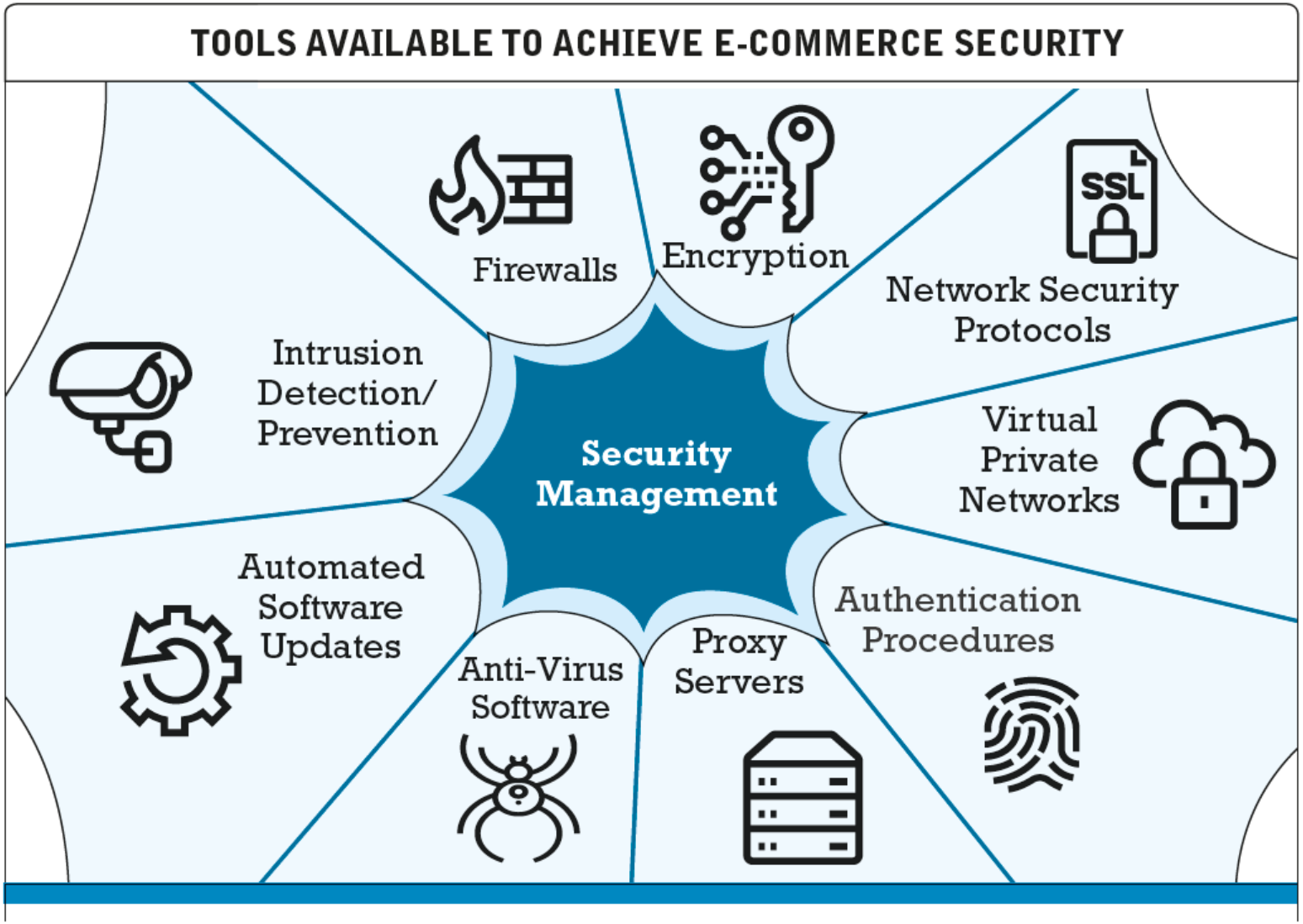
Part III:

Technology Solutions

2. Technology Solutions

技術解決方案



2. Technology Solutions

技術解決方案

- Protecting Internet communications 保護互聯網通信
  - Encryption 加密
- Securing channels of communication 保護通信信道
  - SSL, TLS, VPNs, Wi-Fi

    安全套接層、安全傳輸層、虛擬專用網，無綫網絡
- Protecting networks 網絡保護
  - Firewalls, proxy servers, IDS, IPS

    防火墻、包過濾、入侵檢測系統，入侵防禦系統
- Protecting servers and clients 保護服務器和客戶機
  - OS security, anti-virus software

    提升操作系統安全、 殺毒軟件

2. Technology Solutions

技術解決方案

Protecting Internet Communications

保護互聯網的通信

- Because e-commerce transactions must flow over the public Internet, and therefore involve thousands of routers and servers through which the transaction packets flow, the greatest security threats occur at the level of Internet communications. A number of tools are available to protect the security of Internet communications, the most basic of which is message encryption.

  由於電子商務交易必須通過公共的互聯網進行，數據包在傳遞過程中經過數以千計的路由器和服務器，最大的安全威脅發生在互聯網通信層面．有許多工具可用於保護互聯網通信的安全，其中最基本的是消息加密．

2. Technology Solutions

技術解決方案

Encryption 加密

- **Encryption** is the process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and the receiver.

  加密是將文本或數據轉換爲除發送方和接收方以外的任何人都無法讀取的密文的過程.

- Secures stored information and information transmission.

  保證存儲信息和信息傳送的安全.

- Provides 4 of 6 key dimensions of e-commerce security:

  為電子商務安全的6個關鍵維度中的4個維度提供保障:

  - **Message integrity 信息完整性**
    Provides assurance that the message has not been altered.
    提供消息未被更改的保障
  - **Nonrepudiation 不可否認性**
    Prevents the user from denying he or she sent the message.
    防止用戶否認曾經發送過的信息
  - **Authentication 真實性**
    Provides verification of the identity of the person/computer sending the message.
    提供對發送消息的人（或計算機）的身份驗證
  - **Confidentiality 機密性**
    Gives assurance that the message was not read by others.
    確保證信息不被他人讀取

2. Technology Solutions

技術解決方案

Encryption 加密

- This transformation of plain text to cipher text is accomplished by using a key or cipher. A key (or cipher) is any method for transforming plain text to cipher text.
  從明文到密文的轉換是通過使用密鑰或密碼來完成的. 密鑰（或密碼）就是把明文轉換爲密文的任何方法.
- In a **substitution cipher**, every occurrence of a given letter is replaced systematically by another letter. If we used the cipher "letter plus two"—the word "HELLO" in plain text would be transformed into the g cipher text: "JGNNQ."
  在**替換密碼**中，每個給定字母都會被另一個字母替換. 如果我們使用密碼“字母加二”——明文單詞“HELLO”將被轉換爲密文： “JGNNQ”.
- In a **transposition cipher**, the ordering of the letters in each word is changed in some systematic way, such as the word "Hello" can be written backwards as "OLLEH". A more complicated cipher would (1) break all words into two words and (2) spell the first word with every other letter, beginning with the first letter, and then spell the second word with all the remaining letters. In this cipher, "HELLO" would be written as "HLO EL".
  在**調位密碼**中，每個單詞中字母的順序以某種系統的方式改變，例如單詞“HELLO”可以倒寫爲“OLLEH”. 更爲複雜的密碼可以是：(a)將整個單詞拆分爲兩部分；(b)第一部分由每兩個字母中的第一個字母組成，第二部分由剩下的所有字母組成. 在這種加密方式中，“HELLO”將寫爲“HLO EL”.

2. Technology Solutions

技術解決方案

Encryption 加密

——Symmetric Key Cryptography 對稱密鑰加密

- Also called Secret Key Cryptography

  亦被稱爲私鑰加密
- Sender and receiver use same digital key to encrypt and decrypt message.

  發送方和接收方使用同一把密鑰來加密和解密信息.
- Sender and receiver have to send it over some communication media or exchange the key in person. Symmetric key cryptography was used extensively throughout World War II and is still a part of Internet cryptography.

  發送方和接收方必須通過某種通信媒體來發送密鑰或當面交換密鑰. 對稱密鑰加密在二戰期間被廣泛使用，現在仍然在互聯網加密中使用.

2. Technology Solutions

技術解決方案

Encryption 加密

——Symmetric Key Cryptography 對稱密鑰加密

- Modern encryption systems are digital. The ciphers or keys used to transform plain text into cipher text are digital strings. Computers store text or other data as binary strings composed of 0s and 1s. The strength of modern security protection is measured in terms of the length of the binary key used to encrypt the data. For example, the eight-bit key has 2^8 or 256 possibilities.

  現代加密系統是數字化的. 用於明文轉換爲密文的密碼或密鑰是數字串. 計算機將文本或其他數據存儲爲由0和1組成的二進制字符串. 現代安全保護的强度是用加密數據所使用的二進制密鑰的長度來衡量的. 例如八位密鑰有 2^8 (256) 種可能性.

2. Technology Solutions

技術解決方案

Encryption 加密

——Symmetric Key Cryptography 對稱密鑰加密

- **Data Encryption Standard (DES)** was developed by the National Security Agency (NSA) and IBM in the 1950s. DES uses a 56-bit encryption key. To cope with much faster computers, it has been improved by the Triple DES Encryption Algorithm (TDEA)—essentially encrypting the message three times, each with a separate key.

  數據加密標準由美國國家安全局和IBM在1950年代開發. DES使用56位加密密鑰. 爲了應對速度更快的計算機，它通過三重DES加密算法進行了改進——本質上是對消息進行三次加密，每次使用單獨的密鑰.

- **Advanced Encryption Standard (AES)** is a widely used symmetric key algorithm, which offers key sizes of 128, 192, and 256 bits.

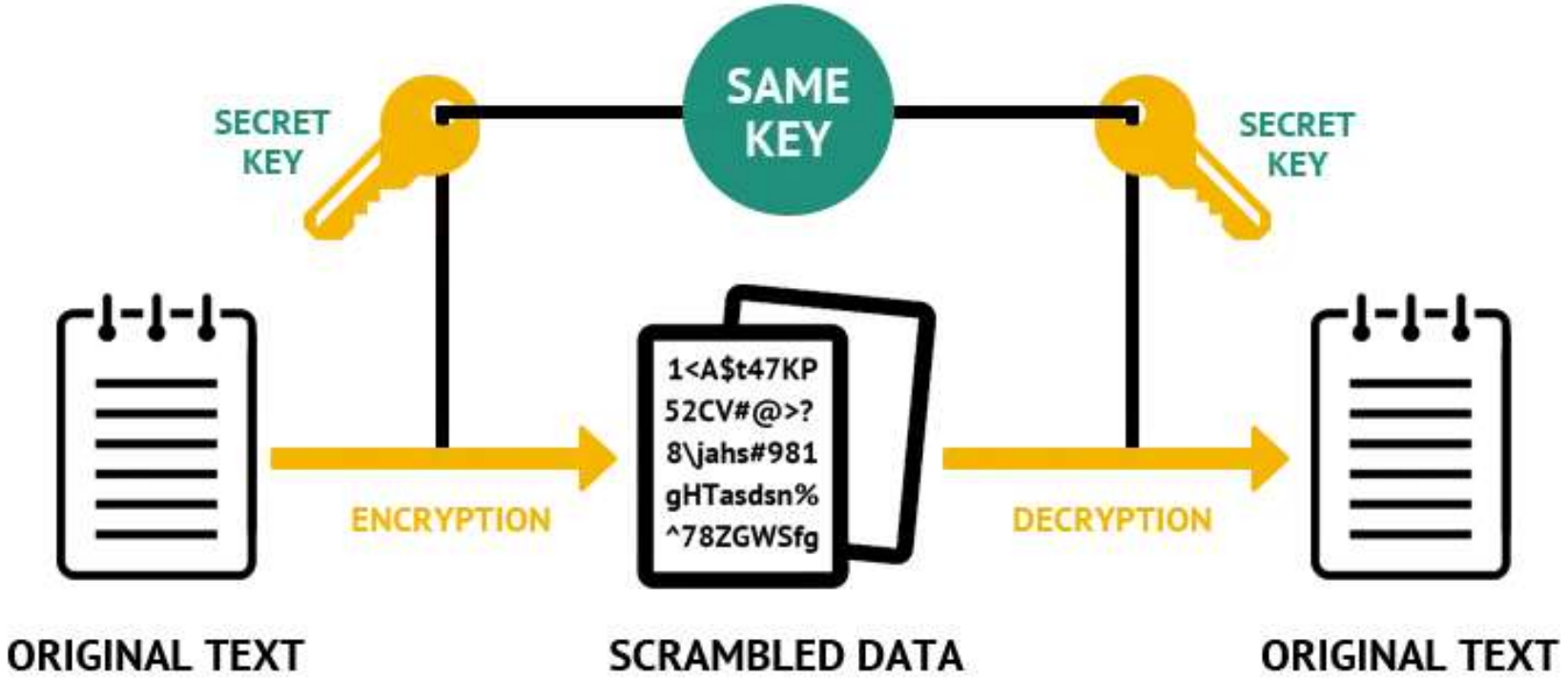
  高級加密標準是一種廣泛使用的對稱密鑰算法，提供128、192 和 256 位的加密密鑰.

2. Technology Solutions

技術解決方案

Encryption 加密

——Symmetric Key Cryptography 對稱密鑰加密



2. Technology Solutions

技術解決方案

Encryption 加密

——Public Key Cryptography 公鑰加密

- Also called Asymmetric Cryptography
  亦被稱爲非對稱加密
- Uses two mathematically related digital keys
  采用兩個算術上相關的數字密鑰
  - Public key (widely disseminated)
    公鑰（廣泛發布）
  - Private key (kept secret by owner)
    私鑰（由所有者保密）
- Both keys used to encrypt and decrypt message
  兩個密鑰都可以用來加密和解密信息
- Once key used to encrypt message, same key cannot be used to decrypt message
  一旦某個密鑰被用來加密信息，就不能再用它來解密信息
- Sender uses recipient’s public key to encrypt message; recipient uses private key to decrypt it
  發件人使用收件人的公鑰加密郵件；收件人使用私鑰解密郵件

2. Technology Solutions

技術解決方案

Encryption 加密

——Public Key Cryptography 公鑰加密

- The mathematical algorithms used to produce the keys are one-way functions. A one-way irreversible mathematical function is one in which, once the algorithm is applied, the input cannot be subsequently derived from the output.

  用於生成密鑰的數學算法是單向函數. 利用這種單向不可逆數學函數作爲來算法，是無法從輸出信息中倒推出輸入信息的.

2. Technology Solutions

技術解決方案

Encryption 加密

——Public Key Cryptography 公鑰加密

PUBLIC KEY CRYPTOGRAPHY—A SIMPLE CASE

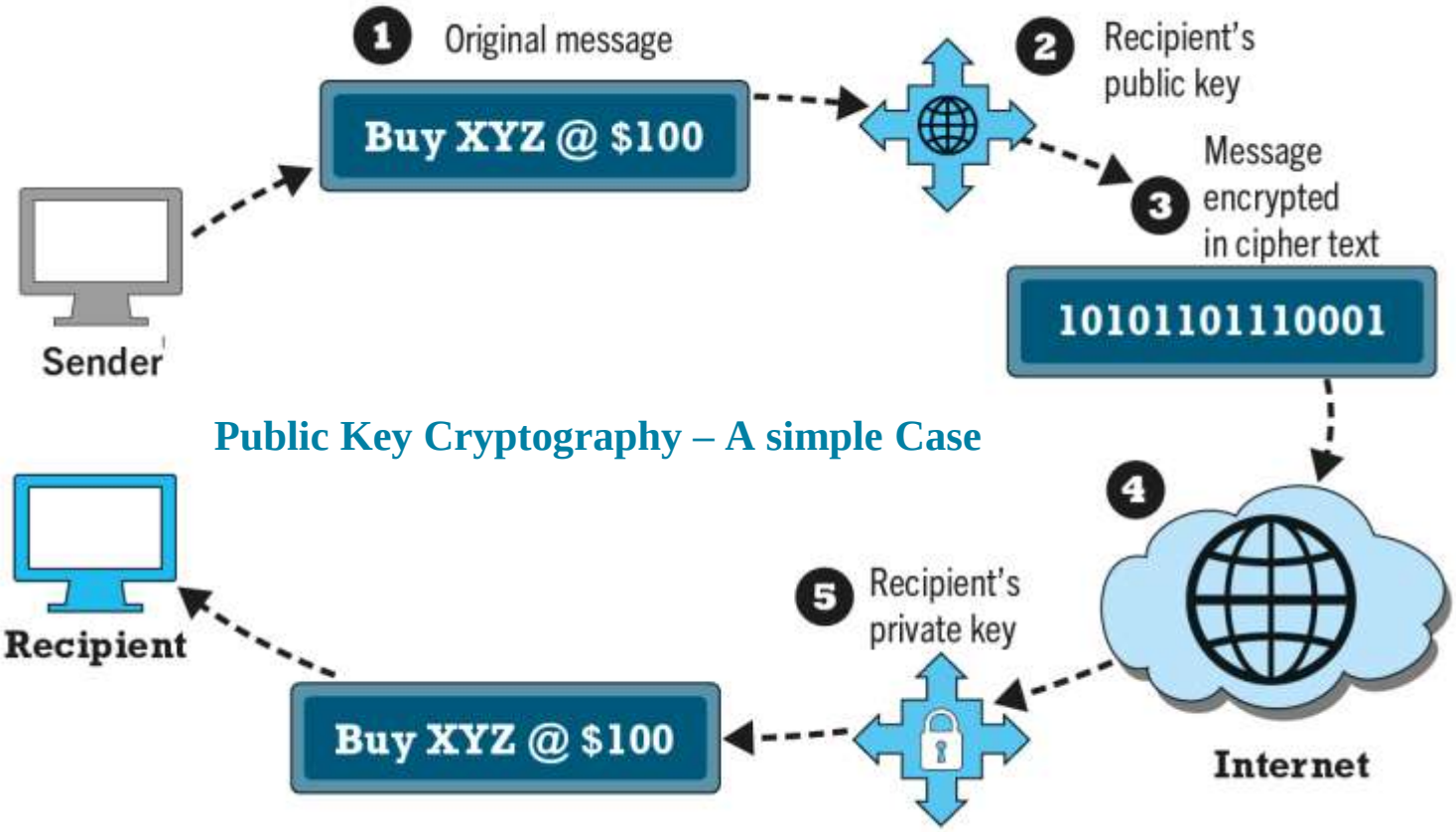
STEP	DESCRIPTION
1. The sender creates a digital message.	The message could be a document, spreadsheet, or any digital object.
2. The sender obtains the recipient's public key from a public directory and applies it to the message.	Public keys are distributed widely and can be obtained from recipients directly.
3. Application of the recipient's key produces an encrypted cipher text message.	Once encrypted using the public key, the message cannot be reverse-engineered, or unencrypted, using the same public key. The process is irreversible.
4. The encrypted message is sent over the Internet.	The encrypted message is broken into packets and sent through several different pathways, making interception of the entire message difficult (but not impossible).
5. The recipient uses the recipient's private key to decrypt the message.	The only person who can decrypt the message is the person who has possession of the recipient's private key. Hopefully, this is the legitimate recipient.

2. Technology Solutions

技術解決方案

Encryption 加密

——Public Key Cryptography 公鑰加密



Public Key Cryptography – A simple Case

2. Technology Solutions

技術解決方案

Encryption 加密

——Public Key Cryptography 公鑰加密

- In the simplest use of public key cryptography, the sender encrypts a message using the recipient's public key and then sends it over the Internet. The only person who can decrypt this message is the recipient, using the recipient's private key. However, this simple case does not ensure integrity or an authentic message.

  在最簡單的公鑰加密使用中，發送方使用接收方的公鑰加密消息，然後通過Internet發送消息．只有接收方可使用其私鑰解密此消息．但是，這種最簡單的情況並不能確保消息的完整性或真實性.

2. Technology Solutions

技術解決方案

Encryption 加密

Factors	Symmetric Key Cryptography	Asymmetric Key Cryptography/Public Key Cryptography
Size of cipher text	The same or smaller than the original plain text	The same or larger than the original plain text
Data size	Used for large amounts of data	Used for small amounts of data
Resource Utilization	Low	High
Key Lengths	128 or 256 bits	2048 or higher
Security	Less secure as only one key is used for both encryption and decryption	More secure as two keys are used, one for encryption and the other for decryption
Number of keys	One key for both encryption and decryption	Two keys, a public key and a private key, one for encryption and the other for decryption
Techniques	Provides confidentiality	Provides confidentiality, authenticity, and non-repudiation
Confidentiality	Only the key holder can decrypt the message	Only the private key holder can decrypt the message
Speed	Fast	Slow
Algorithms	3DES, AES, DES, etc.	Diffie-Hellman, ECC, DSA, RSA, etc.

2. Technology Solutions

技術解決方案

Encryption 加密

——Public Key Cryptography Using Digital Signatures and Hash Digests

使用數字簽名和hash摘要的公鑰加密

- In public key cryptography, some elements of security are missing. Although one can be quite sure the message was not understood or read by a third party (message confidentiality), there is no guarantee that the sender really is the sender—that is, there is no authentication of the sender. This means the sender could deny ever sending the message (repudiation). And there is no assurance that the message was not altered somehow in transit. For example, the message “Buy Cisco @ $16” could have been accidentally or intentionally altered to read “Sell Cisco @ $16.” This suggests a potential lack of integrity in the system. The public key cryptography using digital signatures and hash digests can achieve authentication, nonrepudiation, and integrity.

在公鑰加密體系中，缺少某些安全性元素. 儘管人們可以確信消息不會被第三方讀取（機密性），但不能保證發送者確實是發送方. 也就是說，沒有對發送方的身份進行驗證. 這意味著發送方可以否認發送過消息，並且不能保證郵件在傳輸過程中沒有被篡改. 例如，消息“Buy Cisco @ $16”可能被有意或無意地篡改爲“Sell Cisco@$16”. 這表明這一加密體系可能缺乏完整性. 使用數字簽名和Hash摘要的公鑰加密可以實現真實性、不可否認性和完整性.

2. Technology Solutions

技術解決方案

Encryption 加密

——Public Key Cryptography Using Digital Signatures and Hash Digests

使用數字簽名和hash摘要的公鑰加密

Step

- To check the integrity of a message and ensure it has not been altered in transit, a hash function is first used to create a digest of the message. The results of applying the hash function are sent by the sender to the recipient. Upon receipt, the recipient applies the hash function to the received message and checks to verify that the same result is produced. If so, the message has not been altered.
  爲了檢查消息的完整性並確保消息在傳輸過程中沒有被篡改，首先使用hash函數來創建消息的摘要. 發送方把使用hash函數後的結果發送給接收方. 接收方收到信息後，將同一hash函數應用於接收到的消息，並核對是否有相同的結果. 如果是，則證明該消息尚未被篡改.
- The sender then encrypts both the hash result and the original message using the recipient's public key, producing a single block of cipher text.
  發送方然後使用接收方公鑰對散列結果和原始消息進行加密，從而生成單一的密文塊.
- One more step is required. To ensure the authenticity of the message and to ensure nonrepudiation, the sender encrypts the entire block of cipher text one more time using the sender's private key. This produces a digital signature (also called an e-signature) or "signed" cipher text that can be sent over the Internet.
  還需要一個步驟. 爲了確保消息的真實性並確保不可否認性，發送方使用私鑰再對整個密文塊進行一次加密. 這就產生了數字簽名，也稱爲電子簽名或簽名密文.

2. Technology Solutions

技術解決方案

Encryption 加密

——Public Key Cryptography Using Digital Signatures and Hash Digests

使用數字簽名和hash摘要的公鑰加密

- The recipient of this signed cipher text first uses the sender's public key to authenticate the message. Once authenticated, the recipient uses the recipient's private key to obtain the hash result and original message. As a final step, the recipient applies the same hash function to the original text and compares the result with the result sent by the sender. If the results are the same, the recipient knows the message has not been changed during transmission. The message thus has integrity.

  接收方收到這種簽名密文後，首先使用發送方的公鑰來驗證郵件. 身份驗證通過後，接收方將使用其私鑰來獲取hash結果和原始消息. 最後，接收方將相同的hash函數應用於原始消息，並將結果與發送方發送的結果進行比較. 如果結果相同，則接收方就知道消息在傳輸過程中沒有被篡改，消息具有完整性.

Step

2. Technology Solutions

技術解決方案

Encryption 加密

——Public Key Cryptography Using Digital Signatures and Hash Digests

使用數字簽名和hash摘要的公鑰加密

- A **hash function** is an algorithm that produces a fixed-length number called a hash or message digest. A hash function can be simple and count just the number of digital 1s in a message, or it can be more complex and produce a 128-bit number that reflects the number of 0s and 1s, the number of 00s and 11s, and so on. Standard hash functions are available (MD4 and MD5 produce 128- and 160-bit hashes, respectively). These more complex hash functions produce hashes or hash results that are unique to every message.

hash函數是一種產生固定長度數字的算法. hash函數可以很簡單，可以計算消息中數字“1”的數量；也可以更複雜，可以生成一個128位數字字符串，以反映信息中0的個數、1的個數、00的個數、11的個數等可以使用標準的hash函數（MD4和MD5生成128位和160位的hash值）. 這些更複雜的散列函數可以針對每條消息產生唯一的hash結果.

2. Technology Solutions

技術解決方案

Encryption 加密

——Public Key Cryptography Using Digital Signatures and Hash Digests

使用數字簽名和hash摘要的公鑰加密

- A digital signature (also called an e-signature) is “signed” cipher text that can be sent over the Internet. A digital signature is a close parallel to a handwritten signature. Like a handwritten signature, a digital signature is unique—only one person presumably possesses the private key. When used with a hash function, the digital signature is even more unique than a handwritten signature. In addition to being exclusive to a particular individual, when used to sign a hashed document, the digital signature is also unique to the document and changes for every document. Early digital signature programs required the user to have a digital certificate and were far too difficult for an individual to use. Newer programs are Internet-based and do not require users to install software or understand digital certificate technology.

數字簽名（也稱爲電子簽名）是可以通過Internet發送的“簽名”密文. 數字簽名與手寫簽名非常相似. 像手寫名一樣，數字名也是唯一的. 當與散列函數一起使用時，數字簽名甚至比手寫簽名更獨特. 除了用於特定個人之外，數字簽名在用於簽名散列文檔時，對於文檔也是唯一的，並且對每個文檔都是不同的. 早期的數字簽名程序要求用戶擁有數字證書，並且個人使用起來非常困難. 較新的程序是基於互聯網的，不需要用戶安裝軟件或瞭解數字證書技術.

2. Technology Solutions

技術解決方案

Encryption 加密

——Public Key Cryptography Using Digital Signatures and Hash Digests

使用數字簽名和hash摘要的公鑰加密

PUBLIC KEY CRYPTOGRAPHY WITH DIGITAL SIGNATURES	
STEP	DESCRIPTION
1. The sender creates an original message.	The message can be any digital file.
2. The sender applies a hash function, producing a 128-bit hash result.	Hash functions create a unique digest of the message based on the message contents.
3. The sender encrypts the message and hash result using the recipient's public key.	This irreversible process creates a cipher text that can be read only by the recipient using the recipient's private key.
4. The sender encrypts the result, again using the sender's private key.	The sender's private key is a digital signature. There is only one person who can create this digital mark.
5. The result of this double encryption is sent over the Internet.	The message traverses the Internet as a series of independent packets.
6. The receiver uses the sender's public key to authenticate the message.	Only one person, namely, the sender, can send this message.
7. The receiver uses the receiver's private key to decrypt the hash function and the original message. The receiver checks to ensure that the original message and the hash function results conform to one another.	The hash function is used here to check the original message. This ensures that the message was not changed in transit.

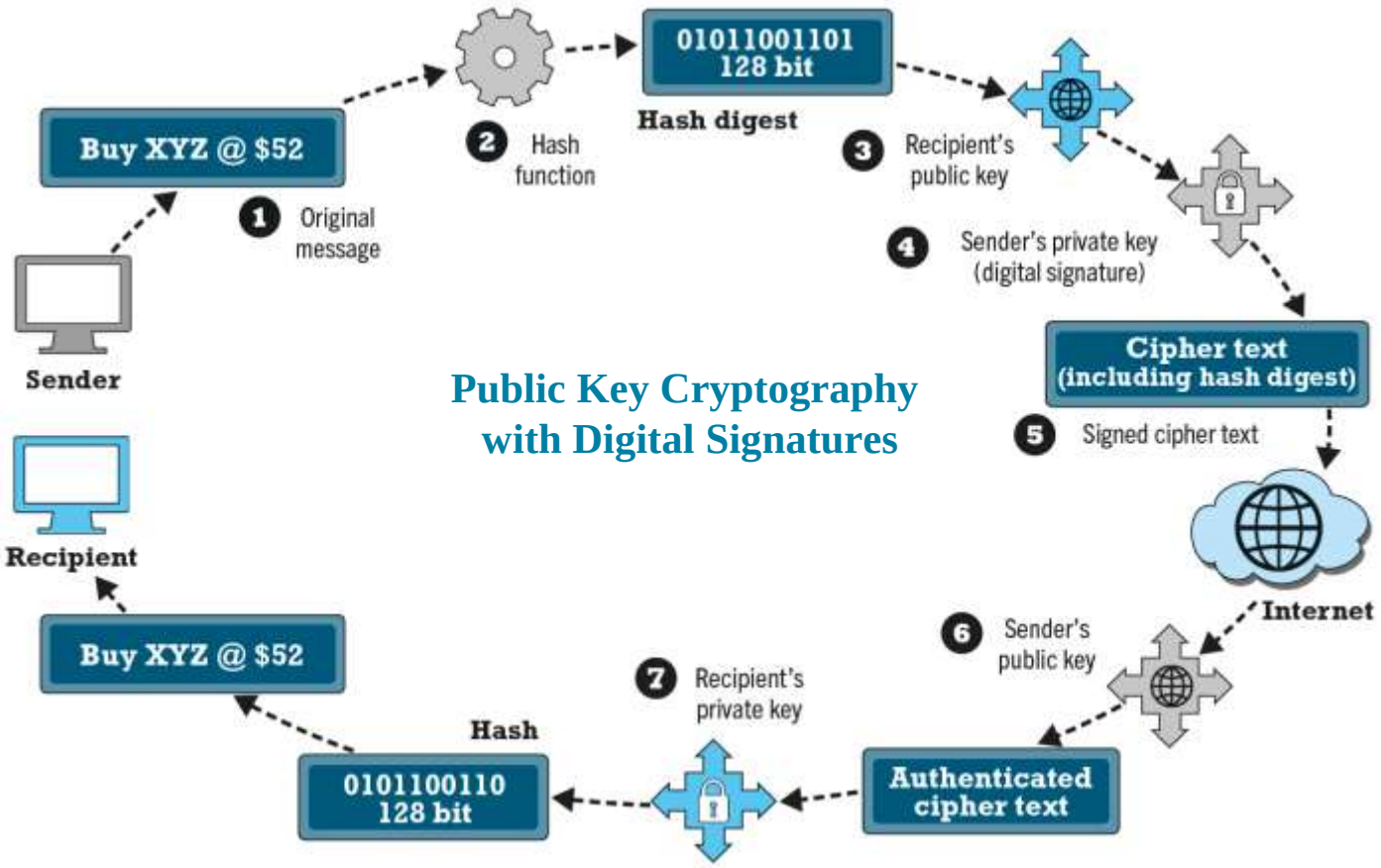
2. Technology Solutions

技術解決方案

Encryption 加密

——Public Key Cryptography Using Digital Signatures and Hash Digests

使用數字簽名和hash摘要的公鑰加密



2. Technology Solutions

技術解決方案

Encryption 加密

——Digital Envelopes 數字信封

- Public key cryptography is computationally slow. If one used 128- or 256-bit keys to encode large documents significant declines in transmission speeds and increases in processing time would occur. Symmetric key cryptography is computationally faster, but it has a weakness—namely, the symmetric key must be sent to the recipient over insecure transmission lines. One solution is to use the more efficient symmetric encryption and decryption for large documents, but public key cryptography to encrypt and send the symmetric key. This technique is called using a **digital envelope**.

  公鑰加密體系在計算速度上很慢. 如果一個人使用128位或256位密鑰對大型文檔進行編碼，則傳輸速度將顯著下降，並且處理時間會增加. 對稱密鑰加密算法的計算速度更快，但它有一個弱點即對稱密鑰必須通過不安全的傳輸介質發送給接收方. 解決這一問題的一個方法是對大型文檔使用更有效的對稱加密和解密，使用公鑰加密體系來加密和發送對稱密鑰. 這種技術稱爲**數字信封**.

2. Technology Solutions

技術解決方案

Encryption 加密

——Digital Envelopes 數字信封

- A simple case: A diplomatic document is encrypted using a symmetric key. The symmetric key—which the recipient will require to decrypt the document—is itself encrypted, using the recipient's public key. So we have a "key within a key" (a digital envelope). The encrypted report and the digital envelope are sent across the Web. The recipient first uses his/her private key to decrypt the symmetric key, and then the recipient uses the symmetric key to decrypt the report. This method saves time because both encryption and decryption are faster with symmetric keys.

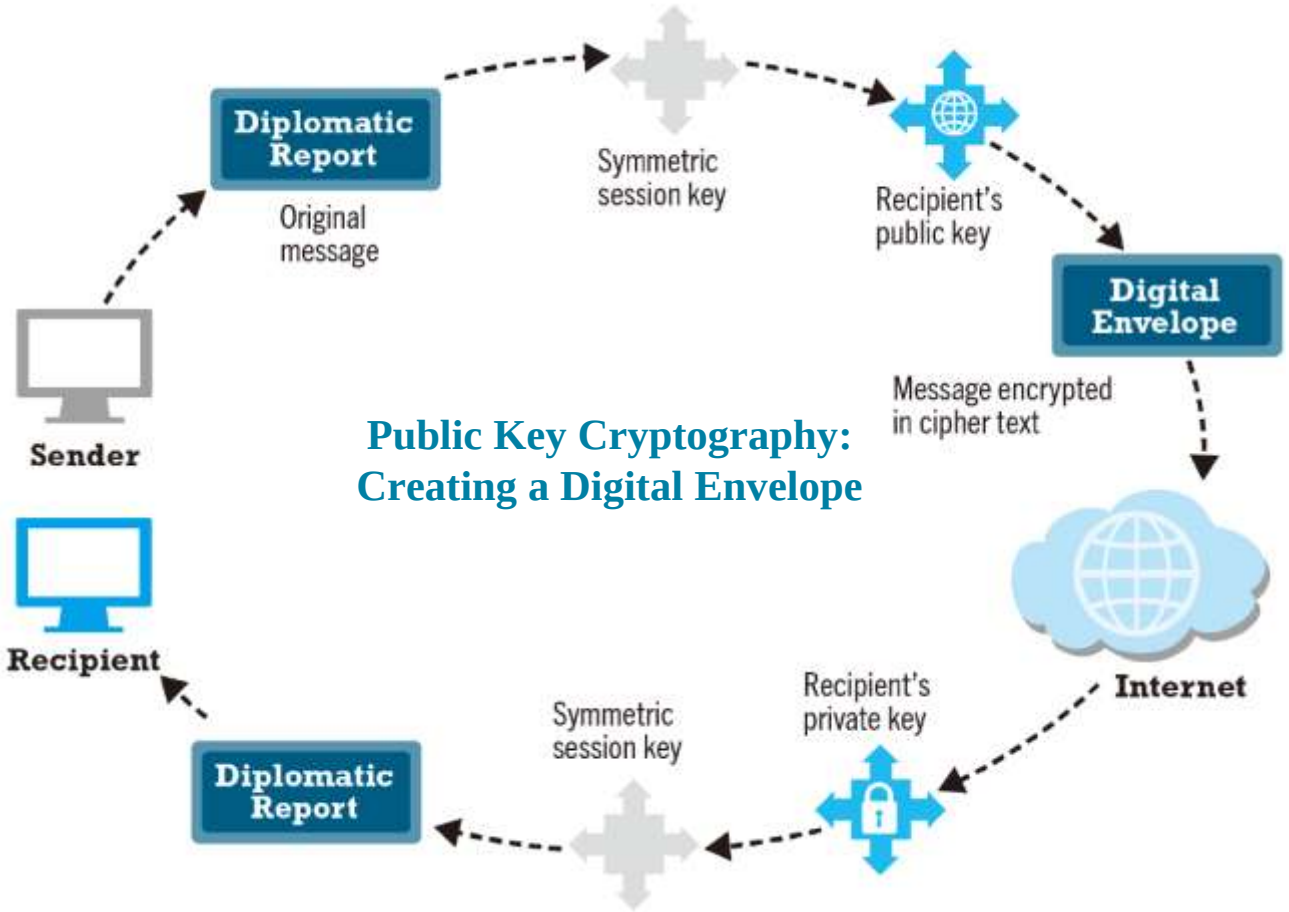
  一個簡單例子：使用對稱密鑰對原始消息進行加密. 對稱密鑰（接收方需要解密該對稱密鑰）本身使用接收方的公鑰進行加密. 因此，我們有一個"密鑰中的密鑰"（數字信封）. 加密的消息和數字信封通過網絡傳輸. 隨後，接收方首先使用他的私鑰解密對稱密鑰，然後接收方使用對稱密鑰解密消息. 該方法節省了時間，因爲使用對稱密鑰加密和解密速度都更快.

2. Technology Solutions

技術解決方案

Encryption 加密

——Digital Envelopes 數字信封



Public Key Cryptography: Creating a Digital Envelope

2. Technology Solutions

技術解決方案

Encryption 加密

——Digital Certificates Digital Certificates and Public Key Infrastructure

數字證書和公鑰基礎設施

- There are still some deficiencies in the message security regime described previously. How do we know that people and institutions are who they claim to be? Anyone can make up a private and public key combination and claim to be someone they are not. In the digital world, we need a way to know who people and institutions really are.

  前面介紹的信息安全措施仍然存在一些缺陷. 我們怎麼知道人和機構就是他們所聲稱的那個?任何人都可以製作一套私鑰和公鑰，然後聲稱自己是某某人. 在數字世界中我們需要一種方法來瞭解人和機構的真實身份.

- Digital certificates, and the supporting public key infrastructure, are an attempt to solve this problem of digital identity.

  數字證書和其所支持的公鑰基礎設施，都是試圖解決數字身份問題的嘗試.

2. Technology Solutions

技術解決方案

Encryption 加密

——Digital Certificates Digital Certificates and Public Key Infrastructure

數字證書和公鑰基礎設施

- A digital certificate is a digital document issued by a trusted third-party institution known as a **certification authority** (CA) that contains:
  數字證書是由受信任第三方機構即**認證中心**頒發的數字文件，其中包含：
  - Name of subject/company 主體或公司名稱
  - Subject's public key 主體公鑰
  - Digital certificate serial number 數字證書序列號
  - Expiration date, issuance date 有效日期、簽發日期
  - Digital signature of CA 認證中心的數字簽名
  - Other identifying information 其他標識信息

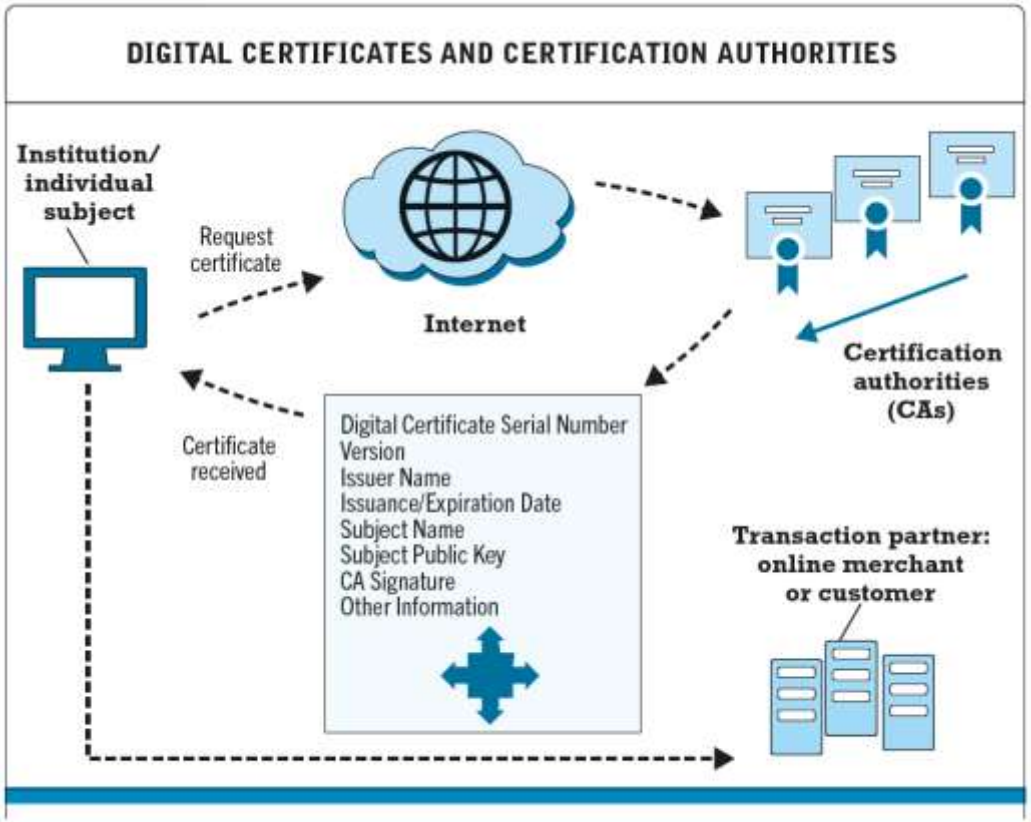
2. Technology Solutions

技術解決方案

Encryption 加密

——Digital Certificates Digital Certificates and Public Key Infrastructure

數字證書和公鑰基礎設施



The PKI includes certification authorities that issue, verify, and guarantee digital certificates that are used in e-commerce to ensure the identity of transaction partners.

2. Technology Solutions

技術解決方案

Encryption 加密

——Digital Certificates Digital Certificates and Public Key Infrastructure

數字證書和公鑰基礎設施

- Worldwide, thousands of organizations issue CAs. A hierarchy of CAs has emerged with less well-known CAs being certified by larger and better-known CAs, creating a community of mutually verifying institutions. **Public key infrastructure** (PKI) refers to the CAs and digital certificate procedures that are accepted by all parties. When you sign into a "secure" site, the URL will begin with "https", and a closed lock icon will appear on your browser. This means the site has a digital certificate issued by a trusted CA. It is not, presumably, a spoof site.

  全世界有成千上萬的機構頒發 CA. 信譽較好、規模較大的CA要爲不太知名的CA做認證，這就形成了一個相互認證的社區，CA是有層級的. **公鑰基礎設施**是指各方都接受的CA和數字證書程序. 當你登錄“安全”網站時，URL將以“https”開頭，並且一個關閉的鎖定圖標將出現在瀏覽器中. 這意味著該網站有一個可信任的CA頒發的數字證書，大概率不是虛假網站.

2. Technology Solutions

技術解決方案

Encryption 加密

——Digital Certificates Digital Certificates and Public Key Infrastructure

數字證書和公鑰基礎設施

- To create a digital certificate, the user generates a public/private key pair and sends a request for certification to a CA along with the user's public key. The CA verifies the information (how this is accomplished differs from CA to CA). The CA issues a certificate containing the user's public key and other related information. Finally, the CA creates a message digest from the certificate itself (just like a hash digest) and signs it with the CA's private key. This signed digest is called the signed certificate. We end up with a totally unique cipher text document—there can be only one signed certificate like this in the world.

  爲創建數字證書，用戶首先生成一個公鑰/私鑰對，並將認證請求與用戶的公鑰一起發送到 CA. CA驗證信息（不同CA的完成方式有所不同）. CA 頒發包含用戶公鑰和其他相關信息的證書. 最後，CA從證書本身創建消息摘要（就像hash摘要一樣），並使用CA的私鑰對其進行簽名. 該簽名摘要稱爲簽名證書. 我們最終得到了一個完全唯一的密文文件——世界上只有一個這樣的簽名證書.

2. Technology Solutions

技術解決方案

Encryption 加密

——Digital Certificates Digital Certificates and Public Key Infrastructure

數字證書和公鑰基礎設施

- There are several ways the certificates are used in commerce. Before initiating a transaction, the customer can request the signed digital certificate of the merchant and decrypt it using the merchant's public key to obtain both the message digest and the certificate as issued. If the message digest matches the certificate, then the merchant and the public key are authenticated. The merchant may in return request certification of the user, in which case the user would send the merchant his or her individual certificate. There are many types of certificates: personal, institutional, web server, software publisher, and CAs themselves.

  證書在商業中的使用方式有多種. 在開始交易前，用戶可以請求商家提供已簽名的數字證書，並使用商家的公鑰對其進行解密，從而獲取消息摘和已頒發的證書. 如果消息摘要與證書匹配，則商家和公鑰就是真實的. 同時，商家也可以請求驗證用戶的證書，在這種情況下，用戶將向商家發送他的個人證書. 證書有多種類型：個人證書、機構證書、web服務器證書、軟件發布者證書和CA自身的証書.

2. Technology Solutions

技術解決方案

Securing Channels of Communication 保密通信信道

——Transport Layer Security (TLS) and HTTPS

- The concepts of public key cryptography are used routinely for securing channels of communication.
  公鑰加密體系的原理通常用於保護通信通道的安全實踐中.
- Secure Sockets Layer (SSL) was the original protocol enabling secure communications over the Internet. Today, however, it has been replaced by the Transport Layer Security (TLS) protocol, which is an updated, more secure version of SSL. When you receive a message from a server on the Web with which you will be communicating through a secure channel, this means you will be using TLS to establish a secure negotiated session. (Notice that the URL changes from HTTP to HTTPS).
  SSL協議是啓用互聯網上安全通信的原始協議. 今天，它已被TLS協議取代，後者是SSL的更新、更安全的版本. 當你從通過安全通道與之通信的網絡上的服務器接收到一條消息時，這意味著你將使用TIS協議建立安全協商會話（請注意，URL從HTTP更改爲HTTPS）.

2. Technology Solutions

技術解決方案

Securing Channels of Communication 保密通信信道

——Transport Layer Security (TLS) and HTTPS

- A secure negotiated session is a client-server session in which the URL of the requested document, along with the contents, contents of forms, and the cookies exchanged, are encrypted. Through a series of handshakes and communications, the browser and the server establish one another's identity by exchanging digital certificates, decide on the strongest shared form of encryption, and then proceed to communicate using an agreed-upon session key. A session key is a unique symmetric encryption key chosen just for this single secure session. Once used, it is gone forever.

  安全協商會話是客戶機/服務器之間的會話，其中請求文檔的 URL以及表單內容和交換的cookies都進行了加密. 通過一系列的信號交換和通信，瀏覽器和服務器通過交換數字證書來確定彼此的身份，確定最强有力的共享加密形式，然後使用商定的會話密鑰進行通信. 會話密鑰是挑選出來的在單個安全會話中使用的唯一的對稱加密密鑰. 會話密鑰一旦用過，就永遠不會再次使用.

- In practice, most private individuals do not have a digital certificate. In this case, the merchant server will not request a certificate, but the client browser will request the merchant certificate once a secure session is called for by the server.

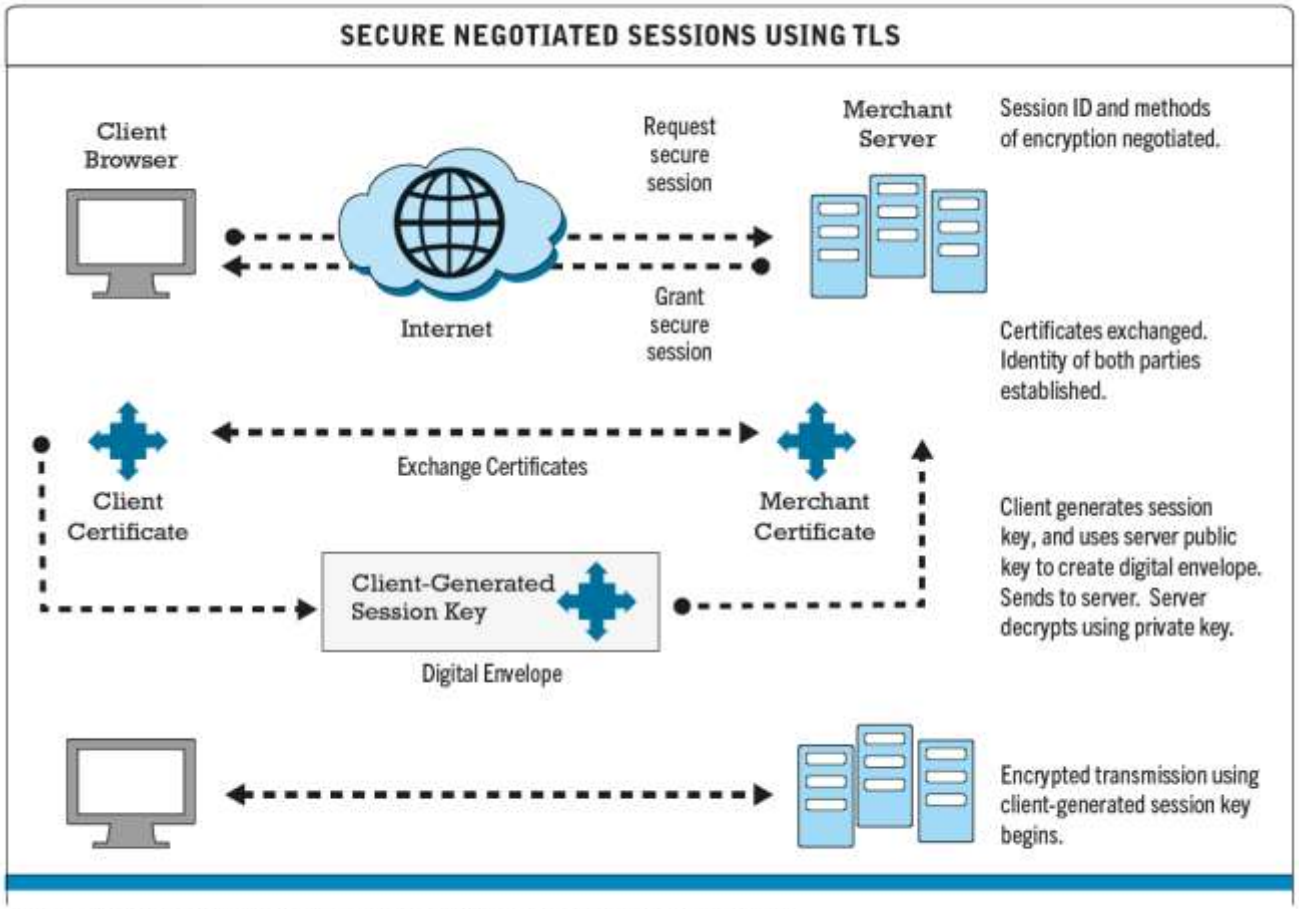
  實際上，大多數個人沒有數字證書. 在這種情況下，商家服務器將不要求個人的數字證書，但是一旦服務器調用安全會話，客戶機瀏覽器便會請求商家證書.

2. Technology Solutions

技術解決方案

Securing Channels of Communication 保密通信信道

——Transport Layer Security (TLS) and HTTPS



Certificates play a key role in using TLS to establish a secure communications channel.

2. Technology Solutions

技術解決方案

Securing Channels of Communication 保密通信信道

——Transport Layer Security (TLS) and HTTPS

- TLS provides data encryption, server authentication, optional client authentication, and message integrity for TCP/IP connections. TLS addresses the issue of authenticity by allowing users to verify another user's identity or the identity of a server. It also protects the integrity of the messages exchanged. However, once the merchant receives the encrypted credit and order information, that information is typically stored in unencrypted format on the merchant's servers. While TLS provides secure transactions between merchant and consumer, it guarantees only server-side authentication. Client authentication is optional. In addition, TLS cannot provide irrefutability—consumers can order goods or download information products and then claim the transaction never occurred.

TLS协議爲TCP/IP連接提供數據加密、服務器身份驗證、可選的客戶機身份驗證和消息完整性. TIS协議通過允許用戶驗證另一個用戶的身份或服務器的身份來解決真實性問題. 它還可以保護所交換消息的完整性. 但是，一旦商家接收到加密的信用卡和訂單信息，該信息通常就以未加密的格式存儲在商家的服務器上. 雖然TLS協議提供了商家和消費者之間的安全交易，但它只能保證服務器端的身份驗證. 客戶機的身份驗證是可選的. 此外，TIS協議不能提供不可否認性保護. 消費者可以訂購商品或下載信息產品，然後聲稱交易從未發生.

2. Technology Solutions

技術解決方案

Securing Channels of Communication 保密通信信道

——Transport Layer Security (TLS) and HTTPS

- TLS is used in conjunction with HTTPS, a secure version of the HTTP protocol that uses TLS for encryption and authentication. It is implemented by a server adopting the HTTP Strict Transport Security (HSTS) feature, which forces browsers to access the server using only HTTPS.

  TLS協議與HTTPS可結合使用，HTTPS是使用TLS協議進行加密和身份驗證的HTTP協議的安全版本. 它由采用HTTP嚴格傳輸安全(HSTS)特性的服務器實現，該功能强制瀏覽器使用HTTPS訪問服務器.

2. Technology Solutions

技術解決方案

Securing Channels of Communication 保密通信信道

——Virtual Private Network (VPNs) 虛擬專用網絡

- A virtual private network (VPN) allows remote users to securely access a local area network via the Internet, using a variety of VPN protocols. VPNs use both authentication and encryption to secure information from unauthorized persons (thus providing confidentiality and integrity). Authentication prevents spoofing and misrepresentation of identities. A remote user can connect to a remote private local network using a local ISP. The VPN protocols will establish the link from the client to the corporate network as if the user had dialed into the corporate network directly. The process of connecting one protocol through another (IP) is called tunneling because the VPN creates a private connection by adding an invisible wrapper around a message to hide its content. As the message travels through the Internet between the ISP and the corporate network, it is shielded from prying eyes by an encrypted wrapper.

  虛擬專用網絡允許遠程用戶使用各種VPN協議通過互聯網安全地訪問公司的局域網. VPN同時使用身份驗證和加密來保護信息不被未經授權的人獲取（提供機密性和完整性）. 身份驗證可防止電子欺騙和虛報身份. 遠程用戶可以使用本地ISP連接到遠程專用本地網絡. VPN協議將建立從客戶機到公司網絡的連接，就好像用戶已直接接入公司網絡一樣. 通過另一個協議連接一個協議的過程稱爲隧道技術，因爲VPN通過給消息添加一個不可見的包裝以隱藏其內容來創建一個私有連接. 當郵件在ISP和公司網絡之間通過互聯網發送時，它被加密的包裝程序屏蔽，防止被窺視.

2. Technology Solutions

技術解決方案

Securing Channels of Communication 保密通信信道

——Virtual Private Network (VPNs) 虛擬專用網絡

- A VPN is “virtual” in the sense that it appears to users as a dedicated secure line when, in fact, it is a temporary secure line. The primary use of VPNs is to establish secure communications between various parties, such as a business and its suppliers, or a business and its employees working remotely. A dedicated connection to a business partner can be very expensive. However, using the Internet and VPN as the connection method significantly reduces the cost of secure communications. The use of VPNs has skyrocketed as a result of the tremendous increase in the number of people working remotely.

  VPN是虛擬的，從某種意義上講，VPN在用戶看來是專用的安全綫路，而實際上却是臨時的安全綫路. VPN的主要用途是在業務合作夥伴(較大的供應商或客戶)和遠程工作的員工之間建立安全的通信. 與業務合作夥伴的專用連接可能非常昂貴. 使用互聯網和 VPN作爲連接方法將大大降低安全通信的成本. 隨著遠程辦公人數的大幅增加，VPN 的使用也急劇增加.

2. Technology Solutions

技術解決方案

Securing Channels of Communication 保密通信信道

——Wireless (Wi-Fi) Networks 無綫網絡

- Accessing the Internet via a wireless (Wi-Fi) network has its own particular security issues. Early Wi-Fi networks used a security standard called Wired Equivalent Privacy (WEP) to encrypt information. WEP was very weak and easy for hackers to crack. An alternative standard, Wi-Fi Protected Access (WPA), was developed that provided a higher standard of protection, but this, too, soon became vulnerable to intrusion. WPA2, introduced in 2004, uses the AES algorithm for encryption and CCMP, a more advanced authentication code protocol. In 2018, the Wi-Fi Alliance, the trade group that oversees the WPA protocol, announced the next generation of the protocol, WPA3, which implements a more robust key exchange protocol and a more secure way to connect IoT devices. It also features expanded encryption for public networks. However, even the updated WPA3 standard has vulnerabilities that could allow attackers to recover passwords.

  通過無綫網絡訪問互聯網有其獨特的安全問題. 早期的Wi-Fi使用一種稱爲“有綫等效保密”的安全標準來加密信息. WEP標準非常脆弱，容易被黑客破解. 已開發出的另一種標準，即 Wi-Fi保護接入，提供了更高的保護標準，但是也很快就容易受到入侵. WPA2於2004年推出，使用AES算法和CCMP（一種更高級的身份驗證代碼協議）進行加密. 2018年，負責WPA協議的貿易組織Wi-Fi聯盟宣布了下一代協議 WPA3，該協議實現了更强大的密鑰交換協議和更安全的連接物聯網設備的方式. 它還具有針對公共網絡的擴展加密功能. 即使更新的 WPA3標準仍然存在漏洞，但可能允許攻擊者恢復密鑰.

2. Technology Solutions

技術解決方案

Protecting Networks 網絡保護

Once you have protected communications as well as possible, the next set of tools to consider are those that can protect your networks as well as the servers and clients on those networks.

保護好通信通道，下一步就是考慮如何保護網絡，包括服務器網絡和客戶機網絡 .

- Firewall 防火墙
  - Hardware or software that uses security policy to filter packets
    指出於安全考慮過濾通信數據包的軟件或硬件
- Proxy servers (proxies) 代理服務器
  - Software servers that handle all communications from or sent to the Internet
    對來自於互聯網或發送到互聯網上的通信信息進行處理的軟件服務器
- Intrusion detection systems 入侵檢測系統
  - IDS examines network traffic, watching to see if it matches certain patterns or preconfigured rules indicative of an attack
    IDS 檢查網絡流量，查看它是否與意味著攻擊的某種模式或預配置規則匹配
- Intrusion prevention systems 入侵防禦系統
  - IPS has all the functionality of an IDS, with the additional ability to take steps to prevent and block suspicious activities
    IPS 具有 IDS 的所有功能，以及具有采取措施防禦和阻止可疑活動的能力

2. Technology Solutions

技術解決方案

Protecting Networks 網絡保護

——Firewalls 防火墙

- A firewall refers to either hardware or software that filters communication packets and prevents some packets from entering or exiting the network based on a security policy.
  防火墙是指基於安全策略過濾通信數據包，阻止某些數據包進入網絡的軟件和硬件.
- The firewall controls traffic to and from servers and clients, forbidding communications from untrustworthy sources and allowing communications from trusted sources to proceed. Every message that is to be sent or received from the network is processed by the firewall, which determines whether the message meets security guidelines established by the business. If it does, it is permitted to be distributed, and if it doesn't, the message is blocked. Firewalls can filter traffic based on packet attributes such as source IP address, destination port or IP address, type of service (such as WWW or HTTP), the domain name of the source, and many other attributes.
  防火墙控制出入服務器和客戶機的流量，阻止不受信任的通信，只允許受信任的通信通過. 防火墙需要處理從網絡發送或接收的每條消息，確定該消息是否符合企業制定的安全準則. 如果符合，則允許傳輸；如果不符合，則阻止傳輸. 防火墙可以根據數據包屬性（例如源IP地址、目標端口或IP地址、服務類型（例如WWW或 HTTP）、源域名以及其他維度）過濾通信流量.

2. Technology Solutions

技術解決方案

Protecting Networks 網絡保護

——Firewalls 防火墙

- Most hardware firewalls that protect local area networks connected to the Internet have default settings that require little if any administrator intervention and employ simple but effective rules that deny incoming packets from a connection that does not originate from an internal request— the firewall allows connections only from servers that you requested service from.

  大多數能保護局域網絡的硬件防火墙都具有默認設置，這些默認設置幾乎不需要管理員干預，就能簡單、有效地阻止內部請求之外的數據包傳入，只允許請求的服務器發送的數據包傳入.

- A common default setting on hardware firewalls (DSL and cable modem routers) simply ignores efforts to communicate with TCP port 445, the most commonly attacked port. The increasing use of firewalls by home and business Internet users has greatly reduced the effectiveness of attacks and forced hackers to focus more on e-mail attachments to distribute worms and viruses.

  常見的硬件防火墙（數字用戶綫路和電纜調制解調器）默認設置忽略了與TCP端口 445(最常受到攻擊的端口)之間的通信. 家庭和公司網絡中越來越多地使用防火墙，大大降低了攻擊的有效性，並迫使黑客將更多的精力放在電子郵件附件上，通過附件傳播蠕蟲和病毒.

2. Technology Solutions

技術解決方案

Protecting Networks 網絡保護

——Firewalls 防火墻

- There are two major methods that firewalls use to validate traffic: packet filters and application gateways.
  防火墻對通信的檢查主要有兩種方式：包過濾和應用網關.
  - Packet filters examine data packets to determine whether they are destined for a prohibited port or originate from a prohibited IP address (as specified by the security administrator). The filter specifically looks at the source and destination information, as well as the port and packet type, when determining whether the information may be transmitted. One downside of the packet filtering method is that it is susceptible to spoofing because authentication is not one of its roles.
    包過濾方式通過對數據包的檢查來判斷它們是否要發送到禁止的目的端口或來自禁止的IP地址（由安全管理者規定）. 過濾器在判斷某信息是否應該傳輸時，尤其注意的是信息源和目標地址，以及端口和數據包的類型. 包過濾方式的一個缺陷是它容易產生電子欺騙，因爲它不對真實性進行驗證.

2. Technology Solutions

技術解決方案

Protecting Networks 網絡保護

——Firewalls 防火墻

- There are two major methods that firewalls use to validate traffic: packet filters and application gateways.
  防火墻對通信的檢查主要有兩種方式：包過濾和應用網關.
  - Application gateways are a type of firewall that filters communications based on the application being requested rather than the source or destination of the message. Such firewalls also process requests at the application level, which is farther away from the client computer than where packet filters process requests. By providing a central filtering point, application gateways provide greater security than packet filters but can compromise system performance.
    應用網關是一種防火墻，它根據請求的應用程序（而不是信息源或目標地址）過濾通信. 這類防火墻需要處理應用層的請求，因此，相比於包過濾方式，應用網關距離客戶計算機更遠. 通過提供一個中央過濾點，應用網關可以提供比包過濾更好的安全性，但可能損害系統性能.

2. Technology Solutions

技術解決方案

Protecting Networks 網絡保護

——Firewalls 防火墻

- Next-generation firewalls use an application-centric approach to firewall control. They are able to identify applications regardless of the port, protocol, or security evasion tools used; identify users regardless of device or IP address; decrypt outbound TLS traffic; and protect in real time against threats embedded in applications.

  下一代防火墻使用以應用程序爲中心的方法進行防火墻控制. 它們能够識別應用程序. 無論所使用的端口、協議或安全規避工具是什麽，它們都能够識別應用程序. 無論設備或IP地址是什麽，都能識別用戶，解密出站SSL，並實時保護用戶免受嵌入應用程序的威脅.

2. Technology Solutions

技術解決方案

Protecting Networks 網絡保護

——Proxy Servers 代理服務器

- Proxy servers (proxies) are software servers (often a dedicated computer) that handle all communications originating from or being sent to the Internet by local clients, acting as a bodyguard for the organization. Proxies act primarily to limit access of internal clients to external Internet servers, although some proxy servers act as firewalls as well. Proxy servers are sometimes called dual-home systems because they have two network interfaces. To internal computers, a proxy server is known as the gateway, while to external computers it is known as a mail server or numeric address.

  代理服务器是一種對來自互聯網或發送到互聯網上的通信信息進行處理的軟件服務器（通常位於某台專用的計算機上），在企業中扮演了發言人或者衛兵的角色．代理服務器主要用於限制內部客戶機對外部互聯網服務器的訪問，儘管某些代理服務器也充當防火墻．代理服務器有時被稱爲雙宿主系統，因爲它有兩個網絡接口．對於內部計算機來說，代理服務器被稱爲網關;而對於外部計算機來說，代理服務器則被稱爲郵件服務器或數字地址.

2. Technology Solutions

技術解決方案

Protecting Networks 網絡保護

——Proxy Servers 代理服務器

- When a user requests a web page on an internal network, the request is routed first to the proxy server. The proxy server validates the user and the nature of the request and then sends the request onto the Internet. A web page sent by an external Internet server first passes to the proxy server. If acceptable, the web page passes onto the internal network web server and then to the client desktop. By prohibiting users from communicating directly with the Internet, companies can restrict access to certain types of sites, such as pornographic, auction, or stock-trading sites. Proxy servers also improve web performance by storing frequently requested web pages locally, thus reducing upload times, and hiding the internal network's address, making it more difficult for hackers to monitor.

  當內部網絡上的用戶請求網頁時，該請求首先被發送到代理服務器．代理服務器驗證用戶和請求的性質，然後將請求發送到互聯網上．外部互聯網服務器發送的網頁首先傳輸到代理服務器．如果可以接收，網頁將被傳輸到內部網絡的網絡服務器，然後傳輸到客戶機桌面．通過禁止用戶直接與互聯網通信，公司可以限制對某些類型網站的訪問，例如拍賣或股票交易網站．代理服務器還通過在本地存儲經常請求的網頁減少上傳時間，並通過隱藏內部網絡的地址來提高網絡性能，從而使黑客更難以監視網絡．

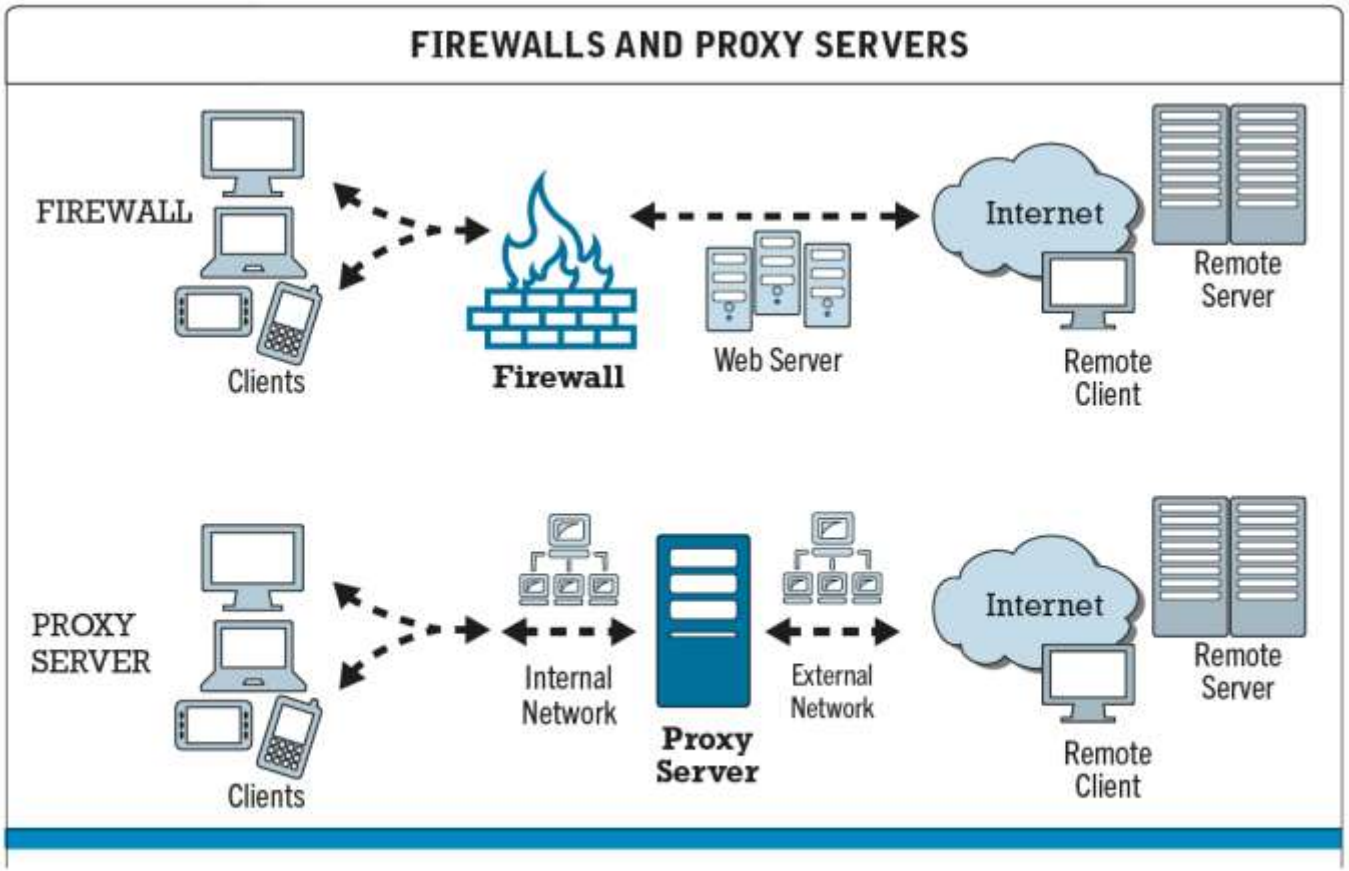
2. Technology Solutions

技術解決方案

The figure illustrates how firewalls and proxy servers protect a local area network from Internet intruders and prevent internal clients from reaching prohibited web servers.

Protecting Networks 網絡保護

——Proxy Servers 代理服務器



The primary function of a firewall is to deny access to local computers by remote client computers. The primary purpose of a proxy server is to provide controlled access from local computers to remote computers.

2. Technology Solutions

技術解決方案

Protecting Networks 網絡保護

——Intrusion Detection and Prevention Systems 入侵檢測和防禦系統

- An intrusion detection system (IDS) examines network traffic, watching to see if it matches certain patterns or preconfigured rules indicative of an attack. If it detects suspicious activity, the IDS will set off an alarm, alerting administrators, and log the event in a database. An IDS is useful for detecting malicious activity that a firewall might miss.

  入侵檢測系統檢查網絡流量，觀察其是否與某些表示攻擊的模式或預先設定的規則相匹配. 如果檢測到可疑活動，IDS會發出警報，警告管理員，並將事件記錄在數據庫中. IDS對於檢測防火墻可能會遺漏的惡意活動很有用.

- An intrusion prevention system (IPS) has all the functionality of an IDS, with the additional ability to take steps to prevent and block suspicious activities. For instance, an IPS can terminate a session and reset a connection, block traffic from a suspicious IP address, or reconfigure firewall or router security controls.

  入侵防禦系統具有IDS的所有功能，並具有采取措施預防和阻止可疑活動的附加功能. 例如，IPS可以終止會話並重置連接，阻止來自可疑IP地址的流量，或者重新設定防火墻或配置路由器安全控件.

2. Technology Solutions

技術解決方案

Protecting Servers and Clients 網絡服务器和客户机

Operating system features and anti-virus software can help further protect servers and clients from certain types of attacks.

操作系統和殺毒軟件可以幫助進一步保護服務器和客戶機免受某些類型的攻擊.

- **Operating System and Application Software Security Enhancements**
  提高操作系統和應用程序軟件安全
  - The most obvious way to protect servers and clients is to take advantage of automatic computer security upgrades. The Microsoft, Apple, and Linux/Unix operating systems are continuously updated to patch vulnerabilities discovered by hackers. The most common forms of malware can be prevented by simply keeping your server and client operating systems and applications up to date. Application vulnerabilities are fixed in the same manner.

    保護服務器和客戶機的最合理的方法是利用計算機安全系統的自動升級功能. 微軟、蘋果和Linux/Unix操作系統會不斷更新，以修補黑客發現的漏洞. 只需使服務器和客戶機操作系統以及應用程序保持最新版本，就可以預防最常見的惡意軟件. 應用程序漏洞以相同的方式修復.

2. Technology Solutions

技術解決方案

Protecting Servers and Clients 網絡服务器和客户机

Operating system features and anti-virus software can help further protect servers and clients from certain types of attacks.

操作系統和殺毒軟件可以幫助進一步保護服務器和客戶機免受某些類型的攻擊.

- **Anti-Virus Software**

  殺毒軟件

  - The easiest and least expensive way to prevent threats to system integrity is to install anti-virus software. Anti-virus suite packages and stand-alone programs are available to eliminate intruders such as bot programs, adware, and other security risks.

    最簡單、最便宜的防止病毒對系統完整性造成威脅的方法是安裝殺毒軟件. 可以使用殺毒套件包和獨立程序來清除入侵程序，例如僵尸程序、廣告軟件和其他安全風險.

3. Policies and Laws

政策和法律

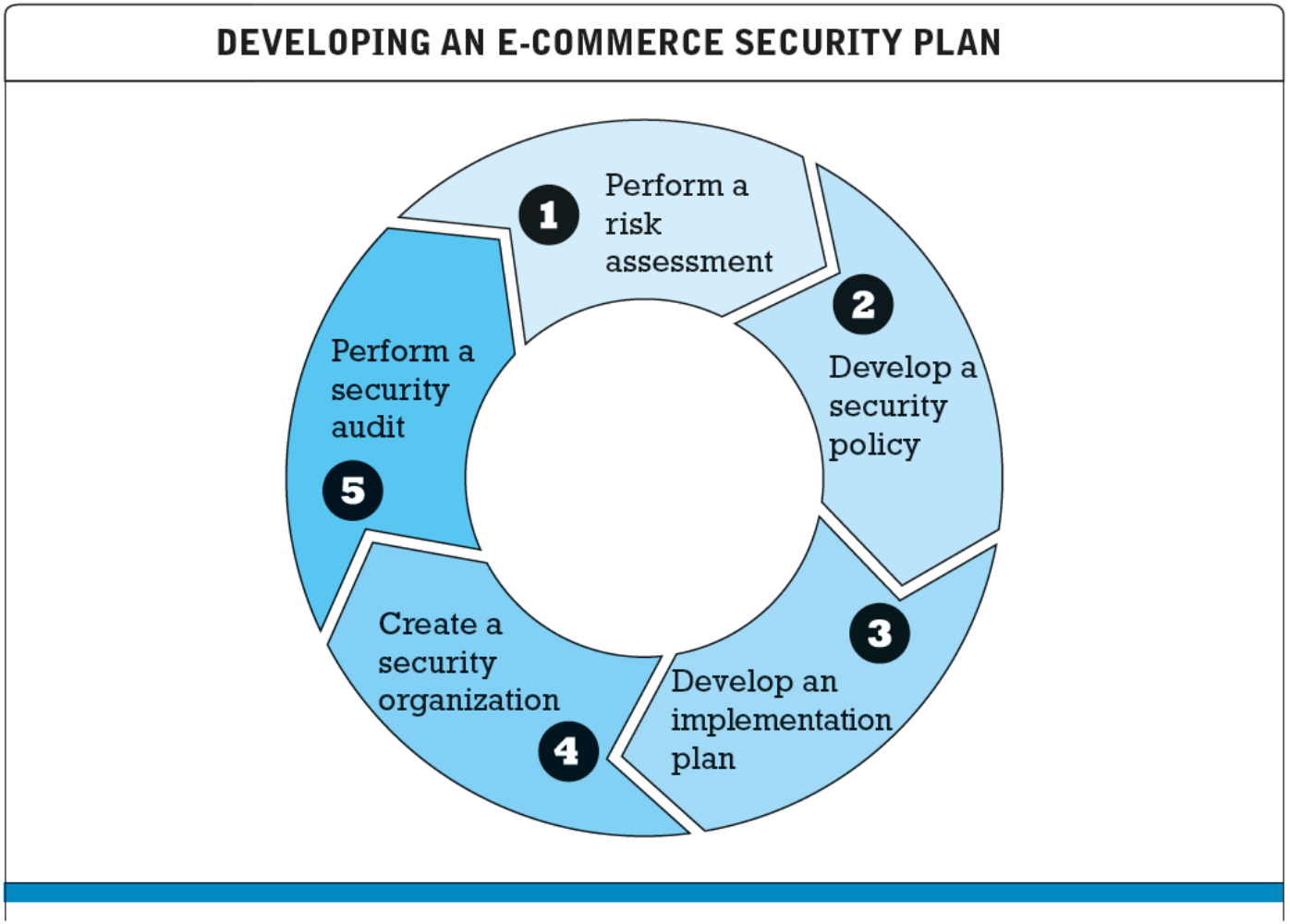
Security Plan: Management Policies 安全計劃：管理政策

- Risk assessment
- Security policy
- Implementation plan
- Security organization
  - Access controls
  - Authentication procedures, including biometrics
  - Authorization policies, authorization management systems
- Security audit

- 風險評估
- 安全策略
- 實施計劃
- 安全組織
  - 訪問控制
  - 身份驗證程序，包括生物測定學
  - 授權策略，授權管理系統
- 安全審計

3. Policies and Laws

政策和法律



There are five steps involved in developing an e-commerce security plan.

3. Policies and Laws

政策和法律

Security Plan: Management Policies 安全計劃：管理政策

——Risk Assessment 風險評估

- A security plan begins with **risk assessment**—an assessment of the risks and points of vulnerability. The first step is to inventory the information and knowledge assets of the e-commerce site and company. What information is at risk? Is it customer information, proprietary designs, business activities, secret processes, or other internal information such as price schedules, executive compensation, or payroll? For each type of information asset, try to estimate the dollar value to the firm if this information were compromised, and then multiply that amount by the probability of the loss occurring. Once you have done so, rank-order the results. You now have a list of information assets prioritized by their value to the firm.

安全計劃的制訂始於**風險評估**，即對風險和薄弱環節的評估. 首先是盤點電子商務站點和公司的信息與知識資產. 哪些信息有風險?是客戶信息專有設計、業務活動、秘密流程，還是其他內部信息如價格表、高管薪酬或工資單？對於每種類型的信息資產，試著估計這些信息如被泄露對公司造成的損失，然後將該金額乘以發生損失的可能性. 完成後，對結果進行排名. 這樣你就有了一個根據對企業的價值進行排序的信息資產列表.

3. Policies and Laws

政策和法律

Security Plan: Management Policies 安全計劃：管理政策

——Security Policy 安全策略

- Based on your quantified list of risks, you can start to develop a **security policy**—a set of statements prioritizing the information risks, identifying acceptable risk targets, and identifying the mechanisms for achieving these targets. You will obviously want to start with the information assets that you determined to be the highest priority in your risk assessment.

  根據你量化的風險列表，你可以制定**安全策略**，即一系列聲明這些聲明對信息風險進行排序，確定可接受的風險目標，並確定實現這些目標的機制. 顯然，你要從風險評估中最高優先級的信息資產入手. .

3. Policies and Laws

政策和法律

Security Plan: Management Policies 安全計劃：管理政策

——Implementation Plan 實施計劃

- Next, consider an **implementation plan**—the steps you will take to achieve the security plan goals. Specifically, you must determine how you will translate the levels of acceptable risk into a set of tools, technologies, policies, and procedures. What new technologies will you deploy to achieve the goals, and what new employee procedures will be needed?

  接下來，考慮制訂**實施計劃**，即爲實現安全策略所采取的行動步驟. 具體來說，你必須確定如何將可接受的風險級別轉換爲一組工具、技術、策略和過程. 你將部署哪些新技術來實現目標，以及將需要哪些新的員工雇傭計劃?

3. Policies and Laws

政策和法律

Security Plan: Management Policies 安全計劃：管理政策

——Security Organization 安全組織

- To implement your plan, you will need an organizational unit in charge of security and a security officer—someone who is in charge of security on a daily basis. For a small e-commerce site, the security officer will likely be the person in charge of Internet services or the site manager, whereas for larger firms, there typically is a dedicated team with a supporting budget. The **security organization** educates and trains users, keeps management aware of security threats and breakdowns, and maintains the tools chosen to implement security.

  要實施你的計劃，你將需要一個負責安全性的組織和一名安全管理員．對於小型電子商務網站，安全管理員可能是負責互聯網服務的人或網站管理者，對於大型公司，通常會有一個專門的團隊，需要有預算支持．**安全組織**對用戶進行教育和培訓，使管理層瞭解安全威脅和故障，並對保障安全的工具進行維護.

3. Policies and Laws

政策和法律

Security Plan: Management Policies 安全計劃：管理政策

——Security Organization 安全組織

- The security organization typically administers access controls, authentication procedures, and authorization policies. Access controls determine which outsiders and insiders can gain legitimate access to your networks. Outsider access controls include firewalls and proxy servers, while insider access controls typically consist of login procedures (usernames, passwords, and access codes).

  安全組織通常對訪問控制、身份驗證程序和授權策略進行管理. 訪問控制確定哪些外部人員和內部人員可以合法訪問你的網絡. 外部人員訪問控制工具包括防火墻等，而內部人員訪問控制通常包括登錄流程控制（用戶名、密碼和訪問代碼）.

3. Policies and Laws

政策和法律

Security Plan: Management Policies 安全計劃：管理政策

——Security Organization 安全組織

- Authentication procedures include the use of digital signatures, certificates of authority, PKI, and multi-factor authentication (MFA) tools that require users to have multiple credentials to verify their identify. Authentication credentials might include something the user knows, such as a password; something the user possesses, such as a smartphone or YUBIkey USB device; and something that the user "is", such as a physical characteristic.
- 身份驗證程序包括使用數字簽名、授權證書、PKI和多因素身份驗證工具，這些工具要求用戶具有多個憑據來驗證其身份. 身份驗證憑據可能包含用戶已知內容如密碼，用戶私人物品如智能手機或YUBIkey USB設備，以及用戶自身特徵如身體特徵.

3. Policies and Laws

政策和法律

Security Plan: Management Policies 安全計劃：管理政策

——Security Organization 安全組織

- Biometric devices can also be used to verify physical attributes associated with an individual, such as a facial, fingerprint, or retina (eye) scan or speech recognition system, and are often part of a multi-factor authentication system. (Biometrics is the study of measurable biological, or physical, characteristics.)
  生物識別設備，如面部、指紋、視網膜(眼睛)掃描設備，以及語音識別系統還可用於驗證與個人相關聯的生理特徵，並且通常是多因素身份驗證系統的一部分. (生物測定學(biometrics)對可測量的生物學或生理特徵進行研究.)
- Security tokens are physical devices or software that generate an identifier that can be used in addition to or in place of a password. Security tokens are used by millions of corporation and government workers to log on to corporate clients and servers. One example is RSA's SecurID token, which continuously generates six-digit passwords.
  安全令牌是生成標識符的物理設備或軟件，這些標識符可在密碼之外或代替密碼使用. 數百萬企業和政府工作人員使用安全令牌登錄企業客戶機和服務器. RSA的SecurID令牌就是安全令牌的一種，它不斷地生成6位密碼.

3. Policies and Laws

政策和法律

Security Plan: Management Policies 安全計劃：管理政策

——Security Organization 安全組織

- **Authorization policies** determine differing levels of access to information assets for differing levels of users. **Authorization management systems** establish where and when a user is permitted to access certain parts of a website. Their primary function is to restrict access to private information within a company's Internet infrastructure. The system encrypts a user session to function like a passkey that follows the user from page to page, allowing access only to those areas that the user is permitted to enter, based on information set at the system database. By establishing entry rules up front for each user, the authorization management system knows who is permitted to go where at all times.

  授權策略爲不同級別的用戶匹配對信息資產的不同訪問級別. **授權管理系統**確定允許用戶在何時何地訪問網站的某些部分. 它的主要功能是限制對公司內網中私人信息的訪問. 系統把一個用戶的會話加密成像跟踪用戶進入一個又一個網頁的通行密碼一樣的函數，根據系統數據庫中的設置信息，只允許用戶訪問那些可以進入的區域. 通過給每個用戶建立進入規則，授權管理系統可以隨時知道誰能訪問什麼地方.

3. Policies and Laws

政策和法律

Laws 法律

- Today, the Internet is no longer an ungoverned, unsupervised, self-controlled technology juggernaut. There is a growing awareness that e-commerce markets work only when a powerful institutional set of laws and enforcement mechanisms are in place. These laws help ensure orderly, rational, and fair markets. Since 1995, as e-commerce has grown in significance, national and local law enforcement activities have expanded greatly. These laws have been passed that grant national, state, and local governments new tools and mechanisms for identifying, tracing, and prosecuting cybercriminals.

  今天，互聯網不再是不受監管、不受監督、自我控制的技術主宰．人們越來越多地認識到只有制定一系列有效的法律制度和强制措施，電子商務市場才能運轉．這些法律有助於確保形成一個有序、合理和公平的市場．自1995年以來，隨著電子商務的迅猛發展，國家和地方執法活動也得到極大發展．新的法律爲國家和地方權力機構識別、跟踪並起訴網絡犯罪分子提供了新的工具和機制．

3. Policies and Laws

政策和法律

Laws 法律

- 《中华人民共和国电子商务法》
- 《中华人民共和国网络安全法》
- 《中华人民共和国反电信网络诈骗法》
- 《中华人民共和国电子签名法》
- 《中华人民共和国数据安全法》
- 《中华人民共和国个人信息保护法》

Part IV:

E-Commerce Payment Systems

E-Commerce Payment Systems

電子商務支付系統

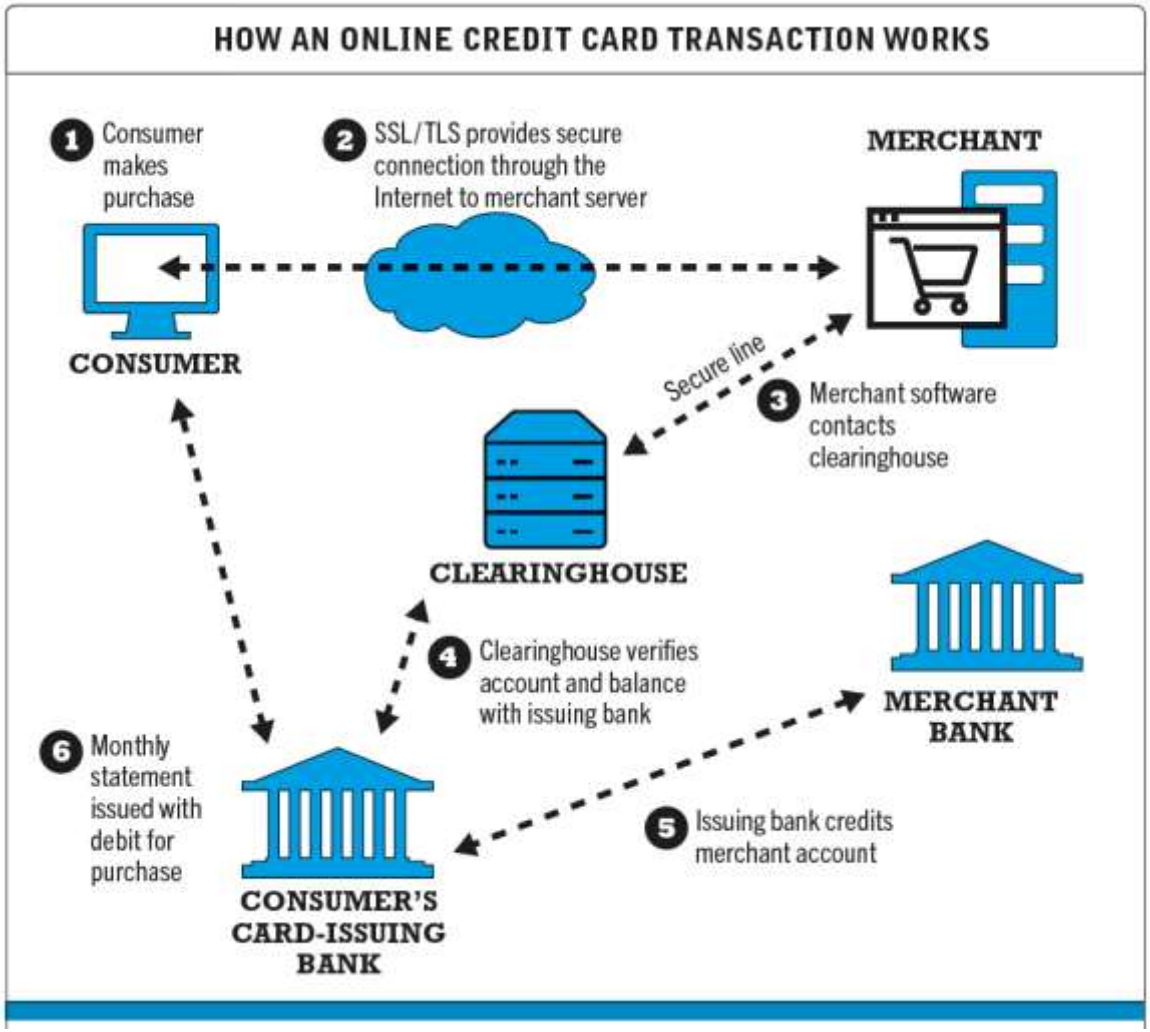
- Online Credit and Debit Card Transactions 在信用卡和借記卡交易
  - Credit and debit card payment processing is a multi-step process involving several intermediaries. Making a card purchase online results in electronic communication between the customer's card issuer and bank, with the merchant's payment processor and merchant account.

    信用卡和借記卡付款處理是一個多步驟過程，涉及多個中介機構. 在綫刷卡購買會導致客戶的發卡機構和銀行與商家的付款處理機構和商家賬戶之間進行電子通信.

E-Commerce Payment Systems

電子商務支付系統

- Online Credit and Debit Card Transactions 在信用卡和借記卡交易



E-Commerce Payment Systems

電子商務支付系統

- Online Stored Value Systems 在綫儲值支付系統
  - Online stored value payment system permits consumers to make instant online payments to merchants and other individuals based on value stored in an online account.

    在綫儲值支付系統允許消費者根據在綫賬戶中存值向商家和其他個人進行即時在綫支付.
  - Example: Alipay, PayPal

E-Commerce Payment Systems

電子商務支付系統

- Mobile Payment Systems 移動支付系統
  - Mobile payments involve any type of payment using a mobile device, including bill pay, online purchases, in-store purchases, and P2P payments. Mobile wallets (sometimes also referred to as digital wallets) are smartphone apps that store debit cards, reward coupons, invoices, vouchers, and other means of payment that might be found in a traditional wallet.

    移動支付包括使用移動設備的所有類型的支付，包括賬單支付、在綫購買、店內購買和P2P付款. 移動錢包（有時也稱爲數字錢包）是智能手機應用程序，用於存儲借記卡、優惠券、發票和傳統錢包中可能存在的代金券.

E-Commerce Payment Systems

電子商務支付系統

- Mobile Payment Systems 移動支付系統
  - **Near field communication (NFC)** technology is the primary enabling technology for universal proximity mobile wallets, while QR code technology is typically used for branded store proximity mobile wallets. Near field communication (NFC) is a set of short-range wireless technologies used to share information among devices within about two inches (50 mm) of each other. NFC devices are either powered or passive. A connection requires one powered device (the initiator, such as a smartphone) and one target device, such as a merchant NFC reader, that can respond to requests from the initiator. NFC targets can be very simple forms such as tags, stickers, key fobs, or readers. NFC peer-to-peer communication is possible when both devices are powered. Consumers can swipe their NFC-equipped phone near a merchant's reader to pay for purchases.

近距離無綫通信技術是通用近場移動錢包應用程序的主要支持技術，而快速響應碼技術通常是品牌商店近場移動錢包應用程序的主要支持技術. NFC是一組短距離無綫技術，用於在約2英寸範圍內的設備之間共享信息. NFC設備要麽是主動啓用，要麽是被動啓用. 連接時需要一個電源設備（啓動器，如智能手機）和一個可以響應發起方的請求的目標設備（如商家NFC讀取器）. NFC目標設備可以是非常簡單的形式，如標簽、貼紙、電子鑰匙鏈或讀取器. 在兩個設備都通電的情況下，NFC對等通信就可以實現. 消費者可以在商家的讀取器附近刷卡，以支付所購商品的費用.

E-Commerce Payment Systems

電子商務支付系統

- Mobile Payment Systems 移動支付系統
  - **Near field communication (NFC)** technology is the primary enabling technology for universal proximity mobile wallets. Near field communication (NFC) is a set of short-range wireless technologies used to share information among devices within about two inches (50 mm) of each other. NFC devices are either powered or passive. A connection requires one powered device (the initiator, such as a smartphone) and one target device, such as a merchant NFC reader, that can respond to requests from the initiator. NFC targets can be very simple forms such as tags, stickers, key fobs, or readers. NFC peer-to-peer communication is possible when both devices are powered. Consumers can swipe their NFC-equipped phone near a merchant's reader to pay for purchases.

    近距離無綫通信技術是通用近場移動錢包應用程序的主要支持技術. NFC是一組短距離無綫技術，用於在約2英寸範圍內的設備之間共享信息. NFC設備要麽是主動啓用，要麽是被動啓用. 連接時需要一個電源設備（啓動器，如智能手機）和一個可以響應發起方的請求的目標設備（如商家NFC讀取器）. NFC目標設備可以是非常簡單的形式，如標簽、貼紙、電子鑰匙鏈或讀取器. 在兩個設備都通電的情況下，NFC對等通信就可以實現. 消費者可以在商家的讀取器附近刷卡，以支付所購商品的費用.

E-Commerce Payment Systems

電子商務支付系統

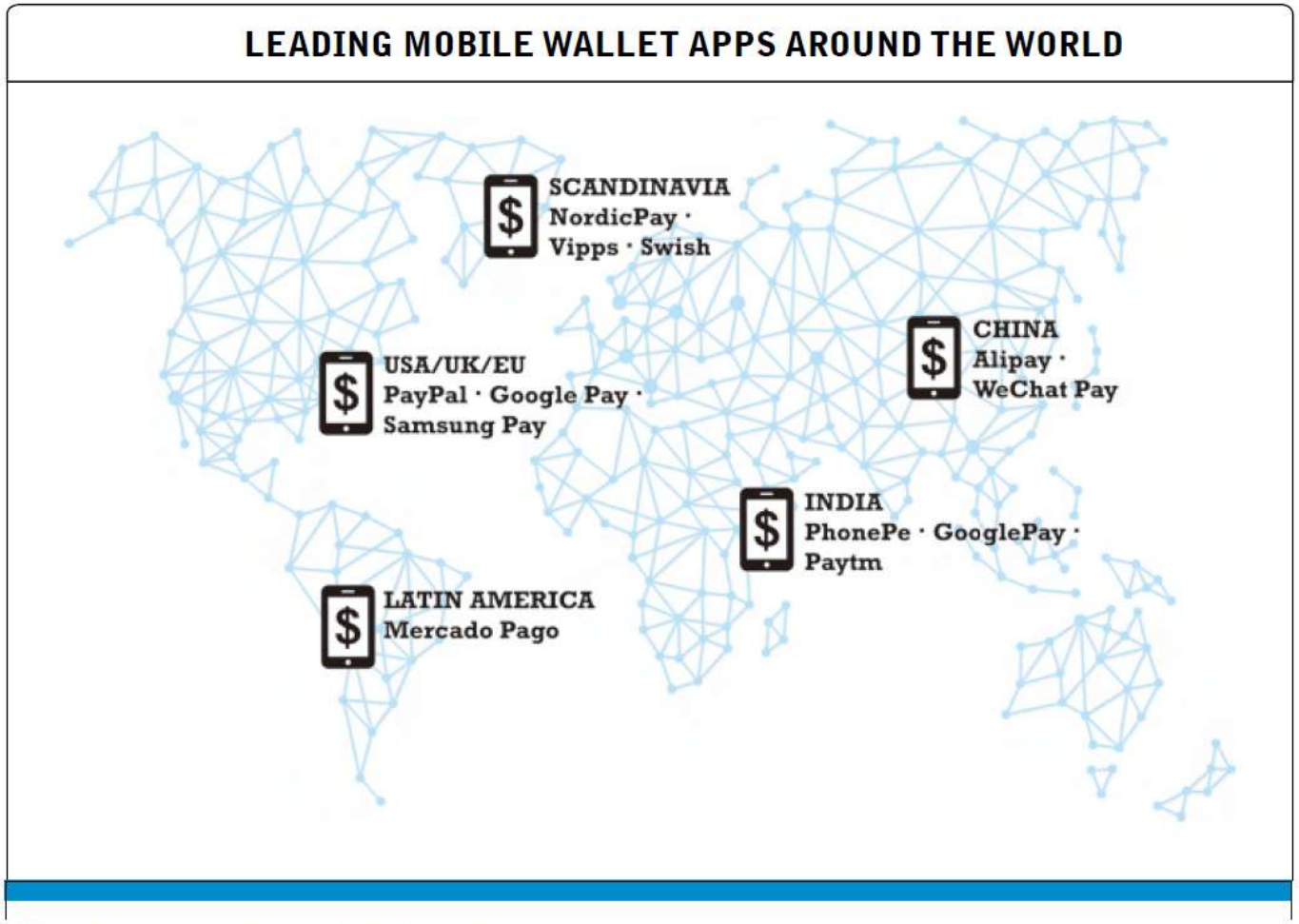
- Mobile Payment Systems 移動支付系統
  - There are three primary types of mobile wallet apps: universal proximity wallets, branded store proximity wallets, and P2P apps. Universal proximity mobile wallets, such as Apple Pay, Google Pay, and Samsung Pay, which can be used at a variety of merchants for point-of-sale transactions if the merchant supports that service (e.g., has an Apple merchant app and can accept such payments), are the most-well-known and common type. Branded store proximity mobile wallets are mobile apps that can be used only at a single merchant. P2P mobile payment apps, such as Venmo, Zelle, and Square Cash, are used for payments among individuals who have the same app.

    移動錢包應用程序主要有三種類型:通用近場移動錢包應用程序、品牌商店近場移動錢包應用程序和P2P移動支付應用程序. 如果商戶支持該服務如（有蘋果商戶應用程序且可以接受這種支付），則可以在各種商戶處使用通用近場移動錢包（如Apple Pay、Google Pay和Samsung Pay）來完成交易. 這種付款方式是最廣爲人知且最常見的移動支付類型. 品牌商店近場移動錢包是只能在特定商家處使用的移動應用程序. P2P移動支付應用程序如Venmo、Zelle和Square Cash，用於在擁有相同應用程序的個人之間進行支付.

E-Commerce Payment Systems

電子商務支付系統

- Mobile Payment Systems 移動支付系統



SOURCES: Based on data from eMarketer, Inc., 2020a.

E-Commerce Payment Systems

電子商務支付系統

- Blockchain and Cryptocurrencies 區塊鏈和加密貨幣
  - **Blockchain** is a technology that enables organizations to create and verify transactions on a network nearly instantaneously without a central authority. Traditionally, organizations maintained their own transaction processing systems on their own databases and used this record of transactions to keep track of orders, payments, production schedules, and shipping. For instance, when you place an order online, it is entered into a transaction database as an order record. As the order works its way through the firm's factories, warehouses, shipping, and payments processes, the initial record expands to record all this information about this specific order. You can think of this as a block of information that's created for every order and that grows over time as the firm processes the order. When the process is completed and the order is fulfilled and paid for, the result is a connected chain of blocks (or linked records) associated with that initial order.

區塊鏈是一項使機構可以在沒有中央授權的情況下幾乎立即在網絡上創建和驗證交易的技術. 從傳統上講，機構自己維護自身的數據庫和交易處理系統，使用交易記錄來進行訂單跟踪、付款，安排生產進度和運輸. 例如，當你在網上下單時，該訂單將作爲訂單記錄輸入交易數據庫中. 當訂單在公司的工廠、倉庫、運輸和付款過程中進行處理時，初始記錄會擴展爲有關此訂單的所有信息的記錄. 你可以將其視爲爲每個訂單創建的信息塊，並且隨著公司不斷地處理訂單而持續發展. 當訂單完成並已付款時，就會產生與該初始訂單相關聯的鏈塊（或鏈接記錄）.

E-Commerce Payment Systems

電子商務支付系統

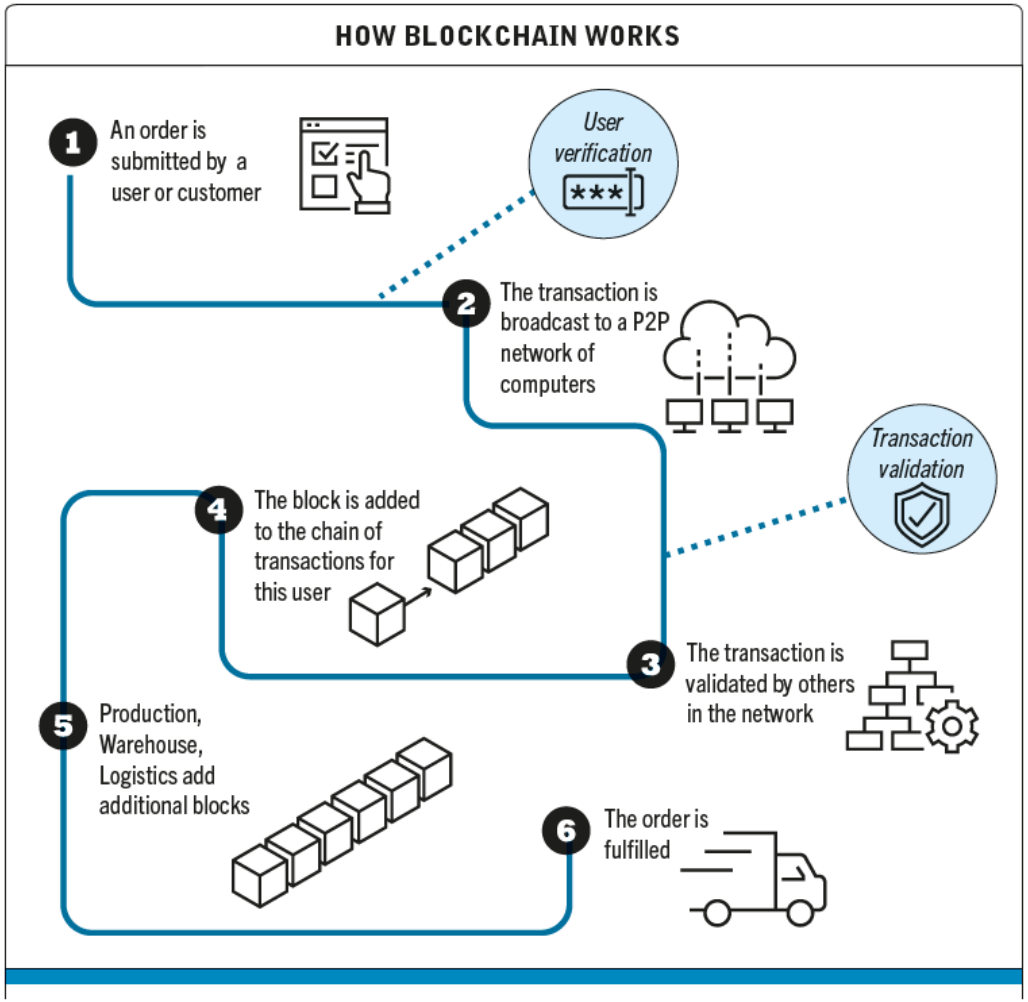
- Blockchain and Cryptocurrencies 區塊鏈和加密貨幣
  - A **blockchain system** is a transaction processing system that operates on a distributed and shared database rather than a single organization's database. The system is composed of a distributed network of computers (called a peer-to-peer [P2P] computer network). Unlike traditional databases, distributed ledgers are managed through a P2P architecture and do not have a centralized database. It is inherently decentralized and is often called a distributed ledger. The blockchain maintains a continuously growing list of records called blocks. Each block contains a timestamp and a link to a previous block. Once a block of data is recorded on the blockchain ledger, it cannot be altered retroactively. When someone wants to add a transaction, participants in the network (all of whom have copies of the existing blockchain) run algorithms to evaluate and verify the proposed transaction. Legitimate changes to the ledger are recorded across the blockchain in a matter of seconds or minutes, and records are protected through cryptography.

    區塊鏈系統是一個在分布式和共享數據庫（稱爲對等或P2P計算機網絡）而不是單個組織的數據庫上運行的交易處理系統. 該系統由計算機的分布式網絡組成. 與傳統數據庫不同，分布式分類帳通過P2P體系進行管理，並且沒有集中式數據庫. 它本質上是分散的. 區塊鏈維護著不斷增長的記錄列表，稱爲記錄塊. 每個塊都包含一個時間戳，並鏈接到前一個塊. 一旦數據塊被記錄在區塊鏈分類帳上，就無法追溯更改. 當某人想要添加交易時，網絡中的參與者(所有參與者都有現有區塊鏈的副本)運行算法來評估和驗證提議的交易. 對分類帳的合法更改將在幾秒鐘或幾分鐘內記錄在整個區塊鏈中，並通過加密對記錄進行保護. .

E-Commerce Payment Systems

電子商務支付系統

- Blockchain and Cryptocurrencies 區塊鏈和加密貨幣



A blockchain system is a distributed database that records transactions in a P2P network of computers.

E-Commerce Payment Systems

電子商務支付系統

- Blockchain and Cryptocurrencies 區塊鏈和加密貨幣
  - Cryptocurrencies are digital tokens. They are a type of digital currency that allows people to make payments directly to each other through an online system. Cryptocurrencies have no legislated or intrinsic value; they are simply worth what people are willing to pay for them in the market. This is in contrast to national currencies, which get part of their value from being legislated as legal tender. There are a number of cryptocurrencies – the most well-known of these are Bitcoin and Ether.

    加密貨幣是數字代幣. 它們是一種數字貨幣, 允許人們通過在綫系統直接相互付款. 加密貨幣沒有法定價值或內在價值; 它們的價值只是人們願意在市場上爲它們支付的價格. 這與國家貨幣形成對比, 國家貨幣的部分價值來自被立法爲法定貨幣. 加密貨幣有很多種——其中最著名的是Bitcoin和Ether.
  - A Central Bank Digital Currency (CBDC) can most easily be understood as a digital form of cash. It can be issued by the central bank, accessible to the general public, and used to settle transactions between firms and households. The unit of account would be the national currency, and it could be exchanged at parity (i.e. one for one) with other forms of money, such as physical currency or electronic deposits with well-regulated financial institutions..

    中央銀行數字是最容易理解爲一種數字形式的現金. 它可以由中央銀行發行, 可供公衆使用, 可用於企業和家庭之間的交易結算. 記帳單位將是國家貨幣, 它可以按平價（即一比一）與其他形式的貨幣（例如實物貨幣或受監管的金融機構的電子存款）進行兌換.

Exercise (Part II)

1) Symmetric key cryptography is also known as _____ cryptography.

2) All the following statements about symmetric key cryptography are true *except*:
A) in symmetric key cryptography, both the sender and the receiver use the same key to encrypt and decrypt a message
B) the Data Encryption Standard is a symmetric key encryption system
C) symmetric key cryptography is computationally slower
D) symmetric key cryptography is a key element in digital envelopes

3) All of the following statements about public key cryptography are true *except*:
A) public key cryptography uses two mathematically related digital keys
B) public key cryptography ensures authentication of the sender
C) public key cryptography does not ensure message integrity
D) public key cryptography is based on the idea of irreversible mathematical functions

Exercise (Part II)

4) A digital certificate contains all of the following *except* the:
A) subject's private key
B) subject's public key
C) digital signature of the certification authority
D) digital certificate serial number

5) Which of the following dimensions of e-commerce security does *not* involve encryption?
A) confidentiality
B) availability.

C) message integrity
D) nonrepudiation.

6) A _____ is a hardware or software component that acts as a filter to prevent unwanted packets from entering a network.

Exercise (Part II)

7) Proxy servers are also known as:
A) firewalls
B) application gateways
C) dual home systems
D) packet filters

8) All of the following are used for authentication *except*:
A) digital signatures
B) certificates of authority
C) biometric devices
D) packet filters

9) An intrusion detection system can perform all of the following functions *except*:
A) examining network traffic
B) setting off an alarm when suspicious activity is detected
C) checking network traffic to see if it matches certain patterns or preconfigured rules
D) blocking suspicious activity

Exercise (Part II)

10) A fingerprint scan is an example of which of the following?
A) biometrics
B) encryption
C) IDS
D) firewall

11) Which of the following is the most common protocol for securing a digital channel of communication?
A) DES
B) SSL/TLS
C) VPN
D) HTTP

12) What is the first step in developing an e-commerce security plan?
A) Create a security organization
B) Develop a security policy
C) Perform a risk assessment
D) Perform a security audit

Exercise (Part II)

13) PayPal is an example of a(n):
A) online stored value payment system
B) digital checking system
C) accumulating balance system
D) digital credit card system

14) Which of the following is a set of short-range wireless technologies used to share information among devices within about two inches of each other?
A) DES
B) NFC
C) IM
D) text messaging

15) Which of the following statements is *not* true?
A) Digital cash is legal tender that is instantly convertible into other forms of value without the intermediation of any third parties
B) The easiest and least expensive way to prevent threats to system integrity is to install anti-virus software
C) SLS/TLS cannot provide irrefutability
D) Digital signatures and hash digests can add authentication, nonrepudiation, and integrity when used with public key encryption

Exercise (Part II)

16) To allow lower-level employees access to the corporate network while preventing them from accessing private human resources documents, you would use:
A) access controls
B) an authorization management system
C) security tokens
D) an authorization policy

17) Which of the following statements is *not* true?
A) Apple's Touch ID stores a user's actual fingerprint
B) Biometric devices reduce the opportunity for spoofing
C) A retina scan is an example of a biometric device
D) Biometric data stored on an iPhone is encrypted

18) Which of the following statements is not true?
A) A VPN provides both confidentiality and integrity
B) A VPN uses both authentication and encryption
C) A VPN uses a dedicated secure line
D) The primary use of VPNs is to establish secure communications among business partners

Exercise (Part II)

19) Which of the following is *not* an example of an access control?
A) firewalls
B) proxy servers
C) digital signatures
D) login passwords

20) All of the following are methods of securing channels of communication *except*:
A) SSL/TLS
B) certificates
C) VPN
D) FTP

21) _____ is the current standard used to protect Wi-Fi networks.
A) WEP
B) TLS
C) WPA2
D) WPA3

Exercise (Part II)

22) The Data Encryption Standard uses a(n) _____-bit key.

23) Advanced Encryption Standard (AES) is a widely used symmetric key algorithm, which offers key sizes of many kinds of bits *except*:
A) 128
B) 192
C) 256
D) 2048

24) A digital certificate is a digital document issued by a trusted third-party institution known as a certification authority (CA) that contains many contents *except*:
A) Name of subject/company
B) Subject's private key
C) Digital certificate serial number and digital signature of CA
D) Expiration date, issuance date

1. List at least 6 major tools available to achieve e-commerce security.

2. What is public key cryptography? Give a simple case to illustrates the simple use of public key cryptography.