E-Business Environment and Architecture

Content

Part II

Chapter 5 Security Issues

1. **Introduction to e-Business Technology**
2. **Introduction to HTML**
3. **Introduction to XML**
4. **Interoperability & Standards**
5. **Security Issues**

Learning Objective

- Understand the basic concepts of security.
- Recognize public-key/private-key cryptography.
- Learn about popular security protocols, such as SSL and SET,
- Understand digital signatures, digital certificates and certification authorities,
- Become aware of various threats to secure systems, such as viruses and denial-of-service attacks.
- Understand emerging security techniques, such as biometrics and steganography.

5.1. Introduction

The explosion of e-business and c-commerce is forcing businesses and consumers to focus on Internet security. Consumers are buying products, trading stocks and banking online. They are providing their credit-card numbers, social-security numbers and other highly confidential information through Web sites. Businesses are sending confidential information to clients and vendors over the Internet. At the same time, we are experiencing increasing numbers of security attacks. Individuals and organizations are vulnerable to data theft and hacker attacks that can corrupt files and even shut down e-businesses. Security is fundamental to e-business.

Modern computer security addresses the various problems and concerns of protecting electronic communications and maintaining network security. There are four fundamental requirements of a successful, secure transaction: *privacy, integrity, authentication* and *non-repudiation.*

- *The privacy* ***issue*** *is the following:* How do you ensure that the information you transmit over the Internet has not been captured or passed on to a third party without your knowledge?

- *The integrity issue is the following:* How do you ensure that the information you send or receive has not been compromised or altered?

- *The authentication issue is the following:* How do the sender and receiver of a message prove their identities to each other?

- *The non-repudiation issue is the following:* How do you legally prove that a message was sent or received?

In addition to these requirements, network security addresses the issue of *availability:* How do we ensure that the network and the computer systems to which it connects will stay in operation continuously?

5.2. Ancient Ciphers to Modern Cryptosystems

The channels through which data pass over the Internet are not secure; therefore, any private information that is being passed through these channels must be protected. To secure information, data can be encrypted. *Cryptography* transforms data by using a key—a string of digits that acts as a password—to make the data incomprehensible to all but the sender and the intended receivers. Unencrypted data are called *plaintext;* encrypted data are called *cipher-text.* Only the intended receivers should have the corresponding key to decrypt the cipher-text into plaintext. A *cipher* or *cryptosystem* is a technique or algorithm for encrypting messages.

Cryptographic ciphers were used as far back as the time of the ancient Egyptians. In ancient cryptography, messages were encrypted by hand, usually with a method based on the alphabetic letters of the message. The two main types of ciphers were *substitution ciphers* and

transposition ciphers. In a substitution cipher, every occurrence of a given letter is replaced by a different letter: for example, if every "a" is replaced by a "b," every 'b" by a "c," etc., the word "security" would encrypt to "tfdvsjuz" In a transposition cipher. the ordering of the letters is shifted; for example, if every other letter, starting with "s,' in the word "security" creates the first word in the cipher-text and the remaining letters create the second word in the cipher-text, the word "security" would encrypt to "scrt euiy" Complicated ciphers were created by combining substitution and transposition ciphers. For example, using the substitution cipher first, then the transposition cipher, the word "security" would encrypt to "tdsu fvjz" The problem with many historical ciphers is that their security relied on the sender and receiver to remember the encryption algorithm and keep it secret. Such algorithms ("algorithm" is a computer science term for "procedure") are called *restricted algorithms.* Restricted algorithms are not feasible to implement among a large group of people.

Modern cryptosystems are digital. Their algorithms are based on the individual *bits* of a message rather than letters of the alphabet. A computer stores data as a *binary string,* which is a sequence of ones and zeros. Each digit in the sequence is called a bit. Encryption and decryption keys are binary strings with a given *key length.* Longer keys have stronger encryption: it takes more time and computing power to "break the code."

5.3. Secret-key Cryptography

In the past, organizations wishing to maintain a secure computing environment used symmetric *cryptography,* also known as *secret-key cryptography.* Secret-key cryptography uses the same symmetric secret key to encrypt and decrypt a message. In this case, the sender encrypts a message using the symmetric secret key, then sends the encrypted message and the symmetric secret key to the intended recipient. A fundamental problem with secret-key cryptography is that before two people can communicate securely, they must find a way to exchange the symmetric secret key and securely. One approach is to have the key delivered by a courier, such as a mail service or Federal Express. While this approach may be feasible when two individuals communicate, it is not efficient for securing communication in a large network, nor can it he considered completely secure. The privacy and the integrity of the message could be compromised if the key is intercepted as it is passed between the sender and the receiver over unsecured channels. Also, since both parties in the transaction use the same key to encipher and decipher a message, you cannot authenticate which party created the

message. Finally, to keep communications private with each receiver, a different key is required for each receiver, so organizations could have huge numbers of symmetric secret keys to maintain.

An alterative approach to the key-exchange problem is to have a central authority, called a *key distribution center (KDC).* The key distribution center shares a (different) symmetric secret key with every user in the network. In this system, the key distribution center generates a *session key* to be used for a transaction. Next, the key distribution center distributes the session key to the sender and receiver, encrypted with the symmetric secret key they each share with the key distribution center, For example, say a merchant and a customer want to conduct a secure transaction, The merchant and the customer each have unique symmetric secret keys they share with the key distribution center. The key distribution center generates a session key for the merchant and customer to use in the transaction. The key distribution center then sends the session key for the transaction to the merchant, encrypted using the symmetric secret key the merchant already shares with the center. The key distribution center sends the same session key for the transaction to the customer, encrypted using the symmetric secret key the customer already shares with the key distribution center. Once the merchant and the customer have the session key for the transaction, they can communicate with each other, encrypting their messages using the shared session key.

Using a key distribution center reduces the number of courier deliveries (again, by means such as mail or Federal Express) of symmetric secret keys to each user in the network. In addition, users can have a new symmetric secret key for each communication with other users in the network, which greatly increases the overall security of the network. However, if the security of the key distribution center is compromised, then the security of the entire network is compromised.

5.4. Public-key Cryptography

Public- key cryptography is asymmetric. It uses two inversely related keys: a *public* key and a *private key.* The private key is kept secret by its owner. The public key is freely distributed. If the public key is used to encrypt a message, only the corresponding private key can decrypt it**,** and vise versa. Each party in a transaction has both a public key and a private key. To transmit a message securely, the sender uses the receiver's public key to encrypt the message.

The receiver decrypts the message using his or her unique private key. No one else knows the private key, so the message cannot be read by anyone other than the intended receiver; this system ensures the privacy of the message. The defining property of a secure public—key algorithm is that it is computationally infeasible to deduce the private key flora the public key. Although the two key's are mathematically related, deriving one from the other should take enormous amounts of computing passer and time, enough to discourage attempts to deduce the private key. An outside patty cannot participate in communication without the correct keys. Thus, the security of the entire process is based on the secrecy of the private keys. If a third party obtains the decryption key, then the security of the whole system is compromised. If the integrity of a system is compromised, you can simply change the key, instead of changing the whole encryption or decryption algorithm.

Either the public key or the private key can he used to encrypt or decrypt a message. For example, if a customer uses a merchant's public key to encrypt a message, only the merchant can decrypt the message, using the merchant's private key. Thus, the merchant's identity can be authenticated, since only the merchant knows the private key. However, the merchant has no way of validating the customer's identity, since the encryption key the customer used is publicly available.

If the decryption key is the sender's public key' and the encryption key is the sender's private key, the sender of the message can he authenticated. For example, suppose a customer sends a merchant a message encrypted using the customer's private key. The merchant decrypts the message using the customer's public key. Since the customer encrypted the message using his or her private key, the merchant can be confident of the customer's identity. This systems works as long as the merchant can be sure that the public key with which the merchant decrypted the message belongs to the customer, not a third party posing as the customer.

These two methods of public-key encryption can actually be used together to authenticate both participants in a communication. Suppose that a merchant wants to send a message securely to a customer so that only the customer can read it, and suppose also that the merchant wants to provide proof to the customer that the merchant (not an unknown third party) actually sent the message. First, the merchant encrypts the message using the customer's public key. This step guarantees that only the customer can read the message. Then the merchant encrypts the result using the merchant's private key, which proves the

identity of the merchant. The customer decrypts the message in reverse order. First, the customer uses the merchant's public key. Since only the merchant could have encrypted the message with the inversely related private key. This step authenticates the merchant. Then the customer uses the customer's private key to decrypt the next level of encryption. This step ensures that the content of the message was kept private in the transmission, since only the customer has the key to decrypt the message.

The most commonly used public-key algorithm is *RSA,* an encryption system developed by Ron Rivest, Adi Shamir and Leonard Adleman in 1977. These three MIT professors founded *RSA* Security, Inc., in 1982. Today, their encryption and authentication technologies are used by most Fortune 1000 companies and leading e-commerce businesses. With the emergence of the Internet and the World Wide Web, their security work has become even more significant and plays a crucial role in e-commerce transactions. Their encryption products are built into hundreds of millions of copies of the most popular Internet applications, including Web browsers, commerce servers and e-mail systems. Most secure e-commerce transactions and communications on the Internet use RSA products. For more information about RSA, cryptography and security, visit www.rsasecurity.com.

Pretty Good Privacy (PGP) is a public-key encryption system used to encrypt e-mail messages and files. It is freely available for noncommercial use. PGP is based on a "web of trust;" each client in a network can vouch for another client's identity to prove ownership of a public key. The "web of trust" is used to authenticate each client. To learn more about PGP and to download a free copy of the software, go to the MIT Distribution Center for PGP, at web.mit.edu/network/pgp.html.

5.5. Key Agreement Protocols

A drawback of public-key algorithms is that they are not efficient for sending large amounts of data. They require significant computer power. which slows down communication. Thus, public-key algorithms should not be thought of as a replacement for symmetric secret-key algorithms. Instead, public-key algorithms can be used to allow two parties to agree upon a key to be used for symmetric secret-key encryption over an un-secure medium. The process by which two parties can exchange keys over an un-secure medium is called a *key agreement protocol.* A *protocol* sets the rules for communication: Exactly what encryption algorithm(s) is (are) going to be used?

The most common key agreement protocol is a *digital envelope*. Using a digital envelope, the message is encrypted using a symmetric secret key, and then the symmetric secret key is encrypted using public-key encryption. For example, a sender encrypts a message using a symmetric secret key. The sender then encrypts that symmetric secret key using the receiver's public key. The sender attaches the encrypted symmetric secret key to the encrypted message and sends the receiver the entire package. The sender could also digitally sign the package before sending it to prove the sender's identity to the receiver. To decrypt the package, the receiver first decrypts the symmetric secret key using the receiver's private key. Then, the receiver uses the symmetric secret key to decrypt the actual message. Since only the receiver can decrypt the encrypted symmetric secret key, the sender can be sure that only the intended receiver can read the message.

5.6. Key Management

Maintaining the secrecy of private keys is crucial to keeping cryptographic systems secure. Most compromises in security result from poor *key management* (e.g., the mishandling of private keys, resulting in key theft) rather than attacks that attempt to decypher the keys.

A main component of key management is key *generation—the* process by which keys are created. A malicious third party could try to decrypt a message by using every possible decryption key. Keys are made secure by choosing a key length so large that it is computationally infeasible to try all such combinations.

Key-generation algorithms are sometimes unintentionally constructed to choose only from a small subset of possible keys. If the subset is small enough, then it may be possible for a malicious third party to try every possible key to crack the encryption. Therefore, it is important to have a key-generation program that is truly random.

5.7. Digital Signatures

Digital signatures, the electronic equivalent of written signatures, were developed to be used in public-key cryptography to solve the problems of authentication and integrity. A digital signature authenticates the sender's identity, and, like a written signature, digital signatures are difficult to forge. To create a digital signature, a sender first takes the original plaintext message and runs it through a *hash function,* which is a mathematical calculation that gives

the message a *hash value.* The hash value is also known as a *message digest.* The chance that two different messages will have the same message digest is statistically insignificant. *Collision* occurs when multiple messages have the same hash value. It is computationally infeasible to compute a message from its hash value or to find two messages with the same hash value.

Next, the sender uses the sender's private key to encrypt the message digest. This step creates a digital signature and authenticates the sender, since only the owner of that private key could encrypt it the message. The original message, encrypted with the receiver's public key, the digital signature and the hash function, is sent to the receiver. The receiver uses the sender's public key to decipher the original digital signature and reveal the message digest. The receiver then uses his or her own private key to decipher the original message. Finally, the receiver applies the hash function to the original message. If the hash value of the original message matches the message digest included in the signature, then there is *message integrity;* the message has not been altered in transmission.

There is a fundamental difference between digital signatures and handwritten signatures. A handwritten signature is independent of the document being signed. Thus, if someone can forge a handwritten signature, they can use that signature to forge multiple documents. A digital signature is created using the contents of the document. Therefore, your digital signature is different for each document you sign.

Digital signatures do not provide proof that a message has been sent. Consider the following situation: A contractor sends a company a digitally signed contract, which the contractor later would like to revoke. The contractor could do so by releasing its private key and then claiming that the digitally signed contract came from an intruder who stole the contractor's private key. *Time-stamping,* which binds a time and date to a digital document, can help solve the problem of non-repudiation. For example, suppose the company and the contractor are negotiating a contract. The company requires the contractor to digitally sign the contract and then have the document digitally time-stamped by a third party called a *time- stamping agency.* The contractor sends the digitally signed contract to the time- stamping agency. The privacy of the message is maintained since the time-stamping agency sees only the encrypted, digitally signed message (as opposed to the original plaintext message). The time-stamping agency affixes the time and date of receipt to the encrypted, signed message and digitally

signs the whole package with the time-stamping agency's private key. The timestamp cannot be altered by anyone except the time-stamping agency, since no one else possesses the time-stamping agency's private key. Unless the contractor reports its private key to have been compromised before the document is time-stamped, the contractor cannot legally prove that the document was signed by a third party. The sender could also require the receiver to digitally sign and time-stamp the message as proof of receipt. To learn more about time-stamping, visit AuthentiDate.com (www.authentidate.com).

5.8. Public-key Infrastructure, Certificates and Certification Authorities

One problem with public-key cryptography is that anyone with a set of keys could potentially assume another party's identity. For example, say a customer wants to place an order with an online merchant. How does the customer know that the Web site being accessed indeed belongs to that merchant and not to a third party that posted a site and is masquerading as the merchant to steal credit-card information? *Public Key Infrastructure (PKI)* integrates public-key cryptography with *digital certificates* and *certification authorities* to authenticate parties in a transaction.

A digital certificate is a digital document issued by a *certification authority (CA).* A digital certificate includes the name of the subject (the company or individual being certified), the subject's public key, a serial number, an expiration date, the signature of the trusted certification authority and any other relevant information. A CA is a financial institution or other trusted third party, such as *VeriSign.* The CA takes responsibility for authentication, so it must carefully check information before issuing a digital certificate. Digital certificates are publicly available and are held by the certification authority in *certificate repositories.*

5.9. Internet Security

The CA signs the certificate by encrypting either the subject's public key or a hash value of the public key using the CA's own private key. The CA has to verify every subject's public key. Thus, users must trust the public key of a CA. Usually; each CA is pan of a *certificate authority hierarchy.* A certificate authority hierarchy is a chain of certificate authorities, starting with the *root certification authority,* which is the Internet Policy Registration Authority (IPRA). The IPRA signs certificates using the *root key.* The root signs certificates

only for *po1ic creation authorities,* which are organizations that set policies for obtaining digital certificates. In turn, policy creation authorities sign digital certificates for CAs. CAs sign digital certificates for individuals and organizations.

VeriSign, Inc., is a leading certificate authority. For more information about VeriSign, visit www.verisign.com.

Periodically changing key pairs is helpful in maintaining a secure system in case your private key is compromised without your knowledge. The longer you use a given key pair, the more vulnerable the keys are to attack. As a result, digital certificates are created with an expiration date, to force users to switch key pairs. If your private key is compromised before its expiration date, you can cancel your digital certificate and get a new key pair and digital certificate. Canceled and revoked certificates are placed on a *certificate revocation list (CRL).* CRLs are stored with the certification authority that issued the certificates.

Many people still perceive e-commerce to be un-secure. In fact, transactions using PKI and digital certificates are more secure than exchanging private information over phone lines, through the mail or even paying by credit card in person. After all, when you go to a restaurant and the waiter takes your credit card in back to process your bill, how do you know the waiter did not write down your credit-card information? In contrast, the key algorithms used in most secure online transactions are nearly impossible to compromise. By some estimates., the key algorithms used in public-key cryptography are so secure that even millions of today's computers working in parallel could not possibly break the code in a century. However, as computing power rapidly increases, key algorithms that are considered strong today could be easily breakable in the near future.

Digital-certificate capabilities are built into many e-mail packages. For example, in Microsoft Outlook, you can go to the Tools menu and select Options. Then click on the Security tab. At the bottom of the dialog box, you will see the option to obtain a digital ID. Selecting the option will take you to a Microsoft Web site with links to several worldwide certification authorities. Once you have a digital certificate, you can digitally sign your e-mail messages.

5.10. Cryptanalysis

Even if keys are kept secret, it may be possible to compromise the security of a system. Trying to decrypt cipher-text without knowledge of the decryption key is known as

cryptanalysis. Commercial encryption systems are constantly being researched by cryptologists to ensure that the systems are not vulnerable to a cryptanalytic attack. The most common form of cryptanalytic attacks are those in which the encryption algorithm is analyzed to find relations between bits of the encryption key and bits of the cipher-text. Often, these relations are only statistical in nature and incorporate outside knowledge about the plaintext. The goal of such an attack is to determine the key from the cipher-text.

Weak statistical trends between cipher-text and keys can be exploited to gain knowledge about the key if enough cipher-text is known. Proper key management and expiration dates on keys help prevent cryptanalytic attacks. Also, using public-key cryptography to securely exchange symmetric secret keys allows you to use a new symmetric secret key to encrypt every message.

5.11. Security Protocols

Everyone using the Web for e-business and e-commerce needs to be concerned about the security of their personal information. There arc several protocols that provide transaction security. such as *Secore Sockets Layer (SSL)* and *Secure Electronic TronsactionTM* (SETISI). We discuss these security protocols in the next two subsections.
7.10.1 Secure Sockets I.ayer (SSL)
The *Secure Sockets Layer (SSL) protocol,* descloped by Netscape Communications, is a nonproprietary protocol commonly used to secure communication on the Internet and the Web.6' 7 SSL is built into many Web browsers, including Netscape Communicator, Microsoft Internet Explorer and numerous other software products.. It operates between the Internet's TCP/IP communications protocol and the application software.
In a standard correspondence over the Internet, a sender's message is passed to a *socket* (which transmits information in a network): the socket interprets the message in Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP is the standard set of protocols used for communication between computers on the Internet. Most Internet transmissions are sent as sets of individual message pieces, called *packets.* At the sending side, the packets of one message are numbered sequentially, and error-control information is attached to each packet. TCP/IP routes packets to avoid traffic jams, so each packet might travel a different route over the Internet. At the receiving end, TCP/IP makes sure that all of the packets have arrived, puts them in sequential order and determines if the packets have arrived without alteration. If the packets have been altered, TCP/IP retransmits them. TCP/ IP then passes the message to the

socket at the receiver end. The socket translates the message back into a fortn that can be read by the receiver's application. In a transaction using SSL. the sockets are secured using public-key cryptography.

SSL uses public-key technology and digital certificates to authenticate the server in a transaction and to protect private information as it passes from one party to another over the Internet. SSL transactions do not require client authentication. To begin, a client sends *a* message to a server. The server responds and sends its digital certificate to the client for

Chapter?
14

Chapter 7

2tt

7.9 Cryptanalysis

.1

194 internet Security

Chapter 7

Chapter 7

Internet Security 195

authentication. Using public-key cryptography to communicate securely, the client and server negotiate *session keys* to continue the transaction. Session keys are symmetric secret keys that are used for the duration of that transaction. Once the keys arc established, the communication proceeds between the client and the server by using the session keys and digital certificates. Although SSL protects information as it is passed over the Internet, it does not protect private information, such as crcdit-card numbers, once the information is stored on the merchant's server. When a merchant receives credit—card information with an order, the information **is** often decrypted and stored on the merchant's server until the order is placed. If the server is not secure and the data are not encrypted. an unauthori,ed party can access the information. Hardware devices called *peripheml* c'ooipooent *i,iterc'onnect (PCI) cords* designed for SSL transactions can be installed on Web servers to secure data for an entire SSL transaction from the client to the Web server.8 The PCI card processes the SSL transactions. freeing the Web server to pertlirm other tasks. Visit www.phobos.com/Products/infami1y.htm for more information about these devices. For more inlormation about the SSL protocol, check out the Netscape SSL tutorial at developer .netscape .com/tech! security/ssl/protOcOl ,html and the Netscape Security Center site at **tscae.com/security/index.html.**

7.10.2 Secure Electronic Transaction'TM (SET'TM)

The *Secure Elcctronii lron.soi'oo'i (SET) protocol,* developed by Visa International tutd MasterCard, was designed specifically to protect c-commerce payment transactions.9 SET uses digital certificates to authenticate each party in an c—commerce transaction. including the customer, the merchant and the nierchant's hank. Public-key cryptography **is** used to secure information as it is passed over the Web.

Merchants must have a digital certificate and special SET software to process tr;uisactions. Customers must have a digital certificate and *thgic'ccI on/let* softsvare. A digital wallet is similar to a real wallet; it stores credit (or debit) card information for multiple cards, as well as a digital certificate serifying the cardholders identity. Digital wallets add convenience to online shopping; customers no longer need to reenter their credit—card information at each shopping site.

When a custonrer is ready to place tin order, the merchant's SET software sends the order information and the merchant's digital certificate to the customer's digital wallet. thus activating the wallet software. The custonter selects the credit card to he used for the transaction. The credit—card and order information are encrypted by using the merchant's hank's public key and sent to the merchant along ss ith the customer's digital certificate. The nterehant then forwards the information to the its bank to process the payment. Only the

merchant's bank can decrypt the message, since the message was encrypted **using** the banks public key. The merchant's bank then sends the amount of the purchase and its own digital certificate to the customer's hank to get approval to process the transaction. If the customer' s charge is approved, the customer's hank sends an authorization back to the merchant's bank. The merchant's bank their sends a credit-card authorization to the merchant. Finally, the merchant sends a confirmation of the order to the customer.
In the SET protocol, the merchant never sees the client's proprietary inlorntation. Therefore. the client's credit-card number is not stored on the merchant's server, considerably reducing the risk of fraud.

Although SET is designed specifically for c-commerce transactions and provides a high level of security, it has yet to become the standard protocol used in the majority of trailsactiOns. Part of the problem **is** that SET requires special software on both the client and server side; that requirement increases transaction costs. Also, the transactions are more tinte consuming than transactions using other protocols...stich as SSL. Both Visa and MasterCard have taken steps to reduce the financial burden to merchants, in an effort to encourage more merchants to use SET. I-losses er, svith higher transaction fees ;snd little pressure from customers. nian businesses are still reluctant to sw itch. 3
SET Secure Electronic Tron.soctio,t LLC is tnt organi/ation fornted hv 'v'isa and MasterCard to manage and promote the SET protocol. For more in torinat ion about SET, visit www.setco.org.www.visa.com and www.mastercard.com. Visa has ademonstration of an on Ii tie shopping transaction **ii s i itg** SET at www . visa . corn/nt / ecoxmn/ security/rnain.htrnl. GloheSet. a digital-ssallet software sendor. also offers a tutorial of a SET tr;m sact ion that uses a digi ltd wallet. ss hich may he found at www. globeset .com.

Microsoft Authenticode

How do you know that the software you ordered online is safe and has not been altered? How can you be sure that you are not dow nlnadi **itg** a computer virus that could ss ipe out your computer? Do you trust the source of the software? \Vith the emergence of ecommerce, software companies are offering their products online, so that customers can download software directly onto their computers. Security technology is used to ensure that the downloaded software is trustworthy and has not been altered. *Microsoft Authenticode,* combined with VeriSign digital certificates (or *cligirrcl iDs).* authenticates the publisher of the softss are and detects whether the softsvare has been altered. Atithenticode is a security feature built into Microsoft Internet Explorer.

To use Microsoft Authenticode technology, each software publisher must obtain a digital certificate specifically designed for the purpose of publishing software; such certificates may be obtained through certification authorities, such as VeriSign (Section 7.8). To obtain a certificate, a softsvare publisher must provide its public key and identification information and sign an agreement that it svill not distribute harmful software. This requirement gives customers legal recourse if any downloaded software from certified publishers causes harm. Microsoft Authenticode **uses** digital-signature technology to sign software (Seetioit 7.5). The sigited software and the publisher's digital certificate provide proof that the software is safe and has not been altered.

When a customer attempts to download a file, a dialog box appears on the screen displaying the digital certificate and the name of the certificate authority. Links to the publisher and the certificate atithority are provided so that customers can learn more about each party before they agree to download the software, If Microsoft Authenticode detennines that the software has been compromised. the transaction is terminated.

To learn more about Microsot't Authenticnde, visit the following sites; msdn.microsoft ,com/workshop/security/authcode/signfag. asp **msdn.microsoft .com/workshop/security/authcode/authwp.asp**

Recent cyberattacks on e-businesses have made the front pages of newspapers worldwide. *Denial-of-sen'ice ottocks, viruses* and *worms* have cost companies billions of dollars. Denial-of-service attacks usually require the power of a network of computers working simultaneously; the attacks cause networked computers to crash or disconnect from the network, making services unavailable. Denial-of-service attacks can disrupt service on a Web site and can even shut dossn critical systems such as telecommunications or flight-control centers.

Viruses are computer programs—often sent as an attachment or hidden in audio clips, video clips and games—that attach to, or overwrite, other programs to replicate themselves. Viruses can corrupt your files or even wipe out your hard drive. Before the Internet, viruses spread through files and programs (such as video games) transferred to computers by removable disks. Today, viruses are spread over a network simply by sharing "infected" files embedded in e-mail attachments, documents or programs. A worm is similar to a virus, except that it can spread and infect files on its own over a network', worms do not need to he attached to another program to spread. Once a virus or worm is released, it can spread rapidly, often infecting millions of computers worldwide within minutes or hours.

A denial-of-service attack occurs when a network's resources are taken up by an unauthorized individual, leaving the network unavailable for legitimate users; typically. the attack is performed by flooding servers with data packets. This action greatly increases the traffic on the network, overwhelming the servers and making it impossible for legitimate users to download information.

Another type of denial-of-service attack targets the *routing tables* of a network. Routing tables are essentially the road map of a network, providing directions for data to get from one computer to another. This type of attack is accomplished by modifying the routing tables, thus disabling network activity. For example, the routing tables can be changed to send all data to one address in the network. In a *distributed denial-of-sers'ice ottack,* the packet flooding does not come from a single source, but from many separate computers. Actually. such an attack is rarely the concerted work of many individuals. Instead, it is the ork of a single individual who has installed viruses on various computers, gaining illegitimate use of the computers to carry out the attack. Distributed denial-of-service attacks can he difficult to stop, since it is not clear which requests on a network are from legitimate users and which are part of the attack. In addition, it is particularly difficult to catch the culprit of such attacks, because the attacks are not carried out directly from the attacker's computer.

Who is responsible for viruses and denial-of-service attacks? Most often the responsible

parties are referred to as *hackers.* Hackers are usually skilled programmers. Some hackers break into systems just for the thrill of it, without causing any harm to the compromised systems (except, perhaps. humbling and humiliating their owners); others have malicious intent. Either way, hackers are breaking the law by accessing or damaging private information and computers. In February 2000, distributed denial-of-service attacks shut down a number of high-traffic Web sites, including Yahoo!. eBay, CNN Interactive and Amazon. In this case, a hacker used a network of computers to flood the Web sites with traffic that overwhelmed the sites' computers. Although, denial-of-service attacks merely shut off access to a Web site and do not affect the victim's data, they can be extremely costly. For example, when eBay's Web site went down for a 24-hour period on August 6, 1999, its stock value declined dramatically. 2

Chapter 7 Internet Security 197

Viruses, one of the most dangerous threats to network security, are typically malicious programs. There are many classes of computer viruses. A *transient virus* attaches itself to a specific computer program. The virus is activated when the program is run and deactivated when the program is terminated. A more powerful type of virus is a *resident virus,* which, once loaded into the memory of a computer, operates for the duration of the computer's use. Another type of virus is the *logic bomb,* which triggers when a given condition is met, such as a *time bomb* that is triggered when the clock on the computer matches a certain time or date. A *Trojan horse* virus is a malicious program that hides within a friendly program or simulates the identity of a legitimate program or feature, while actually causing damage to the computer or network in the background. The Trojan horse virus gets its name from Greek history and the story of the Trojan War. In this story, Greek warriors hid inside a wooden horse, which the Trojans took within the walls of the city of Tray. When night fell and the Trojans were asleep, the Greek warriors came out of the horse and opened the gates to the city. letting the Greek army enter the gates and destroy the city of Troy. Trojan horse viruses can be particularly difficult to detect, since they appear to be legitimate, useful programs. In June 2000. news spread of a Trojan horse virus disguised as a video clip sent as ao e-mail attachment. The Trojan horse virus was designed to give the attacker access to the infected computers. potentially to launch a denial-of-service attack against Web sites. Two of the most famous viruses to date are *Melissa,* which struck in March 1999, and the *ILOVE YOU virus* that hit in May 2000. Both viruses cost organizations and individuals billions of dollars. The Melissa virus spread in Microsoft Word documents sent via e-mail.

When the document was opened, the virus was triggered. Melissa accessed the Microsoft Outlook address hook on that computer and automatically sent the infected Word attachment by e-mail to the first 50 people in the address book. Each time another person opened the attachment, the virus would send out another 50 messages. Once into a system, the virus infected any subsequently saved files.
The ILOVEYOU virus was sent as an attachment to an e-mail posing as a love letter. The message in the e-mail said "Kindly check the attached love letter coming from me." Once opened, the virus accessed the Microsoft Outlook address book and sent out messages to the addresses listed, helping to spread the virus rapidly worldwide. The virus corrupted all types of files, including system files. Networks at companies and government organizations worldwide were shut down for days trying to remedy the problem and contain the virus.
A **e-Fcct7.3**
Estiinutesfordnnmage caused by time !LOVEYOt] riru.s *were ems high as $10 billion to $15 bit- lion. with time niujorriv of the daoioge done in just a few hours.*
Viruses and worms are not just limited to computers. In June 2000, a worm named *Tiinofonico* that was propagated through e-mail quickly made its way into the cellular phone network in Spain, sending prank calls and leaving text messages on the phones. No serious damage was done, nor did the worm infect the cell phones, but experts predict that we will see many more viruses and worms spread to cell phones in the t'uture.t7 Also, viruses spread through handheld devices are starting to appear.
Why do these viruses spread so quickly? One reason is that many people are too willing to open executable files from unknown sources. Have you ever opened an audio clip

7.11 Security Attacks

Chapter 7 .5,
'l

or video clip from a friend? Have you ever forwarded that clip to other friends? Do you know who created the clip and if any viruses are embedded in it? Did you open the ILOVE YOU file to see what the love letter said?

Most antivirus software is reactive, going after viruses once they are discovered, rather than protecting against unknown viruses. New antivinis software, such as Finjan Software's SurfinGuard® (www. finjan.corn), looks for executable files attached to e-mail and runs the executables in a secure area to test if they attempt to access and harm files. For more information about antivirus software, see the feature on McAfee. corn antivirus utilities.

Web defacing is another popular form of attack by hackers, wherein the hackers illegally enter an organization's Web site and change the contents. CNN Interactive has issued a special report titled "Insurgency on the Internet," with news stories about hackers and their online attacks. Included is a gallery of hacked sites. One notable case of Web defacing occurred in 1996. when Swedish hackers changed the Central intelligence Agency Web site odci . ***gov/c±a)*** to read "Central Stupidity Agency." The hackers put obscenities, messages and links to adult-content sites on the page. Many other popular and large Web sites have been defaced.

Cybercrime can have significant financial implications on an organization.14 Companies need to protect their data, intellectual property, customer information, etc. Implementing a *security policy* is key to protecting your organization's data and network. When developing a security plan, organizations must assess their vulnerabilities and the possible threats to security. What information do they need to protect? Who are the possible attackers and what is their intent—data theft or damaging the network? How will the organization respond to incidents?15 For more information about security and security plans, visit www.cerias.com and www. sans. org. Visit www. baselinesoft . corn to cheek out books and CD-ROMs on security policies. Baseline Software's book *Inform otion Policies Mode Eo.sy: Version* 7 includes over 1000 security policies. This book is used by numerous Fortune 200 companies.

The rise in cybercrimes has prompted the U. S. government to take action. Under the National Information Infrastructure Protection Act of 1996, denial-of-service attacks and distribution of viruses are federal crimes punishable by fines and jail time. For more information about the

U.S. government's efforts against cyber crime or to read about recently prosecuted cases, visit the U.S. Department of Justice Web site, at www.usdoj . gov/criminaj/ cybercrirne/cornpcrirne.htrnl, Also check out www.cybercrirne.gov, a site maintained by the Criminal Division of the U. S. Department of Justice.

The ***CERT®*** *(Cooiputer Emergency Response Teaoi) Coordination Center* at Carnegie Mellon University's Software Engineering Institute responds to reports of viruses and denial-of-service attacks and provides information on network security, including how to determine if your system has been compromised. Thc site provides detailed incident reports of viruses and denial-of-service attacks, including descriptions of the incidents, their impact and the solutions. The site also includes reports of vulnerahilities in popular operating systems and software packages. The *CERTSecurity bnproi'eoieot Modules* are excellent tutorials on network security. These modules describe the issues and technologies used to solve network security problems. For more information, visit the CERT Web site, at w'w. cart. org.

To learn more about how you can protect yourself or your network from hacker attacks, visit AntiOnlineTM, at w.antionhine.corn. This site has security-related news and information, a tutorial titled "Fight-back! Against Hackers," information about hackers and an archive of hacked sites. You can find additional information about denial- of-service attacks and how to protect your site at www.irchelp.org/jrchelp nuke.

7.12 Network Security

The goal of network security is to allosv authorized users access to information and services, while preventing unauthorized users from gaining access to, and possibly corrupting. the network, There is a trade-off between network security and network performance: Increased security often decreases the efficiency of the network,

7.12.1 Firewolls

A basic tool in network security is *theJireiivdl.* The purpose of a firewall is to protect a *local area network (LAN)* from intruders outside the network. For example, most companies have internal networks that allow employees to share files and access company informa I

jtt

Mcafee. *corn* ***Antivirus Utilities*** .

McAEee.com provides a variety of antivirus utilities (and other utilities) for users whose computers are not continuously connected to a network, for users whose computers are continuously connected to a network (such as the Internet) and for users connected to a

network via wireless devices, such as personal digital assistants and pagers. For computers that are not continuously connected to a network, McAfee provides its antivirus software *VirusScon*®. This software is configurable to scan files for viruses on demand or to scan continuously in the background as the user does his or her work. For computers that are network and Internet accessible, McAfee provides its online McAfee. corn Clinic. Users with a subscription to McAfee Clinic can use the online virus software from any computer they happen to be using. As with VirusScan software on stand-alone computers, users can scan their files on demand. A major benefit of the Clinic is its *ActiveShield* software. Once installed, ActiveShield can be configured to scan every file that is used on the computer or just the program files, It can also be configured to check automatically for virus definition updates and notify the user when such updates become available. The user simply clicks on the supplied hyperlink in an update notification to connect to the Clinic site and clicks on another hyperlink to download the update. Thus, users can keep their computers protected with the most up-to-date virus definitions at all times. For more information about McAfee, visit www.rncafee.com. Also, check out Norton security products from Symantec, at www. symantec .com. Symantec is a leading security software vendor. Its product NortonTM Internet Security 2000 provides protection against hackers, viruses and threats to privacy for both small businesses and individuals.

Lion. Each LAN can be connected to the Internet through a gateway, which usually includes a firewall. For years, one of the biggest threats to security came from employees inside the firewall. Now that businesses rely heavily on access to the Internet, an increasing number of security thrcats arc originating outside the firewall—from the hundreds of millions of people connected to the company network by the Internet. 8 A firewall acts as a safety barrier for data flowing into and out of the LAN. Firewalls can prohibit all data flow not expressly allowed, or can allow all data flow that is not expressly prohibited. The choice between these two models is up to the netork security administrator and should he based on the need for security versus the need for functionality.

There are two main types of firewalls: *pocket-filtering firewolls* and *application-level gateways.* A packet-filtering firewall examines all data sent from outside the LAN and automatically rejects any data packets that have local network addresses.. For example. if a hacker from outside the network obtains the address of a computer inside the network and tries to sneak a harmful data packet through the firewall, the packet-filtering firewall will reject the data packet, since it has an internal address, hut originated from outside the network. A problem with packet-filtering firewalls is that they consider only the source of data packets:

they do not examine the actual data. As a result, malicious viruses can be installed on an authorized user's computer. giving the hacker access to the network without the authorized user's knowledge. The goal ofan application-level gateway is to screen the actual data. If the message is deemed safe, then the message is sent through to the intended receiver.

Using a firewall is probably the single most effective and easiest way to add security to a small network.tQ Often, small companies or home users who are connected to the Internet through permanent connections, such as DSL lines, do not employ strong security measures. As a result, their computers are prime targets for hackers to use in denial-of-service attacks or to steal information. It is important for alt computers connected to the Internet to have some degree of security on their systems. There are numerous firewall software products available. Several products are listed in the Web resources in Section 7.14.

7.12.2 Kerberos

Firewalls do not protect you from internal security threats to your local area network. Internal attacks are common and can be extremely damaging. For example, disgruntled employees with network access can wreak havoc on an organization's network or steal valuable,

proprietary information. It is estimated that 70 percent to 90 percent of attacks on corporate networks are internal.20 *Kerberos* is a freely available, open-source protocol developed at MIT. Tt employs symmetric secret-key cryptography to authenticate users in a network and to maintain the integrity and privacy of network communications. Authentication in a Kerberos system is handled by a taain Kerberos system and a secondary *Ticket Granting Service (TGS).* This system is similar to key distribution centers, which were described in Section 7.3. The main Kerberos system authenticates a client's identity to the TGS: the TGS attthenticates client's rights to access specific network services, Each client in the network shares a symmetric secret key with the Kerberos system. This symmetric secret key may he used by multiple TOSs in the Kerberos system. The client starts by entering a login name and password into the Kerberos authentication serser. The authentication server maintains a database of all clients in the network. The authetitication server returns a *Ticket-Granting Ticket (TG7)* encrypted with the client's symmetric secret key that it shares with the authentication server. Since the symmetric secret key is

known only by the authentication server and the client, only the client can decrypt the TOT. thus authenticating the client's identity. NeNt, the client sends the decrypted TOT to the Ticket Granting Service to request a *sen'ice ticket.* The service ticket authorizes the client's access to specific network services. Service tickets have a set expiration time. Tickets may be renewed by the TGS.

7.12.3 Biometrics

An innovation in security is likely to be *biometrics.* Biometrics uses unique personal information, such as fingerprints, eyeball iris scans or face scans, to identify a user. This system eliminates the need for passwords, which are much easier to steal. Have you ever written down your passwords on a piece of paper and put the paper in your desk drawer or wallet? These days, people have passwords and PIN codes for everything—Web sites, networks, e-mail, ATM machines and even for their cars. Managing all of those codes can become a burden. Recently, the cost of biometric devices has dropped significantly. Keyboard- mounted fingerprint scanning devices arc being used in place of passwords to log into systems, check e-mail or access secure information over a network. Each user's iris scan, face stan or fingerprint is stored in a secure database. Each time a user logs in, his or her sean **is** compared with the database. If a match is made, the login is successful. Two companies that specialize in biometric devices are IriScan (www.iriscan.com) and Keytronic (www.keytronic.com). Foradditional resources, see Section 7,14.

Currently, passwords are the predominant means of authentication: however, we are beginning to see a shift to smart cards and Biometrics. Microsoft recently announced that it will include the *Biometric Application Progromotiog Intetfoce (BAPI)* in future versions of Windows, which will make it possible for companies to integrate biometrics into their systems.2t *Two-factor outheittication* uses two nieans to authenticate the user, such as biometrics or a smart card used in combination with a password. Though this system could potentially be compromised. using two methods of authentication is more secure than just using passwords alone.

One of the major concerns with biometrics is the issue of privacy. Implementing fingerprint scanners means that organizations will be keeping databases with each employee's fingerprint. Do people want to provide their employers with such personal information? What if those data are compromised? To date, most organizations that have implemented biometric systems have received little, if any, resistance from emploees. For more information on privacy issues, see Chapter II. Legal and Ethical Issues: Internet Taxation.

7.13 Steganography

Stegonograpltv is the practice of hiding information within other information. The term literally means "covered writing." Like cryptography. steganography has been used since ancient tinses. Steganography allows you to take a piece of information, such as a message or image, and hide it within another image, message or even an audio clip. Steganography takes advantage of insignificant space in digital files, in images or on removable disks.22 Consider a simple example: If you have a message that you want to send secretly, you can hide the information within another message. so that no one but the intended receiver can read it. For example, if you want to tell your stockbroker to buy a stock and your message must be transmitted over an unseeure channel, you could send the message "BURIED UN-

DER YARD." If you have agreed in advance that your message is hidden in the first letters of each word, the stock broker picks these letters off and sees "BUY."

An increasingly popular application of steganography is *digital warermarks* for intellectual property protection. An example of a conventional watermark is shown in Fig. 7.7. A digital watermark can he either visible or invisible. It is usually a company logo, copyright notification or other mark or message that indicates the oss ncr of the document. The oss ncr of a document could show the hidden watermark in a court of lass, for example, to prove that the watermarked item was stolen.

Digital watermarking coold have a substantial impact on c-commerce. Consider the music industry. Music publishers are concerned that MP3 technology is llowing people to distribute illegal copies of sotigs and albuots. As a result, many publishers are hesitant to put content online, as digital content is easy to copy. Also, since CD-ROMs are digital. people are able to upload their music and share it over the Web. Using digital watermarks. music publishers can make indistinguishable changes to a part of a song at a frequency **that** is not audible to humans, to show that the song was, in fact, copied.

Blite Spike's Giovanni 151 digital svatermarking software uses cryptographic keys to generate and embed steganographic digital watermarks into digital music and images (Fig. 7.8). The watcrmarks can he used as proof of ownership to help digital publishers protect their copyrighted material. The watermarks are undetectable bvany one ss ho is not pro y to the embedding schetrte, and titus the ss atermarks cannot be identified and removed. The atermarks are placed randomly.

Iatermark Overview.

t ,. **.4** ', visible from both sides

t . .4 , .

•&_ '"'.'-

. **-n-** r -. . .,

4• .. . ..[4 **4**

a .

- ... **Watèrmarks assist in preventinjiff fraud, tamperproofing and** - ' '

authenticating .

.

k 14 t.aw s- ‘fl’i’ ...*eJ ‘?C* UW5.t%

Rg. 7.8 An example of steganogrophy: Blue Spike’s Giovanni digital wotermarking process. (Courtesy at Blue Spike. Inc.)
Giovanni incorporates cryptography and steganography. It generates a symmetric secret key based on an encryption algorithm and the contents of the audio or image file that will carry the watermark. The key is then used to place (and eventually decode) the watermark. The software identifies the perceptually insignificant areas of the image or audio file, enabling a digital watermark to be embedded inaudibly, invisibly and in such a way that if the watermark is removed, the content is likely to be damaged.
Digital atermarking capabilities arc built into some image-editing software applications, such as Adobe PhotoShop 5.5 (ww.adobe .com) Companies that offer digital watermarking solutions include Digimarc digirnark.carn) and Cognicity (www. cognicity. corn).
In the last few chapters, we discussed the technologies involved in building and running an c-business, and how to secure online transactions and communications. tn Chapter 8, Internet Marketing. we discuss how to attract customers to your c-business Web site and build your customer base. We discuss the components of an Internet marketing campaign, including marketing. promotions and public relations.

7.14 Internet and World Wide Web Resources

Security Resource Site.c

WWW. **securitysearch.net**
This is a comprehensive resource for computer security. **The** site has thousands of links to products, Security companies. tools and noire. The site also offers a free weekty nessstetter with information about sn t nerabitities.

01000100. :10101
Multiple watermark layers accessible by separate

Fig. 7.7 Example of a conventional watermark, (Courtesy of Blue Spike, Inc.)

204 Internet Security Chapter 7 Chapter 7 Internet Security 205
www.esecurityonline.com - - *agazines, Newsletters and News sites*
This site is a great resource for information on online security. The site has links to news, tools, events,
www. networkcomputing .com/consensus
training and other valuable security information and resources. - The *Security Alert Consensus* is a free weekly newsletter with information about security threats,
www. epic. org holes, solutions and more.
The *Elecovnic Pt-liars Infrwinatiou Center* deals with protecting privacy and civil liberties.
Visit this ‘ infosecurityrnag . corn
site to learn more about the organization and its latest initiatives. *Inforetazioo Security Magazine* has the latest Web security news and vendor information.
theory.lcs .rnit.edu/-rivest/crypto-security.htnsl . - www.iss1.org/cipher.htn1
The *Ronald L. Rteest: Cnptogropliv and Securirs’* site has an extensive list of links to security resourc- - cj is an electronic newsletter on security and privacy from the Institute of Electrical and Elec es including newsgroups. government agencies, FAQs, tutorials and more. - tronics Engineers (IEEE). You can view current and past issues online.
www.w3.org/Secsarity/Overview.htrn1 . securityportal .com
The *W3C Security Resources* site has FAQs. information about W3C security and e-commerce initi- The Security *Portal* has news and information about security, cryptography

and the latest viruses.
atives and links to other security related Web sites.
www. scmagazane. corn
web. mit . edu/network/ ietf /sa *SC Magazine* has news, product reviesvs and a conference schedule for security events.
The Internet Engineering Task Force tIETF). which is an organization concerned with the architec,
cnn. corn/TECH/specials/hackers
tare of the I steraei, has working groups dedicated to Internet Security. Visit the *IETF Security A ceo*
Insurgency *on the Internet* front CNN Interactive has news on hacking, plus a gallery of hacked sites.
to learn about the ssorking groups. join the mailing list or cheek out the latest drafts of the IETF's
work. rootshell .com/beta/news .htni
Visit Rootshell t'or security-related news and white papers.
dir.yahoo ,com/Coissputers_ancj_Internet/Security_and_Encryption
The *Yahoo* Security and Eiuirvptiuiii page is a great resource for links to Web sites security and cncryp- *Gos'erntuent Sites for computer Security*
tion.
www.cit .nih.gov/security.htmi
se.counterpane.com/hot1ist.html This site has links to security organizations. security resources and tutorials on PKI. SSL and other
The Counterpane Internet Security, Inc.. site includes links to downloads, source code, FAQs, tutori- protocols.
als. alen groups. news and more.
cs-www.ncsl .nist .gov
www. rsasecurity. com/rsalabs/faq
The *ConipuuterSecoi-itv* Resource Clearing *Ho ise* isa resource for network administrators and others
This site is an excellent set of FAQ5 about cryptography from RSA Laboratories, one of the leading concerned svith security. This site has links to incident-reporting centers, information about security
makers of public key crypiosysteins. standards, events. publications and other resources.

www.nsi.org/cornpsec.html www.cdt.org/crypto

Visit the National Security Institute's *Security Resource Net* for the latest security alerts., government Visit the Center for Democracy and Technology for U. S legislation and policy news regarding cryp standards and legislation, as well as security FAQs links and other helpful resources. tography.

www.itaa.org/infosec www.epmornl .gov/-dunigan/security.htrnl

The Information Technology Association of America (ITAA) *lnfoSec* site has information about the This site has links to loads of security-related sites. The links are organized by subject and include

latest U.S. government legislation related to information security, resources on digital signatures. PKI. smart cards,vises, commercial providers, intrusion detection staff .washington.edu/dittrich/misc/ddos and several other topics.

The *Distributed Denial of Service Attacks* site has links to news articles, tools, advisory organizations aiw. nih. gov/Security

and esen a section on secarity humor. The *Contputer Security Information* page is an excellent resource. providing links to news, news ww infoworld. com/ cgi —bin/displayNew . p1? / security/i inks/ groups, organizations. software. FAQs and an extensive nomber of Web links. security_corner .htn www fedcirc .gov

The Securirr *Watch* site on Infoword. corn has loads of links to security resources. The Federal Compoter Incident Response Capability deals with the security of governnuent and civil www antionline .com ian agencies. This site has information about incident statistics, advisories, tools, patches and more.

AntiOnline has security-related nesvs and information, a tutorial titled "Fight-back! Against Hackers:' axion . physics. ubc . ca/pgp .htnl

information about hackers and an archive of hacked sites. This site has a list of freely available cryptosystems, along with a discussion of each system and links www.microsoft . corn/security/default, asp to FAQs and tutorials.

The Microsoft security site has links to downloads, security bulletins and tutorials. ws. icci - gov

The Internet Fraud Cotnplaint Center, founded by the Justice Deparintent and the FBI. fields reports

www. grc .com

This site offers a service to test the security of your cootpoter's Internet connection, of Internet fraud.

206 Internet Security Chapter 7 Chapter 7 Internet Security 207
www.disa.mil/infosec/iaweb/default.html ,jvsw.certicom.com
The Defense Information Systems Agency's *Information Assurance* page includes links to sites on vul- Certicom provides security solutions for the wireless Internet.
nerability warnings, virus information and incident-reporting instructions, as well as other helpful links. raytheon ,corn
'. Raytheon Corporation's *SilentRunner* monitors activity on a network to find intemal threats, such as
Internet Security Vendors 3 data theft or fraud.
www.rsasecurity.com 7 *SSL and SET*
RSA is one of the leaders in electronic security. Visit its site for more information about its current
prodacts and tools, ss hich are used by companies worldwide. . eveloper. netscape.
corn/tech/security! eel/protocol. html
This Netscape page has a brief description of SSL. plus links to an SSL tutorial and FAQs.
www.ca.com/protection
Computer Associates is a vendor of Internet security software. It has various software packages to , www. netscape .corn! security/index. htrnl
The Netscape Security Center is an extensive resource for Internet and Web security. You will find
help companies set up a firewall, scan files for viruses and protect against viruses.
news, tutorials, products and services on this site.

www.checkpoint.com

psych.Psy.uc.oz .au/-ftp/Crypto

Check PointlSi Software Technologies Ltd. is a leading providcr of Internet security products and ser- This FAQs page has an extensive list of questions and answers about SSL technology.

v ices.

www.aetco.org

www . nycio.corn The Secure Electronic Transaction LLC was formed through Visa and MasterCard to work on the SET

MyCIO provides Internet security software and services, specification. Visit this Web site to learn more about SET and the companies using SET in their prod-

www.opsec.com ucts, and check out the brief FAQs list and glossary.

The Open Platform Ibr Security (OPSEC) has over 200 partners that develop security products and

solutions using the OPSEC to allow for interoperability and increased security over a network. Visa International's security page includes information on SSL and SET. The page includes a demon www.baltinor .con stration of an online shopping transaction, which explains how SET works,

Baltimore is an e-comolerce security solutions provider. Its most popular product is UniCERT, a dig- www.nastercard.com/shoponline/set

ital ceoifieate product that is used in PKI. It also offers SET, public-key cryptography and digital cer- The *MosterCo rdSET* Web site includes information about the SET protocol, a glossary of SET-related

tificate solutions. terms, the latest developments and a demonstration walking you through the steps of a purchase using

SET technology.

www . ncipher. corn

nCipher is a vendor of hardware and software security products. Its products include an SSL acceler- ww.openssl .org

ator that speeds up transaction of SSL Web servers and a secure key management systeia. The *Open SSL Project* pros ides a free, open source toolkit for SSL.

entrust .con *Public-key Cryptography*

Entrust Technologies provides c-security products and services.

sesiw. entrust. corn

www. tenf our • co . uk
Entrust produces effective security software products using Public Key Infrastructure (PKI). TenFour provides software for secure e-mail.
www. c se . dnd. ca
www.antivirus.con The Communication Security Establishment has a short tutorial on Public Key Infrastructure (PKI)
SconMoil® is an e-mail virus detection program for Microsoft Exchange. that defines PKI. public-key cryptography and digital signatures.
www.contenttechnologies.con/ads www.magnet.state.nia.us/itd/legal/pki.htm
Content Technologies is a security software provider. Its products include firewall and secure e-mail The Commonwealth of Massachusetts Information Technology page has loads of links to sites related
prograias. t P1(1 that contain information about standards, vendors, trade groups and government organizations.
www.ziaasail.com www.ftech.net/-nonark/crypto/index.htn
Zi.sniorfl5i is a secure e-mail product that allows you to encrypt and digitally sign your messages using *flse Beginner's Guide* to *Cryptogrupliv* is an online tutorial and includes links to other sites on privacy
different e-mail programs. and cryptography.
www.pgp.con/scan www.faqs.org/faqs/cryptography-faq
PGP Security software protects your site from denial-of-service attacks. The *Crsp:ogrophv FAQ* has an extensive list of questions and answers.
web.rnit .edu/network/pgp.htnl www.pkiforuin.org
At this site you can download *Prenv* Good *Pri* racy® freeware, which allows you to send messages.. The PKI Forum promotes the use of PKI.
files. etc.. securely. www.rp.com/pki -risks. html
www.radguard.com Visit the Counterpane Internet Security, Inc.'s site to read she article "Ten Risks of PKI: WhatYou're
Radguard provides large-scale security solutions for c-businesses. Not Heing Told About Public Key Infrastructure:'

208 Internet Security Chapter 7 Chapter 7 Internet Security 209

I

Digital Signatures **5rc.ncsl.nist.gov/nistpubs/8OO—lO**

www.jetf.org/html.chartersfxrnldsig- charter. html Check out this firewall tutorial from the U.S. Department of Commerce.

The *XML Digital Signatures* site was created by a group working to develop digital signatures using www . watchguard . corn

XML. You ran view the group's goals and drafts of their work. WatchGuard® Technologies, Inc.. provides firewalls and other security solutions for medium to large www.elock.com organizations.

E-Lock Technologies is a vendor of digital-signature products used in Public Key Infrastructure. This www . networkice . corn

site has an FAQs list covering cryptography, keys, certificates and signatures. *Black/CE Defrnder,* from Network ICE, combines a firewall with intrsisian detection. www.digeigtrust .com

Kerberos

The Digital Signature Trust Co. is a vendor of Digital Signature and Public Key Infrastructure prod ucts

It has a tutorial titled 'Digital Signatures and Public Key lnfrastrsscture(PKI) 101: www.flrl .na.milfccs/people/kenh/kerberos—faq.html

This site is an extensive list of FAQs on Kerberos from the Naval Research Laboratory.

Digital Certificates web .mit . edu/kerberos/www

www.verisign.com *Kerberos: The Network Authentication Protocol* is a list of FAQ5 provided by MIT.

VeriSign creates digital IDs for individuals, small businesses and large corporations. Check

out its

www.contrib.andrew.cmu. edu/—shadow/kerberos .html

Web site for product information, news and downloads. *The Kerberos Reference Page* **has** links to several informational sites, technical sites and other helpful www.thawte.com resources.

Thawte Digital Certificate Services offers SSL, developer and personal certificates. ssxew.pdc .kth. ee/kth-krb

www. silanie .com/index. htm Visit this site to download various Kerberos white papers and documentation.

Silanis Technology is a vendor of digital-certificate software. *Biometrics*

www.belsign.be

Belsiga issues digital certificates in Europe. It is the European authority for digital certificates, www.ioeoftware.com/products/integration/fiu500/index.htm

www.certco.com This site describes a secarity device that scans a user's fingerprint to verify identity.

Certco issues digital certificates to financial institutions. saw. ident ix.com/flash index. html Identix specializes in fingerprinting systems for law enforcement, access control and network securi www openca . *org*

Set up your own CA using open-source softss are frons The OpenCA Project. ty. Using its fingerprint scanners, you can log on to your system. encrypt and decrypt files and lock applications.

Digital Ballets www.iriscan.com

www . gloheset .com Iriscan's *PR* **lri.5TM** can be used for c-commerce, network and information security. The scanner takes

GlobeSet is a vendor of digital-wallet software, Its site has an animated tutorial demonstrating the use an image of the user's eye for authentication.

of an electronic ss altet in an SET transaction. ww. keytronic .com

www. trintech. corn Key Tronic manufactures keyboards with fingerprint recognition systems.

Trintecls digital ssallets handle SSL and SET transactions.

Steganography and Digital Walermnarking

wallet .yahoo . con

The 'taboo! Wallet is a digital wallet that can be used at thousands of Yahoo! Stores

worldwide. www. bluespike. cons/giovanni/giovmain.html
Blue Spike's *Giovanni* watermarks help publishers of digital content protect their copyrighted mate Firewall rial and track their content that is distributed electronically. www.interhack.net/pubs/fwfaq e.outg'uess.org
This site provides an extensive list of FAQ5 on firewalls. *Outguess* isa freely available steganographic tool.
www.spirit .com/cgi-bin/report.pl www.cl .casss.ac.uk/-fapp2/eteganography/index.html
Visit this site to compare firewall software from a variety of vendors. The Information Hiding Homepage has technical information, news and links related to digital wa termarkin and steganography.
www.zeuros.co.uk/generic/reeource/flrewall
Zeuros is a complete resource for information about firecalls. You will find FAQs. books, articles, sn'jw.demcom.con
training and nsagaztnes on this site. DcmCnm's *Steganas Security Suite* software allows you to encrypt and hide files within audio, video, www.thegild.com/firewall text or HTML files.
The *Firewall Product Os'en'iew* site has an extensive list of firewall products, with links to each yen- www. digimarc .com
dor's site. Digimarc is a leading provider of digital-watermarking software solutions.

www.cognicLty.com

Cogmeity specializes in **digital-watermarking** solutions (or the music and entertainment ittdustries.

Newsgroups

news :comp. security. firewalls news :conp. security .unix news:conp. security.nisc news: conp . protocols. kerberos

SUMMARY

• There are four fundamental requirements of a successful. secure transaction: privacy, integrity .authentication and nonrepudiatron.
• Cry ptography transforms data by using a key—a string of digits that acts as a passssord—to mike the data incomprehensible to all but the sender and the intended receivers. Unencrypted data are called plaintest: encry pted data are called ciphcrtext.
A cipher. or cryptosy stein, **is** a technique or algorithm for encr% pting messages. Longer keys have stronger encryption: **it** takes more tinte **and** computing power to brcak the eacryption code.
Secret.key cryptography uses the sante sy trimetric secret key to ettcrs Pt and decrypt a message.
• In a netssork ss rh a key distribution center, each user shares one synanetrie secret key ss ith the key distribution center.
• One of the most commonly used symmetric encryption algoritlt ms is the Data Eucry ption Standard (DES). which was deseloped by the National Security Agency INSAI and IBM in the 195l)s. The current standard of symntctric encryption is Triple DES, a sariant of DES that is esserttrall three DES systems in a rosr. each basing **its** oss n secret key.
• The **U. S.** goveruntent is in the process ol selecting a ness. more secure standard for symrttctrtc encryption. The new standard will become the Advattced Encryption Standard (AESI.
In 1976. Whitfield Diffie and Manin Bellman. tao researchers at Stanford University. deseloped public-key cryptography to solve the problem of excltanging keys securely. Public-key cry ptography is asymmetric. It uses tsso insersely related keys: a public key attd a

private key. The pris ate key is kept secret by its owner. The public key is freely distributed.
• If the public key is used to encrypt a ntessage. only the corresponding pris ate key can decrypt it. and sice versa.
• If the user's decryption key is the public key and his or ltercttcryption key is private, the sender tsf the tacssage can be authenticated.
• The most comnttsnly used public-key algorithm is RSA. an encry ptuon system developed by Ron Rivest. Adi Shatair and Leonard Adlentan in 1977.
• The process by svhich tsso parties can exchange keys oser an unsecure ntedium is called a key agreement protocol.
• The most common key agreentent protocol is a dtgital envelope.
• Digital signatures. the electronic equisalent of svritten signatures. ssere des eloped to he used in public-key cryptography to solve the prohlcnts of authenttcation and integrity.
• A digital signature authenticates the senders identity. and. like a svritten signature. it is diUicult tis forge.

• A timestamping agency affixes the time and date of receipt to the encrypted, signed message and digitally signs the whole package with the timestamping agency's private key. - The digital authentication standard of the U.S. government is called the Digital Signature Algorithm (DSA).
• public Key Infrastructure lPKl) adds digital certificates to the process of authentication. A digital certificate includes the name of the subject (the company or individual being certified), the subject's public key. a serial number, an expiration date, the authorization of the trusted certification authority and any other relcs ant information.
A certification auttltority I CA) is a fittautcial institution or other trusted third party, such as Veri— Stgn.
Digital certificates are publicly available and are held by the certification authority in certificate
repositories.
• By sonte estintates. the key algorithttts used in ptihlic-key cryptography are so secure that even millions of computers ss orking in parallel could nist possibly break the cnsde in a century.
• Trying to decrypt ciphertest 55 itltout knoss ledge of the decryption key is kuoscn as cryptanalysis. SSL rises public-key technology and digital certificates to authenticate the serser in a transaction and to prnstect pri s tte in forntatioit as it passes from one party' to

Ltnother 05cr the Internet.
- • Session keys are symmetric secret keys that are ttscd for the dttratiott of a transaction.
• SET itses digital certificates to authenticate each party in an e—eonsnteree transaction, including the customer, the ttmerchant and the nmcrehant's hank.
• A digital ss allet is similar to a real svallet: it stores credit (or debit) card infornsatiots for multiple cards, as well as a digital certificate verifying the cardholder's identity.
• In the SE1' protocol, tlse merchant never actually sees the client's proprietars itsformation. There— fore, the client's credit-card number is not stored on the merchant's serser. considerably reducing the risk of fraud.
Microsoft Aathenticode uses digital—signature technology to sign softss are. The signed software and the publisher's digital certificate pros ide protif that the software is safe and has not been altered.
• Virttses are cotuputer prograntts—usually sent as an attachment or hidden in audio clips, video eltps and games—that attach to or overwrite other programs to replicate themselves.
• A ssorm **is** similar to a virus, except that it can spread and infect files on **its** oss n over a netsvork; wornts do not need to he attached to another program to spread.
• A deniul-ol-sers'ice attack occurs svhemn a network's resources are taken up by an unauthorized individual. leasing the netsvork unasuilable ftsr legitimate users; typically, the attack is performed by flooding servers svitlt data packets.
• A logic homh triggers sshen a given condition is ntet, such as sshen the clock on the computer ntatches a ceouin tinse or date.
• A Trojan horse virus **is** a ittalicious program that hides within a friendly program or simulates the identity of a legitimate program or feature, while actually causing damage to the consputeror network in the background.
• Web defacing is another popular fornm of attack by hackers., ssherein the hackers illegally enter an organization's Web site and change the contents.
A firessall protects a local area netsvork (LAN) from intruders outside the netsvork.
• A packet-filtering firesvall examines all data sent front outside the LAN and automatically rejects any data packets that have local network addresses.

212 Internet Security

Chapt 7

Internet Security 213

• The goal ofaappltcation-level gateway is to screen the actual data. If the message is deemed safe, then the message is sent through to the intended receiver.

• Kerberos is a freely available, open-source protocol developed at MIT. It employs symmetric secret-key cryptography to authenticate users in a network and to maintain the integrity and privacy of network communications.

• Biometrics uses unique personal information, such as fingerprints, eyeball iris scans or face scans, to identify a user. This system eliminates the need for passwords, which are much easier to steal.

• Steganography is the practice of hiding information. The term literally means “covered writing.”

1ERMINOLOG V

ActiveShield
Advanced Encryption Standard (AES) application-level gateway asymmetric algorithms authentication
Authenticode (from Microsoft) availability

binary siring

bit

CERT (Computer Emergency Response Teatn) CERT Security Improvement Modules
certification authority (CA)
certificate authority hierarchy
certificate repository
certificate revocation list (CRL)
cipher
ciphersest
collision
cryptanalysis
cryptography
cry ptosystem
Data Encryption Standard (DES)
data packets
decryption
denial-of-service attack
Diffie-Hellman Key Agreement Protocol digital certificate
digital envelope
digital IDs
Digital Signature Algorithm (DSA)
digital signature
digital wallet
digital watermarking
dtstributed denial-of-service attack
encryption
firewall
hacker
hash function

secret key
Secure Electronic Transactions (SET) Secure Sockets Layer (SSL)
service ticket

session keys
SET Secore Electronic Transaction LLC socket
5tegauography
substitution cipher
symmetric encryption algorithms virus
TCP/IP (Transmission Control Protocol/InternetWeb defacing
Protocol) worm

SELF-REVIEW EXERCISES

State whether the following are *(roe orfolxe.* If the answer is *fol.ce,* explain why.
a) In a public-key algorithm, one key is used for both encryption and decryption.
b) Digital certificates are intended to be used indefinitely.
c Secure Sockets Layer protects data ssored on a merchants server.
d) Secure Electronic Transaction is another name for Secure Sockets Layer.
e) Digital signatures can be used to provide undeniable proof of the author ofa document.
f) In a network of 10 users communicating using public-key cryptography, only 10 keys are needed in total.

The security of modern cryptosystems lies in the secrecy of the algorithm. Users should avoid changing keys as much as possible, unless they have reason to believe that the security of the key has been compromised.
Increasing the security of a network often decreases its functionality and el'ficiency. Firewalls are the single most effective way to add security to a small computer network.

k) Kerberos is an authentication protocol that is used over TCP/IP networks.

Fill in the blanks in each of the following statements:
a) Cryptographic algorithms in which the message's sender and receiver both hold an identical key are called _____
b) A _____ is used to authenticate the sender of a docutnent.In a _____,a document is encrypted using a symmetric secret key and sent with that symmetric secret key, encrypted using a public-key algorithm.
c) A certificate that needs to be revoked before its expiration date is placed on a

d) The recent wave of network attacks that have hit companies such as eBay, and Yahoo are known as _____

e) A digital fingerprint of a document can be created using a

I) The four main issues addressed by cryptography are _____ _____

_____ and _____

g) A customer can store purchase information and data on multiple credit cards in an electronic purchasing and stomge device called a _____

h) Trying to decrypt ciphertext without knowing the decryption key is known as

i) A barrier between a small network and the outside world is called a _____

Ticket Granting Ticket (TGT) time bombs timestamping timestamping agency timofonica transient virus transposition cipher Triple DES Trojan horse virus VeriSign

biometrics

7.1

g)

h)

hash value
ILOVEYOU Virus
integrity
Internet Policy Registration Authority (IPRA) Kerberos
key
key agreement protocol
key distribution center
key generation
key length
key management
local area network (LAN)
logic bombs
Melissa Virus

message digest
message integrity
Microsoft Authenticode
National Institute of Standards and Technology network security
nonrepudiation
one-way hash functions
packet-filtering firewall
packets
PCI (peripheral component interconnect) cards plaintext
policy creation authorities
privacy
private key
protocol
public key
public-key algorithms
public-key cryptography
Public Key Infrastructure (PKI) resident virus
restricted algorithms
root certification authority
root key
routing tables
RSA Security, Inc.

i)
j)

7.2

214 Internet Security

Chapter 7

Chapter 7

Internet Security 215

ANSWERS TO SELF-REVIEW EXERCISES

71 a) False. The encryption key is different from the decryption key. One is made public, and the other is kept private. b) False. Digital certificates are created with an expiration date to encourage users to periodically change their public/private-key pair. c) False. Secure Sockets Layer is an Intemet security protocol, which secures the transfer of information in electronic communication. It does not protect data stored on a merchant's server. d) False. Secure Electronic Transaction is a security protocol designed by Visa and MasterCard as a more secure alternative to Secure Sockets Layer. e) False. A user who digitally signed a document could later intentionally give up his or her private key and then claim that the document was written by an imposter. Thus, timestamping a document is necessary, so that users cannot repudiate documents written before the pubic/private-key pair is reported as invalidated. 0 False. Each user needs a public key and a private key. Thus, in a network of 10 users, 20 keys are needed in total. g) False. The security of modem cryptosystems lies in the secrecy of the encryption and decryption keys. h) False. Changing keys often is a good way to maintain the sccurity of a communication system. i) True. j) True. k) True.

7.2 a) symmetric key algorithms. b) digital signature. c) digital envelope. d) certificate revocation list. e) distributed denial-of-service attacks. f) hash function. g) privacy, authentication, integrity, nonrepudiation. h) electronic wallet. i) cryptanalysis. j) firewall.

EXERCISES

7.3 What can online businesses do to prevent hacker attacks, such as denial-of-service attacks and virus attacks?

7.4 Define the following security terms:
a) digital signature
h) hash function

cl symmetric key encryption d) digital certificate
e) denial-of-service attack

0 ssorm

g) message digest
hi collision
i) triple DES
j) session keys

7.5 Define each of the following security terms, and give an example of how it is used:
a) secret-key cryptography
bi public-key cryptography
c) digital signature
di digital certificate
e) hash function
0 SSL
g) Kerberos
h) fircsvall
7.6 Write the full name and describe each of the following acronyms:
a) PKI
b) RSA
c) CRL
d) AES
e) SET

7.7 (floss *Discussion).* The Internet and the wireless intcmet are inherently unsecare, yet we are heading in a direction where many government, militars' and business operations will be conducted online. In that context, discuss the importance of security. Are you satisfied the Internet can be made secure enough to handle these transactions?
7.8 List the four problems addressed by cryptography, and give a real-world exansple of each.

73 Compare symmetric-key algorithms with public-key algorithms. What are the benefits and drawbacks of each type of algorithm? How are these differences manifested in the real-world uses of the two types of algorithms?

7.10 The Visa International Web Site includes an interactive demonstration of the Secure Electronic Transaction (SET) protocol that uses animation to explain this complicated protocol in a way that most people will understand. Visit Visa at n'iw.visa.com/nt/gecfno shock, jntroL . html to view the demo. Write a short summary of SET. How does SET differ from SSL? Why are digital wallets important? How arc they used? if you were asked to choose between the twn protocols. which would you choose, and why?

7.11 Explain how, in a network using symmetric-key encryption, a key distribution center can play the role of an authenticator of parties.

7-12 Go to the VeriSign Web site, at www. verisign - cony Write an analysis of the features and security of VeriSign's digital certificates. Then go to five other certification authorities and compare the features and security of their digital certificates with that of VeriSign.

7.13 Research the Secure Digital Music Initiative lwww.sdmi.org), Describe how security technologies such as digital watermarks can help music publishers protect their copyrighted work.

714 Distinguish between packet-filtering firewaths and application-level gateways,

7.15 Using steganography, hide the message "MERGER IS A GO" inside a seemingly unrelated paragraph of text. Insert your secret message as the second character of each word in the paragraph.

WORKS CITED

The notation www. domajn—nne . cons> indicates that the citation is for information found at the Web site,

1. A. Harrison, "Xerox Unit Farms Out Security is 52051 Deal:' *Coniputc'nrorld* 5 June 2000: 24.

2. RSA Laboratories, 'RSA Laboratories' Frequently Asked Questions About Today's Cryptography. Version 4.1:' <www - **rsaaecurity** . com/rsa1ab / faq>, RSA Security, inc.. 2000.

3. A. Harrison, "Advanced Encryption Standard' Cooipurenrorld 29 May 2000: 57.

4. RSA Laboratories, "RSA Laboratories' Freqtiently Asked Questions About Today's Cryptography, Version 4.1 ," rsasecssr-ity. com/rsalaba/faq>, RSA Security. Inc. 2000.

5. R. Yasin, “PKI Rollout to Get Cheaper, Quicker:’ Internet Week 24 July 2000: 28.
C. S. Abbot, “The Debate for Secure E’Commerce,” Pesfrnno,tce Computing February 1999” 37- 42
7. T. Wilson, “E-Btz Bucks Lost Under the SSL Train,” Ittrerner Week 24 May 1999: 1,3.
8. M. Bull, “Ensuring End-to-End Security with SSL.” Nerii’ork *World* 15 May 2000: 63.
9. 5. tachlis.,”IBM Hedges its Bets on SET:- €‘onipurersrorld 20 July 1998: 4.
10. J. McKcndrick, “is Anyone SET for Secure Electronic Transactions:’ *ENT4* March 1998: 44,
46.

ii. W. Andrews, “The Digital Wallet: A concept revolutionizing c-commerce:’ Internet H’brkj 15
October 1999: 34-35.

12. “Securing B28,” *Global Technology Business* July 200: 50-51
13. S. Machlis, “MasterCard Makes SET More Attractive,’ *Coinputerworid* 12 January 1998: 3.
14. R. Marsland, “Hidden Cost of Technology.” *Financial Ti,nes* 2 June 2000: 5.
15. F. Avolio, “Best Practices in Network Security,” *Network Computing* 20 March 2000: 60-72.
16. H. Bray. “Trojan Horse Attacks Computers. Disguised as a Video Chip,” *The Boston Globe* 10 June2000: Ci+.
17. A. Eisenberg, “Viruses Could Have Your Number,” *The New York Thnes* 8 June 2000: E7.
18, R. Marshland, “Hidden Cost of Technology.” *Financial Ti,ne.c* 2 June 2000: 5.
19. T. Spangler, “Home is Where the Hack Is,” *Inter@ctise Week* 10 April2000: 28-34.
20. S. Gaudin, “The Enemy Within,” *Network World* 8 May 2000: 122-126.
21. D. Deckmyn. “Companies Push New Approaches to Authentication.” *Computerworid.* IS

May
2000: 6.
22. S. Katzenbeisser and F. Petitcolas. Ed., *info rmation Hidinç': Techniques for Steganograpln and Digital Watertnarking* (Norwood, MA: Artech House, Inc.. 2000) 1-2.

RECOMMENDED READINGS

Bennato, S. "Feds Sign Off on c-Signatures." *eWeek* 29 May 2000: 20-21.
Deitel, 11. *An Introduction to Operating Systems* Second Edition, Reading. MA: Addison Wesley.
1990.
DiDio, L. "Private-key Nets Unlock c-Commerce." *Cooiptstersrorld* 16 March 1998: 49-50.
Ford, W., and M. Baum. *Secure Electronic Comnu'rc,e: Building the inftsrctrucrure for Digital Signo— tures and Encryption.* Upper Saddle River, NJ: Prentice HaIl, 1997.
Gartinkel, 5. and Spafford, G. *Web Security and Commerce.* Cambridge. MA: O'Reilly, 1997.
Ghosh, A. *E-'ommerce Security: Weak Links, Best Defenses.* New York, NY: Wile3 Computer Publishing, 1998.
Goncalves. M. *Firewalls: A Complete Guide.New* York. NY: McGraw-Hill, 2000.
Kippenhahn, R. *Code Breaking.* New York, NY: The Overlook Press, 1999.
Kosiur, D. *Understanding Electronic Commerce.* Redmond. WA: Microsoft Press, 1997.
Marsland, R. "Hidden Cost of Technology." *Financial Tunes* 2 June 2 2000: 5.
Pileeger, C. *Security in Computing.' Second Edirion.* Upper Saddle River, NJ: Prentice Hall. 1997.
RSA Laboratories RSA *Laboratories' Frequently Asked Questions About Today's Cryptography.*
Version 4.1." **<'tw.rsasecurity.com/rsa1abs/faq** RSA Security **Inc.,** 2000.
Sager, 1. "Cyber Crime." *Business Week* 21 February 2000: 37-42.
Schneier, B. *Applied Cryptography: Protocols, Algorithms and Source Code in C.* New York, NY:
John Wiley & Sons, Inc., 1996.
Sherif, M. *Protocols for Secure Electronic Commerce.* New York, NY: CRC Press, 2000.
Smith, R. *Internet Cryptography.* Reading, MA: Addison Wesley. 1997.
Spangler, T. "Home Is Where The Hack Is." *inser@ctis'e Week* 10 April 2000: 28-34.
Wrixon, F. *Codes, Ciphers & Other Crs'ptic & Clandestine Crunmunicarion* New York. NY: Black
Dog & Leventhal Publishers. 1998.

References

1. P.Gloor, “Making the e-Business Transformation”, Springer, London.
2. D.Amor, “Electronic Business Revolution”, Prentice Hall, NJ, 2000, ISBN:013085123X
3. H. Bidgoli, “Electronic Commerce: Principles and Practice”, Academic Press, New York, 2002, ISBN: 0-12-095977-1
4. H. M. Deitel, P. J. Deitel and K.Steinbuhler, “e-Business and e-Commerce for Managers”, Prentice-Hall, New Jersey, 2001, ISBN: 0-13-032364-0