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 Publİc-Key Cryptography

Public- key cryptography is asymmetric. It uses two inversely related keys: a *pu blic* 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, derivi ng 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 DİGİTAL SİGNATURES

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 CRYPTANALYSİS

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

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.

Appendix I

Doubleclick - *Marketing with Personal Information* [1]

While privacy advocate groups argue that the Web will not survive without some login of regulation advertising organizations disagree. DoubleClick, an Internet advertising firm suggests that advertising must be effective to minimize Internet-related costs. Regulation of the Internet could limit a company's efforts to buy and sell advertising. As with television and radio advertising, the money generated by Internet advertising can allow people of all economic means to use the medium.

Web sites use a variety of tracking methods to record where visitors come from, where they go and what catches their interest along the way. This information is tied to your computer's IP address (i.e., the numerical address of your computer on the Internet), Web browser and operating system; it is used by marketers to target relevant advertisements at specific computers. DoubleClick has an advertising network of more than l,500 sites where banner advertisements for 11,000 of its clients appear. This network enables DoubleCliek to combine data from many sites to target advertisements for particular computers.

However, targeting a specific IP address, browser and operating system is less effective than targeting a specific consumer. In 1999, DoubleCliek acquired Abacus Direct Corporation, a direct-marketing organization. Abacus stores names, addresses, telephone numbers, age, gender, income levels and a history of purchases at retail, catalog and online stores. This acquisition enabled DoubleClick to attach personal information to the activities of what were once “nameless” personal computers.

One concern with this method of collecting and using data is termed *digital redlining.* Digital redlining suggests that a company could skew an individual's knowledge of available products by basing the advertisements the user sees on past behavior. This practice could allow advertisers to influence consumers' habits by limiting the information they see to what the advertisers determine the consumers want to see.

Direct marketing in the traditional sense affords a certain time lapse between an individual's purchases, the processing of that information and the use of that information to target the particular customer. However, users can be targeted instantly as they browse the Internet.

Perhaps of greater concern is the recording of personal activities. The Internet is appreciated as a medium in which users can search for information and express opinions anonymously. Privacy advocates are concerned that such data could be used against individuals attempting to obtain housing, get a loan, and apply for insurance coverage. For example, a user visiting a Web site to learn more about an illness might not want that information to be made available to insurance companies. DoubleCliek promises to uphold its privacy policy, which assures users that the company will not collect financial, sexually oriented or medical information. In response to concerns about privacy, DoubleCliek has joined the Network Advertising Initiative.