Chapter 21
Security

Learning objectives

By the end of this chapter you should be able to:

- show understanding of the terms: public key, private key, plain text, cipher text, encryption and asymmetric key cryptography
- show understanding of how the keys can be used to send:
  - a private message from the public to an individual/ organisation
  - a verified message to the public
- show understanding of how a digital certificate is acquired and used to produce digital signatures
- show awareness of the purpose of Secure Socket Layer (SSL)/Transport Layer Security (TLS); its use in client–server communication and situations where its use would be appropriate
- show understanding of malware: viruses, worms, phishing and pharming
- describe vulnerabilities that the various types of malware can exploit
- describe methods that can be used to restrict the effect of malware.

21.01 Encryption fundamentals

Encryption can be used as a routine procedure when storing data within a computing system. However, the focus in this chapter is on the use of encryption when transmitting data over a network.

The use of encryption is illustrated in Figure 21.01.The process starts with original data referred to as **plaintext**, whatever form it takes. This is encrypted by an encryption algorithm which makes use of a key. The product of the encryption is **ciphertext**, which is transmitted to the recipient. When the transmission is received it is decrypted using a decryption algorithm and a key to produce the original plaintext.

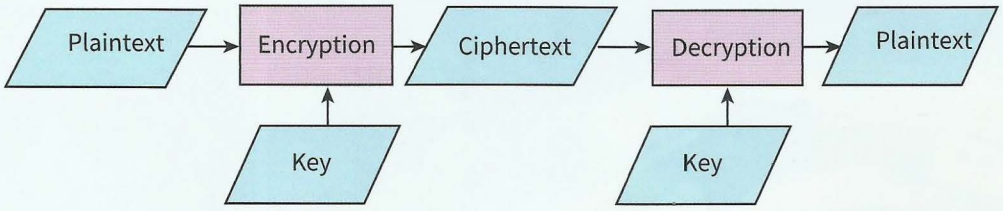

Figure 21.01 Overview of encryption and decryption

KEY TERMS

Plaintext: data before encryption

Ciphertext: the result of applying an encryption algorithm to data

Security concerns

There are a number of security concerns relating to a transmission:

- Confidentiality: Only the intended recipient should be able to decrypt the ciphertext.
- Authenticity: The receiver must be certain who sent the ciphertext.
- Integrity: The ciphertext must not be modified during transmission.
- Non-repudiation: Neither sender nor receiver should be able to deny involvement in the transmission.
- Availability: Nothing should happen to prevent the receiver from receiving the transmission.

This chapter will consider only confidentiality, authenticity and integrity.

The confidentiality concern arises because a message could be intercepted during transmission and the contents read by an unauthorised person. The concern about integrity reflects the fact that the transmission might be interfered with deliberately but also that there might be accidental corruption of the data during transmission.

Encryption methods

The fundamental principle of encryption is that the encryption algorithm must not be a secret: it must be in the public domain. In contrast, an encryption key must be secret. However, this is not quite the full story. There are two alternative approaches. One is symmetric key encryption; the other is asymmetric key encryption.

In symmetric key encryption there is just one key which is used to encrypt and then to decrypt. This key is a secret shared by the sender and the receiver of a message. In asymmetric key encryption two different keys are used, one for encryption and a different one for decryption. Only one of these is a secret.

So, how does this work? What happens at the sending end is straightforward. The sender has a key which is used to encrypt some plaintext and the ciphertext produced is transmitted to the receiver. The question is, how does the receiver get to have the key needed for decryption? If symmetric key encryption is used, there needs to be a secure method for the sender and receiver to be provided with the secret key.

Using asymmetric key encryption, the process actually starts with the receiver. The receiver must be in possession of two keys. One is a public key which is not secret. The other is a private key which is secret and known only to the receiver. The receiver can send the public key to a sender, who uses the public key for encryption and sends the ciphertext to the receiver. The receiver is the only person who can decrypt the message because the private and public keys are a matched pair. The public key can be provided to any number of different people allowing the receiver to receive a private message from any of them. Note, however, that if two individuals require two-way communication, both communicators need a private key and must send the matching public key to the other person.

There are two requirements to ensure confidentiality should the transmission be intercepted and the message extracted: the encryption algorithm must be complex and the number of bits used to define the key must be large.

Extension Question 21.01

The details of encryption algorithms are beyond the scope of this book. However, you might wish to investigate the type of approach used in established examples, such as DES or RSA. Also, you might wish to consider the number of different combinations for a 64-bit or 128-bit key.

The above account does not completely answer the question of how encryption works. The missing factor is an organisation to provide keys and to ensure their safe delivery to individuals using them.

21.02 Digital signatures and digital certificates

Using asymmetric encryption, the decryption–encryption works if the keys are used the other way round. An individual can encrypt a message with a private key and send this to many recipients who have the corresponding public key and can therefore decrypt the message. This approach would not be used if the content of a message was confidential. However, it could be used if it was important to verify who the sender was. Only the sender has the private key and the public keys only work with that one specific private key. Therefore, used this way, the message has a digital signature identifying the sender.

There is a disadvantage in using this method of applying a digital signature in that it is associated with an encryption of the whole of a message. An alternative is to use a cryptographic one-way hash function which creates from the message a number, uniquely defined for the particular message, called a 'digest'. The private key is used as a signature for this digest. This speeds up the process of confirming the sender's identity. The process at the sender's end of the transmission is outlined in Figure 21.02. A public one-way hash function is used.

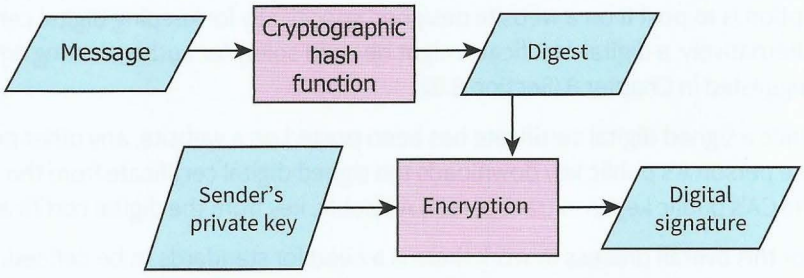

Figure 21.02 Sender using a one-way hash function to send a digital signature

We will assume that the message is transmitted as plaintext together with the digital signature as a separate file. The processes that take place at the receiver end are outlined in Figure 21.03. The same public hash key function is used that was used by the sender so the same digest is produced if the message has been transmitted without alteration.

The decryption of the digital signature produces an identical digest if the message was genuinely sent by the original owner of the public key that the receiver has used. This approach has allowed the receiver to be confident that the message is both authentic and unaltered.

This sounds good but unfortunately it does not consider the fact that someone might forge a public key and pretend to be someone else. Therefore, there is a need for a more rigorous means of ensuring authentication. This can be provided by a Certification Authority (CA) provided as part of a Public Key Infrastructure (PKI).

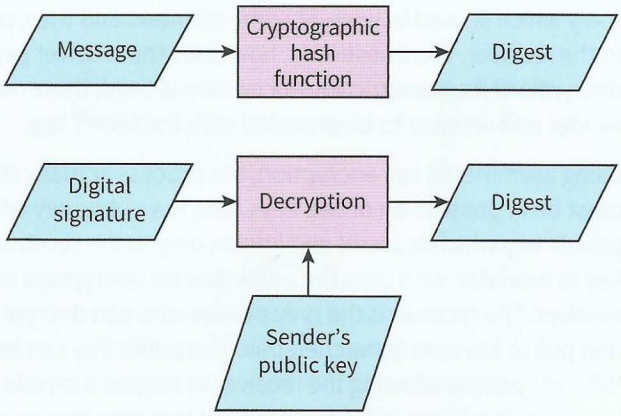

Figure 21.03 Checking received transmissions

Let's consider a would-be receiver who has a public–private key pair. This individual wishes to be able to receive secure messages from other individuals. The public key must be made available in a way that ensures authentication. The steps taken by the would-be receiver to obtain a digital certificate to allow safe public key delivery are illustrated in Figure 21.04. The process can be summarised as follows:

- An individual (person A) who is a would-be receiver and has a public–private key pair contacts a local CA.
- The CA confirms the identity of person A.
- Person A's public key is given to the CA.
- The CA creates a public-key certificate (a digital certificate) and writes person A's public key into this document.
- The CA uses encryption with the CA's private key to add a digital signature to this document.
- The digital certificate is given to person A.
- Person A posts the digital certificate on a website.

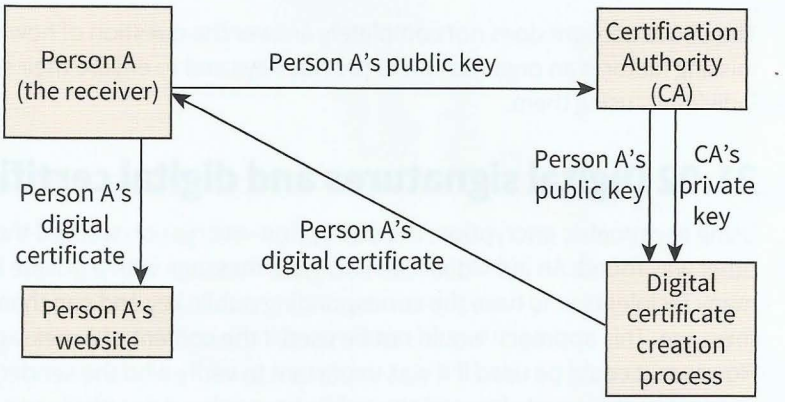

Figure 21.04 Processes involved in obtaining a digital certificate

Figure 21.04 has person A placing the digital certificate on that person's website but another option is to post it on a website designed specifically for keeping digital certificate data. Alternatively, a digital certificate might be used solely for authenticating emails as was suggested in Chapter 8 (Section 8.02).

Once a signed digital certificate has been posted on a website, any other person wishing to use person A's public key downloads the signed digital certificate from the website and uses the CA's public key to extract person A's public key from the digital certificate.

For this overall process to work there is a need for standards to be defined. As ever, the name for the standard, X.509, is not very memorable.

21.03 SSL and TLS

Secure Socket Layer (SSL) and Transport Layer Security (TLS) are two closely related protocols providing security in using the Internet. TLS is a slightly modified version of SSL. We concentrate on SSL here. The main context for the use of SSL is a client–server application. As described in Chapter 17 (Section 17.04), the interface between an application and TCP uses a port number. In the absence of a security protocol, TCP services an application using the port number. The combination of an IP address and a port number is called a 'socket'. When the Secure Socket Layer protocol is implemented it functions as an additional layer between TCP in the transport layer and the application layer. When the SSL protocol is in place, the application protocol HTTP becomes HTTPS. Note that although SSL is referred to as a protocol, it is in fact a protocol suite.

The starting point for SSL implementation is a connection between the client and the server being established by TCP. The Handshake Protocol from the SSP suite is used to create a session to allow the client and the server to communicate. Once the session has been established, the client and server can agree which encryption algorithms are to be used and can define the values for the session keys that are to be used. This interchange may involve checking digital certificates. For the transmission, SSL provides encryption, compression of the data and integrity checking. When the transmission is complete the session is closed and all records of the encryption disappear.

An application running HTTPS can guarantee secure communication allowing users to send confidential information such as credit card details in an ecommerce transaction. The user is completely unaware of the processes involved in ensuring confidential transmission with data integrity assured.

Discussion Point:

Chapter 8 (Section 8.01) discussed security and privacy issues. The use of encryption has always been a controversial subject. There are two important aspects to this. The first is whether powerful, unbreakable encryption algorithms should be made available to the public. The second relates to the key escrow scheme, which allows governments access to all secret keys. You may wish to revisit your Chapter 8 discussions.

21.04 Malware

Types of malware

Malware is the colloquial name for malicious software. Malicious software is software that is introduced into a system for a harmful purpose. One category of malware is where program code is introduced to a system. The various types of malware-containing program code are:

- virus: tries to replicate itself inside other executable code
- worm: runs independently and propagates to other network hosts
- logic bomb: lies dormant until some condition is met
- Trojan horse: replaces all or part of a previously useful program
- spyware: collects information and transmits it to another system
- bot: takes control of another computer and uses it to launch attacks.

The differences between the different types are not large and what is always called an 'anti-virus' package will detect all of the different types. The virus category is often subdivided according to the software that the virus attaches itself to. Examples are boot sector viruses and macro viruses.

Malware can also be classified in terms of the activity involved:

- phishing: sending an email or electronic message from an apparently legitimate source requesting confidential information
- pharming: setting up a bogus website which appears to be a legitimate site
- keylogger: recording keyboard usage by the legitimate user of the system.

System vulnerabilities

Many system vulnerabilities are associated directly with the activities of legitimate users of a system. Malware can be introduced inadvertently by the user in a number of ways:

- attaching a portable storage device
- opening an email attachment
- accessing a website
- downloading a file from the Internet.

Alternatively, a legitimate user with a grievance might introduce malware deliberately.

Other vulnerabilities are indirectly associated with the activities of legitimate users. By far the most significant is the use of weak passwords and particularly those which have a direct connection to the user. A poor choice of password gives the would-be hacker a strong chance of being able to gain unauthorised access. Other examples include a legitimate user not recognising a phishing or pharming attack and, as a result, disclosing sensitive information.

Systems inherently lack optimum security. Operating systems are notorious for lacking good security. There is a tendency for operating systems to increase in complexity which tends to offer the potential for more insecurity. The regular updates are often required because of a newly discovered security vulnerability. In the past, commonly used application packages have allowed macro viruses to flourish but this particular problem is largely under control.

A very specific vulnerability is buffer overflow. Programs written in the C programming language, of which there are very many, do not automatically carry out array bound checks. A program can be written to deliberately write code to the part of memory that is outside the address range defined for the array implemented as a buffer. This will overwrite what is stored there so when a subsequent program reads this overwritten section it will not execute as it should. This might just cause minor disruption but if cleverly engineered it could lead to an attacker gaining unauthorised access to the system and causing serious problems.

Chapter 8 (Section 8.02) has a discussion of the standard security measures for computer systems such as firewalls and anti-virus software.

Summary

- Alternatives for encryption are symmetric, using one key, or asymmetric, using two different keys.
- Encryption converts plaintext to ciphertext; decryption reverses the process.
- The five main security concerns when transmitting messages are: confidentiality, authenticity, integrity, non-repudiation and availability.
- Authentication can be achieved using a digital signature and a digital certificate.
- A digital certificate is provided by a certification authority within a public key infrastructure.
- Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocols provide security for transmissions using the Internet.
- The following are types of malware: virus, worm, logic bomb, Trojan horse, spyware and bot.
- Malicious activities include pharming, phishing, keylogging and hacking.
- Malware can inadvertently enter a system through a user attaching a portable storage device, opening an email attachment, accessing a website or downloading a file from the Internet.

Exam-style Questions

1 a When transmitting data across a network three concerns relate to: confidentiality, authenticity and integrity.
Explain each of these terms. [4]

b Encryption and decryption can be carried out using a symmetric or an asymmetric key method.
Explain how keys are used in each of these methods. You are not required to describe the algorithms used.
Your account must include reference to a public key, a private key and a secret key. [6]

c Digital signatures and digital certificates are used in message transmission.
Give an explanation of their use. [5]

2 Malware is a serious concern for computer system users.

a Give the names of two types of malware which involve some malicious code being input into a system. [2]

b Explain the difference between the two types of code. [3]

c Identify and explain two approaches for preventing malicious code from entering a computer system. [4]

d Explain the terms 'phishing' and 'pharming'. [3]

e Identify one possible policy for reducing the threat from phishing or pharming. [2]