grows more pressing as the network perimeter erodes and the need to provide application-based security increases in importance. However, a piecemeal approach to application security can overwhelm users with constant authentication sessions and multi-level passwords. While simple in principle, implementing a comprehensive approach to application security — sometimes known as *secure single sign-on* — is a non-trivial undertaking. One of the primary challenges is appending a common set of security features into various network resources that often are not “security aware”.

There are a number of technology implementations designed to manage access to sensitive files and applications on a network. One of the earliest systems was Kerberos, developed at MIT in the late 1970s and named for the three-headed sentry dog from Greek mythology. In this approach, the central security server uses symmetric cryptography to issue an encrypted “ticket” to the user at logon, which is verified by protected applications and resources on the network that the user seeks to access. Kerberos has achieved a degree of success, and is still in use today; however, this approach suffers from difficulty of implementation, limited scalability and does not address the need to secure interactions between organizations. Today, most information security practitioners see asymmetric cryptography — better known as “public key” cryptography — as a better and more scalable security solution.

There are many implementations of public key cryptography which provide user identification and access control, ranging from comprehensive network access systems at one end, to more modest application-specific implementations on the other. A relatively familiar example is that of securing access to a private Web site, such as an online brokerage service, using SSL encryption. While the main purpose of SSL is protecting the privacy of communications, access control can also be implemented.

In this SSL example, the client generates an encryption key for use during the session to preserve the secrecy of the password and other data transmitted; this key is communicated with the server privately using the server's public key. Once the client has been authenticated, the server issues a "cookie" to the client's browser software, which can include any access privileges and length of validity. Each user request for information or resources from a server within that protected domain will prompt the verification of the existence and current validity of the cookie before responding; these access credentials are protected by the encryption scheme agreed to at the initiation of the secure SSL session. When the user logs off from the site, the cookie is removed to protect against "session hijacking", where an unauthorized third party tries to continue using the credentials of the valid user.

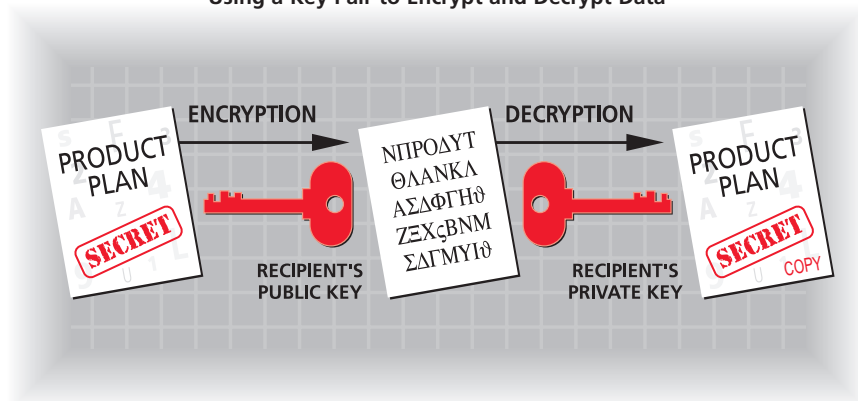
While on the surface, these two approaches may seem quite similar — one using "tickets", the other using "cookies" — there is an important difference that goes beyond nomenclature: the latter implementation, by virtue of its use of public key technology, offers a scalable, interoperable solution, while also providing the additional security services of data privacy, integrity and non-repudiation. To fully appreciate the difference, one must understand the principles behind public key cryptography.

Public Key Cryptography: The Yin and Yang Approach to Security

Where symmetric encryption uses the same key to encrypt and decrypt data, asymmetric encryption uses one key to encrypt data, and a completely different, but mathematically related, key to decrypt it. Either key can be used to encrypt a file; however, only the *complementary* key can decrypt the file.

This yin-yang relationship of key pairs creates a powerful tool for security purposes. Because one key is kept private, the other key can be made public or distributed widely: anyone can use it to encrypt a confidential message for the person who owns the private key. Conversely, anything that decrypts correctly with an individual's public key clearly was encrypted with their private key. In public key cryptography, a critical issue is therefore to attest to the validity of the key pair. For example, if a message decrypts using what is presented as the company president's public key, how can you trust that it really IS the president's public key?

Using a Key Pair to Encrypt and Decrypt Data



The *digital certificate* is the means for accomplishing this, binding an individual's identity to a public key. It is an encrypted file that attests to the authenticity of the bearer, created by a trusted third party known as a *certificate authority*. Proof of the authenticity of the certificate is that it decrypts correctly using the recognized "public key" of the certificate authority (or CA). The CA may be a secure server on the network (known as a "single party trust model") or an external organization recognized by many (the "multi-party trust model"). Verisign, GTE and Netscape all run public CAs.

While **public key technology** can easily be put to work within an organization, it can also provide interoperable security services between organizations. Any party can instantly be recognized in a secure fashion by a public key system, if it bears a certificate from a trusted CA. Public Key Infrastructure (PKI) consists of **protocols, services and standards** supporting interoperable applications of public key **cryptography**. Vendors are working to create an industry-standard implementation of public key technology, which **standardizes** not only certificate types, but also the principles used for **recognizing and managing** a certificate authority — the **trusted parties** that issue certificates to known parties. Other **critical issues** in standardizing PKI systems are the use of directory services for locating certificates for specific individuals, and **communicating** revocation of certificates.

Advanced access control systems

While verifying the authenticity of the user is a primary issue in information security, closely related is the issuance of comprehensive access rights — known as user identification — for validated parties. While the online brokerage example stated previously lays out the simple concepts involved in using public key technology to enforce access controls based on user identity, it is useful to understand how a more comprehensive system designed to protect an enterprise network might function. Software "agents", akin to security guards, are placed at strategic points throughout the network: embedded in networking devices, built into operating systems and placed to protect sensitive applications and files, such as ERP applications or private Web pages. Even applications that do not natively support security features can be "wrapped" with a software agent, to offer protection from illicit access.

Whenever a user logs on to the network, the agent positioned at the point of first contact — network server, RAS or router — initiates user authentication. When the user has been authenticated, the next step is to grant the user access rights; typically, these rights are defined in a central *access control list* (ACL) of valid users. The ACL defines access rights based on role, division and possibly other factors. The security server issues the user two different digital certificates to enable access across the network: an *identity certificate*, which is a standard X.509 digital certificate attesting to the identity of the user and his or her public key, and a separate *attribute certificate*, which is a secure file listing the user's access rights. Because a network server issues the attribute certificate, the user is able to log on from remote or shared computers, without losing access to his credentials.

The authenticated individual is then free to use network services. Each time a protected asset on the network is called on, the agent standing guard verifies the user's credentials — both identity and attribute certificates — in a manner that is transparent to the user. Such features as the length of validity for the certificates, or the amount of dormant time allowed before revocation, can be set by administrator policies. Also, systems built on smart card authentication can require that the smart card remain in the reader device to allow access, thus temporarily suspending the user's credentials while away from their desk.

Data Privacy

Once a connection to a secured resource or network has been established, the next issue is that of protecting the privacy of the information accessed. The primary technology used is *encryption* — rendering the information into a meaningless code while it is in transit and storage, but reconstituting it into readable form when needed. As suggested earlier, there are two main variants of encryption: *symmetric* encryption, where the same key is used to encrypt and decrypt the file, and *asymmetric* encryption, where one key encrypts and its partner decrypts (and vice versa).

All encryption functions by essentially throwing a needle into a haystack, while providing your intended recipient (and *only* the intended recipient) with the magnet needed to find it easily. More specifically: a relatively simple calculation can convert information into a cipher, while multiple billions of calculations are needed to test all possible alternatives in order to unlock the cipher. The term *modulus* refers to the “root” of the encryption key, or *key length*; a longer modulus (40-bit, 56-bit, 128-bit, etc.) increases the possible answers to test exponentially, therefore making it more difficult to unlock the cipher without the valid key. As computer CPUs become more powerful and thus able to test decryption alternatives faster, encryption can be made more difficult by employing longer moduli.

Symmetric encryption. Data Encryption Standard (DES) is the most widely used symmetric encryption standard. It is commonly used for encrypting long communications, and has the advantage of speedy decryption. To overcome the fact that DES is a relatively old system with a rather short modulus, an approach called *Triple DES* is used: the same data is DES encrypted three times, employing two or sometimes three different keys. This increases the strength of the encryption exponentially.

The security of symmetric encryption relies on the fact that only the creator and the receiver share the cryptographic *key* (or keys in the case of Triple DES). To accomplish this, the keys are often communicated under the protection of some pre-existing master key that both share, or using the public key of one of the parties. When these methods are not possible, mathematically abstruse systems such as the Diffie-Hellman Key Agreement or the Department of Defense's Key Exchange Agreement (KEA) provide a kind of protocol where the two parties can exchange unencrypted messages which allow them and only them to derive a common secret key value.

Public key cryptography. While we have discussed the digital certificate's use in verifying a user's identity, public key systems also provide data privacy through encryption. For example, the Secure Sockets Layer (SSL) encryption described earlier imposes encryption to protect Internet traffic from eavesdropping. Similarly, users can securely encode e-mail communications using the public keys of their recipients. Because of the speed of its decryption, it is common to encrypt a lengthy document with DES and then include the DES key, which has been encrypted with the recipient's public key.

Data Integrity

Even with the use of cryptography to prevent outsiders from intercepting a private communication, we often need an additional level of proof that a particular message or transaction was not tampered with. This can be especially true if a sensitive item has been stored on a hard drive for a long period, with ample opportunity for tampering.

Symmetric cryptography systems do not support enhanced proofs of data integrity. In public key systems, the *digital signature* is used to assure both that a sensitive document originated as represented, and also that it was not tampered with since origination. Before sending a particular communication, the issuer of the document creates a unique fingerprint of the document in its original form, which is encrypted and included in the transmission.

This "fingerprint" is the product of an algorithm called a *one-way hash function* — a special kind of encryption that is not intended to be decrypted. Rather, the hash function is designed to transform a document into a unique character string of fixed length, called a *digest*; changing even a single character in the original document will result in a different digest. When receiving a file that includes a digital signature, the receiver runs the same hash function on the received file; only an unaltered version will duplicate the digest.

Digital signatures offer strong **proof** that a file is **genuine** and **faithful** to the original form. This same quality allows digital signatures to play an important role in providing **non-repudiation** services.

Non-Repudiation

As organizations endeavor to transact commercial activities over the Internet, disputes will inevitably arise over the specifics of agreements and performance, just as they do in the non-electronic world. Devices such as postmarks, registered mail receipts and notarized documents — all of which exist to provide evidence of the performance of parties engaged in a business or legal transaction — have equivalents in cyberspace. The core issue is called *non-repudiation*; it is our ability to overcome the opponent's objection to or repudiation of the facts as we present them.

There are many facets to the issue of non-repudiation, though three issues stand out as most pressing.

- > Non-repudiation of *origin* — proving to the receiving party that the sender is genuine, and not an impostor. This demonstrates to a vendor, for example, that an electronic order is from a valid customer.
- > Non-repudiation of *submission* — an analog to the postmark, which proves that the sender not only created but *actually sent* something at a particular time.
- > Non-repudiation of *receipt* — proving that the other party received the sent communication. Other less common issues of non-repudiation relate to verifying the time and place of electronic communications.

At the simplest level, common e-mail programs offer some help. By sending a copy of an e-mail message to her or himself, one can generate some proof of both origin and submission. Requesting a return receipt from the receiver's e-mail server provides some proof of delivery. These vehicles will likely carry some weight in a legal dispute, but they are far from ironclad.

A higher level of assurance is available by using trusted third parties to verify these issues of origin, submission and receipt. Public key certificate authorities (CAs) can provide this kind of incontrovertible evidence by applying digital signatures to communications; the process differs somewhat depending on which form of proof is required.

For example, the holder of the private key that is matched to a digital certificate can request the CA's digital signature on a communication that is being created. The digital signature is encrypted with the CA's private key, attesting to the authenticity of the document and its creator, thus providing stronger proof of origin than a simple e-mail copy.

Proof of receipt is a similar process, played in reverse: the recipient creates a digitally-signed document via his or her CA stating that the message has been received. Proof of submission is essentially the same as proof of receipt, with the e-mail system certifying that it has received the message for transport.

Technologies for Managing Security

The task of managing security policy involves identifying the information security risks faced by the enterprise. However, it is still very common for organizations to be without either the ability to detect attempts at unauthorized access, or log suspicious activity. Many therefore find themselves without a paper trail when it comes time to confront an employee, or to prosecute the criminals behind unlawful or damaging acts.

As a first step, a *network security assessment* is usually advisable. A number of companies now offer “tiger team” or “samurai” services, where information security experts literally attempt to penetrate the corporate network. Some also use social engineering techniques, in order to assess the weakness of the human dimension of the security equation as well.

Security assessment software is also available. These tools perform a number of system checks, often including:

- > *Password cracking* and password strength checking, to identify vulnerable user passwords;
- > *Access control* checking, to identify user accounts with excess access privileges;
- > *User account restrictions*, to uncover dormant user accounts that could be countermanded by hackers;
- > *System vulnerability auditing*, to isolate and remove known system bugs which are often exploited by hackers;
- > *Data confidentiality checks*, to verify the effectiveness of privacy safeguards; and
- > *Virus checking*, to assess the vulnerability of network files to losses due to virus infection or power outage.

In addition to periodic security audits, *intrusion monitoring* software provides active, 24-hour surveillance and logging of suspicious activity. Some also provide real-time alerts to system managers via an audible alarm, pager, e-mail or other interactive technology. System managers define alarm conditions, which can include repeated failed login or file access attempts, browsing or curious users, excessive privilege granting, “ghost” user IDs and masquerading users, denial of service situations, and administrative ID abuse, among others. However, one of the weaknesses of monitoring software is that it is essentially reactive — focused on detecting breaches before they inflict damage — rather than preventative in nature. Monitoring tools should be used in conjunction with proactive audit tools.

STANDARDS IN SECURITY TECHNOLOGY

Once the network manager scratches the surface of security technology, he or she is bound to discover that the field can be exasperatingly complex. Acronyms abound, various technologies compete, and even relatively simple security concepts are often described in obscure and unfathomable ways. Adding to the confusion, a multiplicity of companies, workgroups and standards bodies are responsible for having created the foundations of today's security technology.

There is good news, however. The emergence of the Internet as the *sine qua non* of computing has had the important side effect of quieting much of the cacophony of competing security approaches. Now the landscape is a good deal simpler: technology companies that want to be in the game must play by the accepted rules of the Internet — which often come down to the rules of the Internet Engineering Task Force (IETF), the workgroup responsible for proposing the official standards and protocols used on the Internet. What follows is a brief look at the most important general-purpose information security standards that managers should be aware of as they begin considering various technology alternatives.

SSL: Making online commerce secure

The Secure Sockets Layer (SSL) handshake protocol was developed by Netscape Communications to provide security and privacy to Internet transactions. SSL is a "layer" in the sense that it is application independent: once an SSL session is begun, other protocols like HTTP and FTP can be layered on top of it transparently. It is a client-server approach that uses both public key and symmetric encryption to protect from eavesdropping information passed between systems.

The SSL handshake authenticates the server, although an optional client authentication phase is available. When a client requests a secure connection, the server responds by sending its digital certificate, which includes its public key. The client then generates a master symmetric encryption key, which is encrypted with the server's public key and sent back. The two parties have now agreed on a shared symmetric encryption method in full privacy. For added security, the second client authentication phase can be enacted: the server sends a challenge to the client, which must then authenticate itself to the server via its digital signature.

SSL has quickly emerged as one of the most popular security protocols in all of computing, and is now implemented widely in a number of areas outside the Internet due to its performance and ease of implementation. For more information on SSL, see http://www.rsasecurity.com/standards/protocols/ssl_tls.html.

IPSec: Building security into Internet connections

While SSL is a commercial solution designed to implement security on the Web, the independent IETF has created its own set of specifications for implementing cryptographically-based authentication, integrity and confidentiality services at the IP *datagram* layer. The work of the IPSec group defines the basis for interoperable, secure host-to-host and client-to-host connections known as VPNs. Where SSL allows two systems to communicate in a secure fashion over an *insecure* connection, with IPSec a *secured connection* is created between two systems.

Since IPsec is built into the network layer, any protocols operating at higher layers can transparently make use of encryption services. The IPsec protocol format includes an Authentication Header (AH) and an IP Encapsulating Payload (ESP), which are independent of specific cryptographic algorithms; the protocol allows either the ESP, or both AH and ESP to be encrypted. IPsec uses the Internet Key Exchange (IKE) framework for key management (formerly called ISAKMP/Oakley), which also supports multiple algorithms. More information on IPsec is available at <http://www.ietf.org/html.charters/ipsec-charter.html>.

S/MIME: Secure messaging

The Internet MIME (Multipurpose Internet Mail Extensions) specification allows for a standard means of attaching additional files such as pictures, audio and application files to basic e-mail text messages. S/MIME adds security features like digital signatures and encryption services to the MIME specification, thus allowing users to protect the privacy of e-mail communications and attachments. The syntax of S/MIME was derived from the Public Key Cryptographic Standards — specifically PKCS #7 — which define how interoperable public key systems should behave. More information on S/MIME is available at <http://www.rsasecurity.com/standards/smime>.

PKIX: The IETF defines interoperable Public Key Infrastructure

Public key technology, as discussed in this chapter and elsewhere in this document, provides important services for identification and authentication, privacy, integrity and non-repudiation. While public key systems can be implemented within an organization, greater benefits can be achieved when implemented between organizations. Thus, the PKCS standards were developed by RSA Data Security, Inc. — the originators of public key technology — in cooperation with a consortium that included Apple, Digital Equipment, Lotus, Microsoft, MIT and Sun, to foster the use of interoperable public key technology. More recently, the task of defining a standard, interoperable PKI approach has been taken up by the IETF with its PKIX workgroup.

The PKIX working group, whose goal is to foster use of public key security services over the Internet, has addressed multiple aspects of PKI, built on the X.509 standard which defines directory services and certificates. Thus, in addition to specifying fundamental mechanisms for encryption and describing the structure of public and private keys, certificates and digital signatures, PKIX has also addressed the management of certificates, protocols for addressing hosts, running a certificate authority, and issues of policy and administration. More information is available at <http://www.ietf.org/html.charters/pkix-charter.html>.

Other standards in information security

While the four standards discussed above form the foundation for most security systems, some additional standards and approaches bear discussion here.

CAPI — The term CAPI stands for Cryptographic API (Application Programming Interface), an interface to a library of functions that developers can use to implement security and cryptographic services in their software applications. There are a number of CAPIs available, including RSA's Cryptoki, NSA's Fortezza, GSS-API and others.

To some degree, however, the term CAPI has become synonymous with Microsoft's Crypto API, which has been put forth as an alternative to the PKCS #11 standard, which defines access to cryptographic and smart card credentials. Because of export requirements, this CAPI requires third-party cryptographic products to be submitted for Microsoft approval, and thus has not been widely implemented.

CDSA — The Common Data Security Architecture is an alternative CAPI, originally created by Intel and IBM for the UNIX environment, and now owned by the Open Group. This is an emerging security technology, which is gaining some degree of support.

GSS-API — The Open Group adopted the Generic Security Service API specification as a means for implementing security in distributed computing environments. Despite the fact that Version 2 of the GSS-API was included in Internet Proposed Standard RFC 2078, only a handful of vendors support this approach.

Kerberos — The Kerberos approach to user identification and access management is a security standard in the sense that it was one of the earliest access control systems designed for open networks, and is still widely used. Its advantages and weaknesses were discussed in the previous chapter; the fact that PKI offers a greater range of security services than Kerberos has led most information security practitioners to conclude that PKI is a more suitable approach for the future.

RADIUS — Livingston Enterprises (recently acquired by Lucent Technologies) developed RADIUS (Remote Authentication Dial-In User Service) to provide authentication, authorization and accounting services for remote access. The RADIUS protocol is now defined by the IETF 2138 and 2139 RFC specifications. The protocol operates on a client/server model, with a Network Access Server (NAS) operating as a client of the RADIUS server; the NAS interacts with users and passes user information to designated RADIUS servers, which perform user authentication and then return configuration information necessary to deliver services to the user. One of the strengths of RADIUS is that it enables central management of user passwords and account information.

RSA SecurID® — RSA SecurID® and RSA ACE/Server® together make up the world's leading two-factor authentication systems, and offer the broadest compatibility with networking equipment. In addition to authenticating access via remote log-in, the system can also be used to protect local LAN access, implement secure extranet solutions, protect administrative consoles, and provide strong authentication for comprehensive PKI solutions.

SET — Visa and Mastercard have jointly developed the Secure Electronic Transaction (SET) protocol as a method for secure, cost-effective bankcard transactions over open networks. SET includes protocols for purchasing goods and services electronically, requesting authorization of payments, and requesting credentials (certificates), among others. Recently developed, SET is being promoted as an open specification for the industry, which may be used by software vendors to develop applications; it has yet to achieve wide adoption.

TACACS+ — An acronym for Terminal Access Controller Access Control System, TACACS and the enhanced TACACS+ were created by Cisco Systems as a means to centrally validate users attempting to gain access to a router or access server. The protocol provides detailed accounting information, and flexible administrative control over authentication and authorization processes.

SUMMARY

Perhaps more than any other factor, the rise of Internet-based electronic commerce has accelerated the evolution of information security technology over recent years. This path of evolution is certain to continue, as more organizations seek to automate more transactions with their customers, suppliers and partners.

The fundamental tasks of information security, however, are unchanging: to provide authentication, user identification, data privacy, data integrity and non-repudiation of communications and transactions. We believe that advances in security technology will enable electronic commerce to flourish, providing services that are faster and more convenient for users, while more straightforward for organizations to implement.

It is our hope that this Guide proves valuable to its users in understanding and adopting information security technology — both today, and in the future.

ABOUT RSA SECURITY INC.

RSA Security Inc., the most trusted name in e-security, is focused on strong authentication, encryption and public key management systems that help organizations conduct e-business with confidence. RSA Security has the unrivaled technical experience and proven leadership to address the changing security needs of e-business and to bring trust to today's online economy. Today, there are more than 5 million users of RSA SecurID user authentication systems, and more than 450 million copies of RSA BSAFE encryption technologies installed worldwide. The Company's RSA Keon family of interoperable, standards-based PKI products help organizations manage digital certificates to ensure authenticated, private and legally binding electronic communications and transactions.

GLOSSARY

3DES

See *Triple-DES*.

ACL (Access Control List)

An organization's central listing of security privileges granted to each employee.

Algorithm

A complex mathematical function; used to *encrypt* and *decrypt* private information.

ANSI (American National Standards Institute)

The organization that created the *DES* standard.

API

Application Programming Interface; a set of programming rules used to create or modify application code.

Applet

A small program written in Sun Microsystems' Java language; can function as a *Trojan horse virus*.

Application-level firewall

A *firewall* system that operates on the application layer; used to readdress outgoing Internet traffic in order to shield private IP addresses.

Application security

Security enforced by individual software applications, rather than at a global network level.

Asymmetric encryption

A *cryptographic* approach that uses one *key* to *encrypt* a message, and a different key to *decrypt* the message; the foundation of *Public Key Infrastructure*. Compare to *symmetric encryption*.

Attack

An attempt to access or destroy private information, communication or resources by an unauthorized party; the actualization of a *threat*.

Audit

The process of assessing an organization's security policies and systems.

Authentication

The process of verifying the identity of an individual or system.

Authentication server

A server that provides authentication services on a network.

Authentication token

A device issued to authorized individuals which generates a code used to provide proof of their identity in a *two-factor authentication* system; can be a *hardware token* or a *software token*. Also called an "authenticator".

Authorization

The granting of appropriate access privileges to authenticated users.

Availability

The uptime of a computer system; some *hacker* attacks are designed to eliminate the availability of a key system.

Backdoor

An undocumented or illicit entry point into a protected system, often created by the system programmer, or installed by a successful *hacker*.

Bastion host

A security system, such as a *firewall*, placed between two networks; serves as a first line of defense.

Belt and suspenders

Use of redundant security systems, such as a *bastion host*, to strengthen information security.

Biometrics

User *authentication* based on unique physical characteristics, such as fingerprints, *retinal scans*, voice print, *hand geometry* or others.

Block cipher

An *encryption* approach (like DES) which breaks information into blocks of fixed size; compare to *stream cipher*.

Boot control

Preventing access to a PC until the correct *password* (or other security method) is supplied.

Breach

A successful *attack* against protected information or resources.

Broadcast revocation list

A push method for communicating revoked certificates in a *public key* system.

Broadcast storm firewall

A *firewall* system used to stop broadcast storm attacks, where multicast *packets flood* a network.

Browser

Software such as Netscape Navigator or Microsoft Internet Explorer, used to view Web pages on the Internet or company *intranet*.

Brute force

A hacking technique that uses sheer repetition rather than logic to overcome protection; used to test *password* alternatives, or to locate active modem lines.

CA

See *Certificate authority*

Callback

A security approach where a *remote access* connection to a private network can only be made when the internal server originates the call to a pre-approved phone number.

CAPI (Cryptographic Application Programming Interface)

A standardized way of programming security features into systems.

CDSA

A CAPI developed by Intel and IBM, and now owned by the Open Group; an emerging security programming standard.

Cert

A *digital certificate*.

Certificate

A data structure used in a *public key* system to bind a particular, authenticated individual to a particular *public key*.

Certificate authority (Also CA)

In a *public key* system, the trusted party that vouches for the authenticity of the individual or system in question, by issuing *certificates* or *digital signatures*.

Certificate revocation list (Also CRL)

The certificate authority's listing of invalidated certificates. Revocation can be due to time lapse, employment change, theft of private key, or other reason.

CHAP Challenge

Handshake Authentication Protocol; a log in protocol for dial-up connections that includes *challenge/response* capabilities.

Challenge/Response

An *authentication* approach where the *authentication server* provides a message (the challenge) which the user must process and enter correctly (the response) to prove identity.

Cipher (or ciphertext)

Information which has been *encrypted* into seemingly meaningless code.

Clear

Communications that are not *encrypted* are said to take place "in the clear."

Cleartext

A message that has not been *encrypted*.

Confidentiality

Limiting the communication of private content to known, authorized parties.

Crack

To overcome *password* protection or *encryption*. Crack is also the name of a popular password-breaking utility.

Cracker

Hacker term for a "principled hacker"; compare to *hacker*.

CRL

See *Certificate revocation list*.

Cryptography

The science of translating information into an indecipherable code, rendering it privy only to authorized parties.

Datagram

In an *IP* transmission, the body of the message, which follows a header.

Data integrity

Proof that a file or communication has been unchanged since origination.

DCE (Distributed Computing Environment)

The internetworked application environment defined by the Open Software Foundation (now called the *Open Group*).

Decryption

The rendering of ciphertext back into its original plaintext version.

Denial of service

A *hacker attack* designed to shut down or overwhelm a critical system, such as an *authentication server* or *Web server*.

DES (Data Encryption Standard)

The most common *symmetric encryption* method. Provides fast processing, and thus is often used with *asymmetric encryption* methods to encrypt lengthy text.

Dial-up

A *remote access* connection to a company network via a telephone line and modem.

Diffie-Hellman key agreement

An approach wherein two parties can communicate in *cleartext* to agree on a key for use in *symmetric encryption*, without compromising the secrecy of the key itself.

Digest

A scrambled piece of data produced by a *one-way hash function*, which serves as a unique fingerprint of an original document; used in a *digital signature* to provide assurance of *data integrity*.

Digital certificate

A data structure used in a *public key system* to bind a particular, authenticated individual to a particular *public key*.

Digital signature

A technique for proving that a message has not been tampered with, using *public key cryptography*. Example: a hashed *digest* of a message is created, *encrypted* with the sender's *private key*, and included with the message itself (in essence, attaching a secret fingerprint of the original file). The recipient uses the sender's *public key* to *decrypt* the digest, which is then compared with a hash digest of the actual message received.

Directory

In *public key cryptography*, a look-up table of user names and public keys based on standards such as *X.509* or *SPKI*.

Distinguished name

In *public key cryptography*, the concept that each individual must have a unique name in the directory.

DSA (Digital Signature Algorithm)

An *algorithm* for use in *digital signatures* as defined by *NIST* in its Digital Signature Standard (DSS).

DSS (Digital Signature Standard)

A standard for *digital signatures* defined by *NIST*.

Dumpster diving

The method of gathering private information by searching through trash.

Dynamic authentication server

An *authentication server* that supports *one-time use passwords*.

Elliptic curve algorithm

An alternative to the *RSA* algorithm and *DSA* for generating *digital signatures*; an elliptic curve is a more difficult mathematic problem to solve, giving a stronger cryptographic result with a shorter *key*.

Encryption

Translating information into *ciphertext*, rendering it privy only to authorized parties.

Encryption algorithm

The mathematical formula used to *encrypt* information; based on the idea that factoring down a very large number (thousands of digits) is much more difficult than the task of generating it.

ESP (Encapsulating Security Payload)

Encryption of an *IP datagram*. See also *IPsec*.

Event detection

The information security approach which focuses on detecting attempted break-ins as a means of enhancing security measures and policy.

Extranet

Making information on a *private network* available to authorized parties outside the organization, using Internet technology.

Firewall

A system for isolating and protecting networks; typically used to prevent Internet-based users from *breaching* a *private network*.

Flooding

Overwhelming a system with incoming messages or hits to render it unavailable.

GSSAPI (Generic Security Services API)

A standard for implementing security services in software that allows applications to pass user credentials between them, without forcing re-authentication.

Hacker

A person who attempts to bypass computer security systems.

Hand geometry

A *biometric authentication* approach, based upon recognizing unique characteristics of an individual's hand; less intrusive than *retinal scanning* or other biometric techniques.

Hardware token

A code-generating device, often the size of a credit card, that an authorized user carries to provide *authentication* when logging on to a secure network or application.

Hash code

A short piece of *ciphertext* created by a one-way hash algorithm; provides a unique fingerprint of the total keystrokes in a document, without the need to decrypt.

Hash function

Also *one-way hash algorithm*; the mathematical formula that turns a text block into a unique block of ciphertext of a fixed length.

Hijack

To interrupt and take control of an existing connection session, without the knowledge of one party. Also called "session hijacking."

HTTPS

Secure Sockets Layer (SSL) encryption used in a Web browser.

IAB (Internet Activities Board)

The body responsible for coordinating the engineering, design and management of the Internet. Its two major task forces include the *IRTF*, for long-term research and design, and the *IETF*, for shorter-term engineering issues.

IDEA (International Data Encryption Algorithm)

A *symmetric encryption* standard popular in Europe.

Identification

A computer's recognition of a unique individual, through user name, *certificate* or other factor.

Identity-based policy

Security policy based on defining security privileges for all individuals in an organization; compare with *role-based policy*.

IESG (Internet Engineering Steering Group)

The leadership body of the *IETF*, which recommends standards for the Internet.

IETF (Internet Engineering Task Force)

The body responsible for deciding on short-term engineering issues for the Internet. Compare with *IRTF* and *IESG*.

IKE

Part of the IPsec protocol; specifies how compliant devices share a *public key* when creating an encrypted *tunnel*. Formerly called ISAKMP/Oakley.

Information security

An approach to network security which emphasizes securing individual information and applications, rather than just network connection points such as RAS servers and *routers*.

Infrastructure

The hardware, software and firmware assets used to provide network services.

Insider

For information security purposes, a *threat* arising from within the organization.

Integrity (Data integrity)

Refers to a duplicate or transmitted version that bears fidelity to the original in every way.

Integrity check-value

A value calculated from the contents of a message, used in a symmetric key system to verify that the original message was not tampered with; compare to *digital signature*.

Internet

The global public computer network built on the IP protocol.

Intranet

The use of Internet technology (especially browsing) on a *private network*.

IP (Internet Protocol)

The protocol used on the *Internet* to define connections between computers.

IPRA (Internet Policy Registration Authority)

The top-level *certificate authority* used in the Privacy Enhanced Mail (*PEM*) system.

IPsec (Pronounced "I-P sec.")

A set of protocols being developed by the *IETF* to build enhanced security features into the IP layer; used to implement secure connections, such as *VPNs*. See also *IKE*, *transport mode* and *tunnel mode*.

IP spoofing

A *hacker* trick which involves using a false *IP* address to gain access to protected resources; UNIX systems often use an incoming IP address as a form of *authentication*.

IRTF (Internet Research Task Force)

The body responsible for recommending long-range technical alternatives for the *Internet*.

ISO (International Organization for Standardization)

The standards body that defined the seven-layer Open Systems Interconnect (OSI) reference model for internetworking, among others.

ISP (Internet Service Provider)

A company that supplies *Internet* access or other networking services to individuals or organizations.

Issuing authority (also IA)

Synonymous with *certificate authority*.

ITU (International Telecommunication Union)

The United Nations agency known for creating the *X.500 directory* standard. Its CCITT committee was responsible for recommending numerous telecommunications standards.

KEA (Key Exchange Algorithm)

A public means of agreeing on a *symmetric encryption key* without compromising its secrecy. A U.S. government classified implementation of the *Diffie-Hellman key agreement*, used for military messaging.

Kerberos

A client-server *authentication* and *authorization* system developed by MIT in the late 1970s; uses *symmetric encryption*.

Key

The secret used to *encrypt* or *decrypt ciphertext*; the security of encryption depends on keeping the key secret.

Key pair

The two *keys* generated in *asymmetric encryption*; whatever one key encrypts, the other decrypts. Often used as *public* and *private keys* in PKI.

L2F (Layer 2 Forwarding)

Cisco Systems' enhancement of PPP designed to enable *VPNs*. Merged with *PPTP* to create *L2TP*.

L2TP (Layer 2 Tunneling Protocol)

An enhancement to PPP, created by the combination of Microsoft's *PPTP* and Cisco's *L2F*, to enable secure connections (or *tunnels*) between points on the Internet.

LDAP (Lightweight Directory Access Protocol)

A simplified implementation of X.500 standards which is compatible with TCP/IP networks.

MAC (Message Authentication Code)

A function which transforms a variable-length input, using a secret key, to produce a unique fixed-length output which serves as a kind of fingerprint for the original file. MACs can be *hash functions*, *stream ciphers* or *block ciphers*.

Man in the middle

A *hacker attack* where the hacker positions himself between two unsuspecting parties in a communication session.

Masquerade

A *hacker attack* where the hacker fraudulently assumes the identity of another person.

Message digest

The *ciphertext* of a sensitive message generated by a *hash function*, used to verify the *integrity* of that communication.

MD5

A *hash function* developed by RSA Laboratories.

MIME (Multipurpose Internet Mail Extensions)

The standards for attaching additional files or information to e-mails.

Modulus

The integer used in cryptosystems as the base of cryptographic transforms.

Non-repudiation

The inability to deny actions. *Non-repudiation of delivery* prevents a recipient from denying receipt of a message; *non-repudiation of origin* prevents the creator from denying that he or she wrote the message; *non-repudiation of submission* provides proof of the time and date the message was sent.

One-time password

A system where a password is valid for only one login, changing in a pattern known only to the authorized individual and security server.

One-way function

A cryptographic function designed to transform source data into apparently unmeaningful data; the resulting *ciphertext* is unique, and not meant to be decrypted.

Open Group

The industry association that manages open standards in UNIX computing. Formerly called the Open Software Foundation.

OSI

The industry association that formalized the seven-layer model used in TCP/IP.

OTP (One-Time Password)

A particular implementation of a single-use password scheme for use over unsecured networks, where the actual password does not traverse the network.

PAC (Privilege Attribute Certificate)

In PKI-based *Single Sign-On* systems, a *digital certificate* that contains a user's privileges. Accompanies an X.509 certificate which proves identity.

Packet

In telecommunications, a recognizable parcel of information that traverses telephone lines or networks.

Packet filtering

An approach used by some *firewalls* to prevent illegal access based on attributes of the transmitted *packets*.

Packet switching

A technology for managing network traffic where messages are broken up into small packets; prevents individual sessions from monopolizing network bandwidth.

Passive attack

A *hacker* attack that does not involve active participation on the part of the hacker; network *sniffing*, for example.

Password cracking

The guessing or decrypting of valid passwords.

PAP (Password Authentication Protocol)

A popular protocol for enforcing password protection.

Perimeter

The physical bounds of a private network, as defined by routers and RAS ports.

PGP (Pretty Good Privacy)

An *encryption system* marketed by Network Associates.

PIN

Personal Identification Number.

PKCS (Public Key Cryptography Standards)

A set of *public key* standards created by RSA Laboratories and a consortium of technology companies in order to propagate the adoption of public key technology.

PKI (Public Key Infrastructure)

A system that uses *asymmetric encryption* to provide proof of identity, data privacy, non-repudiation and data integrity. *Digital certificates* and *digital signatures* are PKI elements.

PKIX

The *IETF* working group that articulates *public key* standards for use on the *Internet*.

Plaintext

Non-encrypted messages or data.

Policy

Business rules used to guide employee actions; security policy sets the framework for security technology.

Port

A physical or logical connection point; a single router can support many logical connection ports at one time.

PPTP (Point to Point Tunneling Protocol)

A connection protocol developed by Microsoft and the PPTP Forum, which provides for encrypted *VPN* connections. Merged with Cisco's *Layer 2 Forwarding (L2F)* to create *Layer 2 Tunneling Protocol (L2TP)*.

Private key

In *asymmetric encryption* or PKI, the confidential *encryption key* held privately by the user. The private key can be used to encrypt a message, which provides proof of authentic message creation when decrypted by the corresponding public key; because the private key can also be used to *decrypt* a message, it protects the privacy of incoming communication from others, who use the *public key* to encrypt messages.

Private network

A network owned by a business or organization, and built on private data connection media; compare to the *Internet*.

Profile

Security administrator's data on an individual user, typically including name, location and access rights.

Protocol

An agreed-upon set of interactions which structure a computer interchange.

Proxy

A computer that takes the place of another; used for example by certain *firewall* systems to isolate host computers from outsiders.

Public key

In *asymmetric encryption* or PKI, the *encryption key* posted publicly for communicating securely with the holder of a *private key*. The public key can be used to decrypt a message created by the user's private key, which provides proof of authentic message creation; the user's public key can be used to encrypt a private message for only that recipient.

Public network

A computer network such as the Internet, which is not privately owned and managed.

RADIUS

Remote Authentication Dial-In User Service software originated by Livingston Technologies used to manage users and passwords centrally.

RAS (Remote Access Server)

A device used to establish a dial-up connection to a network.

RC2, RC4, RC5

Ciphers created by Ron Rivest for RSA Security.

Realm

A sub-portion of an enterprise network, for administrative purposes.

Relative distinguished name

In *X.500*-based directory services, the concept of defining individuals so that each — even multiple people with the same name — have a unique entry.

Remote Access

The ability to dial-in to a private network via a modem and telephone line.

Replay

A *hacker* trick of capturing an *encrypted password* and using it later to establish a fraudulent connection; including a timestamp in the passcode eliminates this risk.

Repudiation

To deny an asserted set of facts. Compare with *non-repudiation*.

Retinal scan

A *biometric authentication* approach that meters features of the retina of the eye.

Reversible cryptosystem

A *cryptographic* technique that involves both *encrypting* and *decrypting* information; compare with *one-way hash function*.

RFC (Request For Comments)

The *IETF* document that states agreed-upon standards.

Rogue

A person or system that behaves outside the scope of its authority.

Role-based policy

An approach which defines access privileges based on belonging to a particular role or class of employee; compare to *identity-based policy*.

Root-level authorization

The most far-reaching network access privileges, typically granted only to system administrators.

Router

A device for managing traffic between networks.

RSA

The first public key cryptosystem, patented in 1983.

Samurai

A technology expert hired to test security systems protecting a network.

Sandbox

A Java *applet* that behaves in a rogue manner is said to be “outside the sandbox,” or exhibiting the possibility of being a *virus* or *Trojan Horse*.

SATAN (Security Administrator’s Tool for Analyzing Networks)

Administrative software designed to *scan* a network for security weaknesses.

Scan

A security auditing technique which involves automated testing of all systems for typical weaknesses.

Screening router

A router which screens traffic based on packet content.

SDSI (Simple Distributed Security Infrastructure)

A proposal produced by Ron Rivest and Butler Lampson in 1996 to create a simple alternative to *X.509*.

Secure

Free from vulnerabilities.

Security domain

Range of network infrastructure that a specific administrator or security server has authority over.

SESAME

A *single sign-on system* that is widely used in Europe.

Session encryption

Encryption that is used for the duration of a communication session, such as during a secure connection to a Web server using SSL.

Session hijacking

A *hacker* approach of *masquerading* as one party in an existing communications session.

SET (Secure Electronic Transaction)

A security approach developed by Visa and MasterCard to protect credit card transactions.

Shared secret

The key used in *symmetric cryptography*.

S-HTTP

A security extension to HTTP designed to allow *authentication*, *integrity*, and *confidentiality* services.

Signature scanning

A *virus*-detection method which scans incoming files for code segments characteristic of known viruses.

S/KEY

A *one-time password* system developed by Bellcore; evolved into *OTP*.

SKIP (Simple Key management for IP)

A security approach implemented at the IP level. The *IETF* instead chose the rival *IKE* protocol for inclusion in *IPsec*.

SKIPJACK

The *block cipher* used in the Clipper chip designed by the NSA.

Smart card

A credit card-like device with both memory and CPU built-in, used to store personal credentials or other information; can be used for *authentication* purposes.

S/MIME (Secure MIME)

The *IETF* specification that defines a framework for the *encryption* and/or digital signing of an electronic message, or part of a message.

Sniffing

The use of monitoring software to capture private information off of a network.

SPKI (Simple Public Key Infrastructure)

An *IETF* effort to create a simplified subset of *PKI* protocols.

SNMP (Simple Network Monitoring Protocol)

The protocol by which network devices communicate with a monitoring agent.

Snooping

A hacker attack that involves logging onto a private network or server and seeing what's there.

SSL (Secure Sockets Layer)

A technique developed by Netscape for creating an *encrypted* communication session between two computer applications, using *public key* technology.

Social engineering

A hacker term for gaining access credentials or other secret information by tricking people, rather than through technologic means.

Soft token

Also software token; a software utility that generates login codes for two-factor *authentication systems*.

SSO, SSSO (Single Sign-On and Secure Single Sign-On)

A systematic approach for providing access right that prevents users from redundant logons.

Stream cipher

A *symmetric encryption* technique that operates on one bit of data at a time; compare to *block cipher*.

Symmetric encryption

An approach that uses the same algorithm or key to both encrypt and decrypt information; compare to *asymmetric encryption*.

Threat

A recognized security risk; compare to attack.

Ticket

In the *Kerberos* system, a protected data item presented to an authenticated user that grants privileges with target servers; comparable to a *PAC* (privilege attribute certificate) in a *public key system*.

Tokencode

The numeric code generated each minute by a hardware or software token for purposes of strong, *two-factor authentication*.

Transform

A mathematical term for applying a complex function or algorithm to a starting value; the result is called a "transform."

Transport mode

IPsec encryption mode where the payload is encrypted, leaving the header intact; compare with *tunnel mode*.

Trapdoor

Secret information that, if known, can be used to easily decrypt information.

Triple-DES

A technique used to make *DES encryption* stronger; a given message is encrypted three times using multiple DES keys.

Trojan horse

A *hacker attack* wherein a damaging item (such as a *virus* or *back door*) is hidden in an innocent-looking file.

Trust

In security technology, the definition of the relationship between two parties or computers, wherein certain rights or privileges are granted to the trusted party.

Trusted third-party

The reliance on a third party, such as a *certificate authority*, to vouch for the identity of one or both members in a transaction.

Tunnel

A connection between computers that enforces the secrecy of communications; used to create *VPNs*.

Tunnel mode

IPsec encryption mode where the entire message, including both header and payload are encrypted; more secure than *transport mode*.

Two-factor authentication

Stronger-than-password authentication that is based on the presence of two factors: something the user knows (such as a PIN), and something the user has.

VeriSign

Vendor of a *PKI system*, and *certificate authority*.

Virus

A program designed to secretly infect other computer systems.

Virtual Private Network

The use of an *encrypted tunnel* over a *public network*, to provide privacy on par with a *private network*.

VPN

See *Virtual Private Network*.

Web spoofing

Masquerading as a valid Web site; generally used to defraud visitors or make political statements.

Worm

A computer *virus* that, once introduced, replicates itself into multiple files and systems.

X.3.92

The 1980 *ANSI* specification which standardized *DES*.

X.400

The ISO/ITU standard which defines e-mail addressing.

X.500

Generically, the *ANSI* standards which define *directory services*, including *digital certificates*.

X.509

The standard which defines the *digital certificate*.

Zero-knowledge technique

A *cryptographic* system where proof of *authenticity* is made by proving that one is in possession of certain information, without revealing any of the information itself.

ADDITIONAL INFORMATION RESOURCES

Those interested in learning more about information security can find a host of resources on the Web. For general information, two of the best sites are the Internet Engineering Task Force (<http://www.ietf.org>) and RSA Security (<http://www.rsasecurity.com>). The IETF site gives specific information on Internet initiatives, workgroup charters (such as PKIX and IPSEC), and the RFCs which define Internet standards. The RSA Security site includes a number of excellent white papers and backgrounders on topics like SSL, S/MIME and VPNs, as well as a comprehensive FAQ that covers a wide range of security topics.

Information on specific security systems and technologies is available at the commercial sites of product vendors. For more information on authentication technologies, see the RSA Security Web site (<http://www.rsasecurity.com>); the Cisco Systems site has information on TACACS, and Lucent features white papers on RADIUS. VeriSign and RSA Security offer information on their PKI solutions, as well as background information on topics like digital certificates, digital signatures and more. Vendors of firewalls, VPN systems, routers and switches all offer information on their respective technologies.

Industry associations and institutions are also good sources of information. For more on SET, the credit card security standard, see <http://www.setco.org>. The Smart Card Forum has a Web site at <http://www.smartcrd.com>. The FBI offers some statistics on computer crime (<http://www.fbi.gov>), and MIT maintains a Web site of information on Kerberos at <http://web.mit.edu/kerberos>.

There are also a number of books available on information security topics. Two books that offer a comprehensive overview and also depth of coverage are *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption*, Prentice Hall PTR, Upper Saddle River, NJ; and *Intranet Security*, Charles River Media, Inc., Rockland, Mass.



RSA Security Inc.
20 Crosby Drive
Bedford, MA 01730 USA
Tel (US) 1 877 RSA 4900, +1 781 301 5000
Fax +1 781 301 5170

www.rsasecurity.com

RSA Security Ireland Limited
Bay 127, Shannon Free Zone
Shannon, County Clare, Ireland
Tel +353 61 72 5100
Fax +353 61 72 5110

www.rsasecurity.ie

ACE/Server, SecurID and BSAFE are registered trademarks, and RSA and Keon are trademarks of RSA Security Inc.

All other trademarks are the property of their respective owners.

©1999 RSA Security Inc. All rights reserved.

ST-GD-0999