Chapter 5

E-Commerce Security and Payment Systems

Learning Objectives

- **Know the key security threats in the e-commerce environment**

  了解電子商務環境中的主要安全威脅

- **Know how technology helps secure Internet communications channels and protect networks, servers, and clients**

  了解科技如何保護互聯網通信信道以及網絡、服務器和消費者機

- **Know the importance of policies, procedures, and laws in creating security**

  了解各種安全政策、程序和法律對創建安全環境的重要性

Contents

- **Background of The E-commerce Security Environment**
  電子商務安全環境背景
- **Security Threats in the E-Commerce Environment**
  電子商務環境中的安全威脅
- **Technology Solutions**
  技術解決方案
- **Management Policies, Business Procedures, and Public Laws**
  管理政策、企業流程和法律
- **E-commerce Payment Systems**
  電子商務支付系統
- **Electronic Billing Presentment and Pay**
  電子賬單的展示與支付

Part I:

Background of The E-Commerce Security Environment

Background

SOME MAJOR TRENDS IN E-COMMERCE SECURITY

- Large-scale data breaches continue to expose data about individuals to hackers and other cybercriminals; hacking related to cryptocurrencies skyrockets.
- Mobile malware presents a tangible threat as smartphones and other mobile devices become more common targets of cybercriminals, especially as their use for mobile payments increases.
- Malware and ransomware attacks rise.
- Distributed Denial of Service (DDoS) attacks are now capable of slowing Internet service within entire countries.
- Hackers and cybercriminals continue to focus their efforts on social networks to exploit potential victims via social engineering and hacking attacks.
- Politically motivated, targeted attacks by hacktivist groups continue, in some cases merging with financially motivated cybercriminals to target financial systems with advanced persistent threats.
- Software vulnerabilities, such as the Apache open-source software Log4j vulnerability, as well as other zero-day vulnerabilities, continue to create security threats.
- Software supply chain attacks, such as the SolarWinds attack, in which hackers target development environments to infect software that is then downloaded by end users, increase in frequency.

Background

The Cyber Black Market for Stolen Data

DATA	PRICE*
Individual U.S. card number with expiration date and CVV2 (the three-digit number printed on back of card) (referred to as a CVV)	$5–$8
Individual U.S. card number with full information, including full name, billing address, expiration date, CVV2, date of birth, mother's maiden name, etc. (referred to as a Fullz or Fullzinfo)	$20–$60
Dump data for U.S. card (the term "dump" refers to raw data such as name, account number, expiration data, and CVV encoded on the magnetic strip on the back of the card)	$60–$100
Bank account login credentials	$80–$700
Online payment service accounts (PayPal, etc.)	$20–$300
Drivers license information	$20
Online account login credentials (Facebook, Twitter, eBay, Apple)	$10–$15
Medical information/health credentials	$10–$20
1,000 e-mail addresses	$1–$10
Scan of a passport	$1–$25
Social security number	$1

SOURCES: Based on data from Symantec, 2019; Stack, 2018; Osborne, 2018.

*Prices vary based on supply and quality (freshness of data, account balances, validity, etc.).

1. What Is Good E-Commerce Security?

什麼是良好的電子商務安全？

- Good e-commerce security requires a set of laws, procedures, policies, and technologies that, to the extent feasible, protect individuals and organizations from unexpected behavior in the e-commerce marketplace.

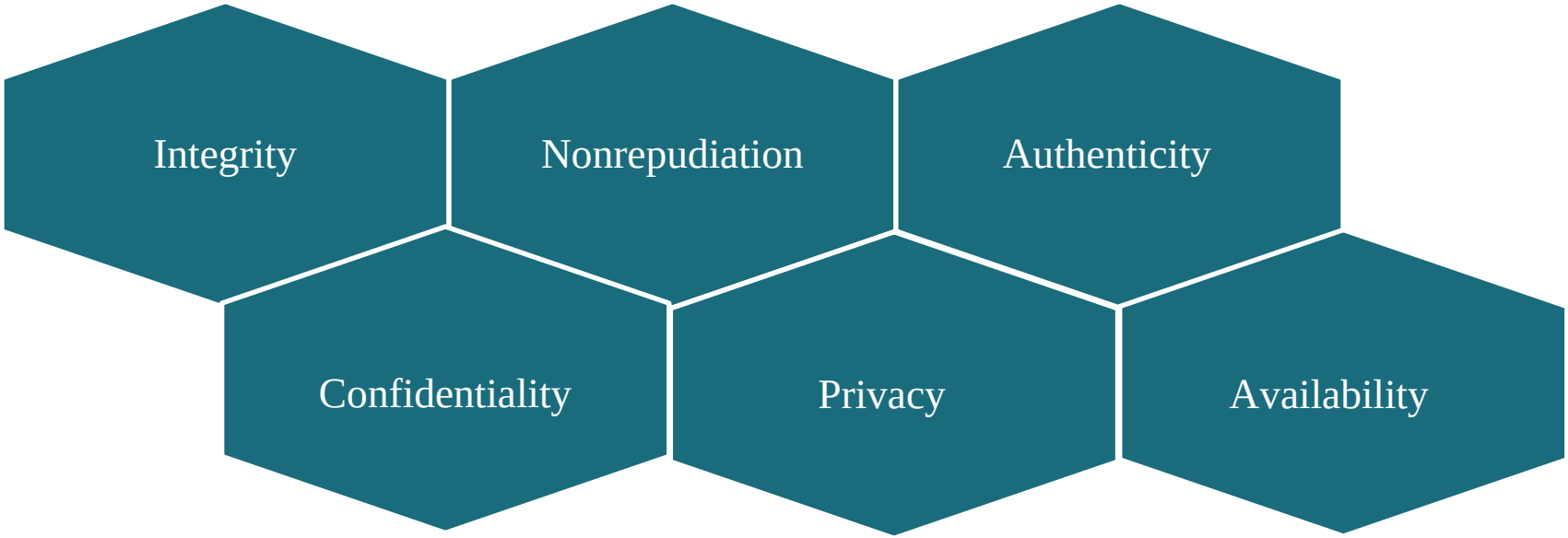
  良好的電子商務安全需要一系列的法律、程序、政策和技術的保障，在可行的範圍內保護個人和組織免受電子商務市場中無法預料的行爲.

2. Dimensions of E-commerce Security

電子商務安全的維度

- There are six key dimensions to e-commerce security: integrity, nonrepudiation, authenticity, confidentiality, privacy, and availability.

  電子商務安全有六個關鍵維度：完整性、不可否認性、真實性、機密性、隱私性和可用性.



2. Dimensions of E-commerce Security

電子商務安全的維度

- **Integrity** refers to the ability to ensure that information being displayed on a website, or transmitted or received over the Internet, has not been altered in any way by an unauthorized party. For example, if an unauthorized person intercepts and changes the contents of an online communication, such as by redirecting a bank wire transfer into a different account, the integrity of the message has been compromised because the communication no longer represents what the original sender intended.

  完整性是指確保網站上發布的的信息或通過互聯網傳輸或接收的信息不會被任何未經授權方以任何方式修改的能力. 例如，如果某個未經授權者截獲並更改了某條網上信息內容，比如重置某條銀行轉賬信息，使款項劃入其他賬戶，那麼該信息就不再代表原始發送者的初衷，意味著信息的完整性受到破壞.

2. Dimensions of E-commerce Security

電子商務安全的維度

- **Nonrepudiation** refers to the ability to ensure that e-commerce participants do not deny (i.e., repudiate) their online actions. For instance, the availability of free e-mail accounts with alias names makes it easy for a person to post comments or send a message and perhaps later deny doing so. Even when a customer uses a real name and e-mail address, it is easy for that customer to order merchandise online and then later deny doing so.

  不可否認性是指確保電子商務參與者不能否認其在綫行爲的能力. 例如, 通過使用匿名的免費電子郵件帳戶, 一個人可以很容易地發表評論或發送消息, 而事後可能否認曾做過這些事. 即使客戶使用真實姓名和電子郵件地址在網上訂購商品後, 否認曾下過訂單也很容易.

2. Dimensions of E-commerce Security

電子商務安全的維度

- **Authenticity** refers to the ability to identify the identity of a person or entity with whom you are dealing on the Internet. How does the customer know that the website operator is who it claims to be? How can the merchant be assured that customers really are who they say they are? Someone who claims to be someone he is not is “spoofing” or misrepresenting himself..

  真實性是指識別在互聯網上與你交易的個人或實體的身份的能力. 客戶如何知道網站經營者就是所聲稱的人？商家如何保證顧客真的是他本人？有些人聲稱自己是某某人或者某某商家，其實是在進行“電子欺騙”或虛假陳述.

2. Dimensions of E-commerce Security

電子商務安全的維度

- **Confidentiality** refers to the ability to ensure that messages and data are available only to those who are authorized to view them. Confidentiality is sometimes confused with **privacy**, which refers to the ability to control the use of information a customer provides about himself or herself to an e-commerce merchant.

  機密性是指確保信息和數據只能被得到授權的人讀取的能力. 機密性有時會與隱私相混淆，**隱私性**是指控制客戶提供給電子商務商家的關於他或她個人信息如何使用的能力.

  - E-commerce merchants have two concerns related to privacy. They must establish internal policies that govern their own use of customer information, and they must protect that information from illegitimate or unauthorized use. For example, if hackers break into an e-commerce site and gain access to credit card or other information, this violates not only the confidentiality of the data, but also the privacy of the individuals who supplied the information.

    電子商務商家會涉及兩個與隱私性相關的問題：他們必須建立內部政策來管理他們自己對消費者信息的使用，並且他們必須保護這些信息不被非法或未經授權使用. 例如，如果黑客闖入電子商務網站並獲取了信用卡或其他信息，這不僅損害了信息的機密性，而且還侵犯了提供信息的個人的隱私.

2. Dimensions of E-commerce Security

電子商務安全的維度

- **Availability** refers to the ability to ensure that an e-commerce site continues to function as intended.
  可用性是指確保電子商務網站繼續按預期功能運行的能力.

2. Dimensions of E-commerce Security

電子商務安全的維度

CUSTOMER AND MERCHANT PERSPECTIVES ON THE DIFFERENT DIMENSIONS OF E-COMMERCE SECURITY

DIMENSION	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Integrity	Has information I transmitted or received been altered?	Has data been altered without authorization? Is data being received from customers valid?
Nonrepudiation	Can a party to an action with me later deny taking the action?	Can a customer deny ordering products?
Authenticity	Whom am I dealing with? How can I be assured that the person or entity is who they claim to be?	What is the real identity of the customer?
Confidentiality	Can someone other than the intended recipient read my messages?	Are messages or confidential data accessible to anyone other than those authorized to view them?
Privacy	Can I control the use of the personal information that I am transmitting to an e-commerce merchant?	What use, if any, can be made of personal data collected as part of an e-commerce transaction? Is the personal information of customers being used in an unauthorized manner?
Availability	Can I access the site or app?	Is the site or app operational?

3. The Tension Between Security & Ease of Use

安全與易用間的關係

Can there be too much security? The answer is yes. Security is not an unmitigated good. Computer security adds overhead and expense to business operations and often complicates the process of making a purchase.

需要這麼多安全舉措嗎?答案是肯定的. 安全並不是無懈可擊. 計算機安全給企業增加業務運營的開銷和費用，並且通常會使購買過程複雜化.

- **Security and Ease of Use 安全與易用**
  - There are inevitable tensions between security and ease of use. In general, the more security measures added to an e-commerce site, the more difficult it is to use and the slower the site becomes. Digital security is purchased at the price of slowing down processors and adding significantly to data storage demands on storage devices. Security is a technological and business overhead that can detract from doing business. Too much security can harm profitability, while not enough security can potentially put you out of business. One solution is to adjust security settings to the user's preferences.

    安全性與便於使用之間存在不可避免的取捨關係. 一般來說，電子商務網站的安全措施越多，使用起來越不方便，網站的運行速度就越慢. 數字安全是以降低處理器速度和提高存儲設備的數據存儲能力爲代價的. 安全需要技術支持和耗費業務成本，會影響企業運營. 過多的安全措施會損害企業盈利能力，而安全力度不夠可能會使企業破產. 一種解決方案是根據用戶的喜好調整安全設置.

3. The Tension Between Security & Ease of Use

安全與易用間的關係

Can there be too much security? The answer is yes. Security is not an unmitigated good. Computer security adds overhead and expense to business operations and often complicates the process of making a purchase.

需要這麼多安全舉措嗎?答案是肯定的. 安全並不是無懈可擊. 計算機安全給企業增加業務運營的開銷和費用，並且通常會使購買過程複雜化.

- **Security and Ease of Use 安全與易用**
  - It is possible to have both ease of use and security by adjusting the authentication process for each customer, providing options from automatic login (low security), to downloadable one-time passwords (high security).

    通過調整每個消費者的身份驗證過程，提供從自動登錄（低安全性）到可下載的一次性密碼（高安全性）等選項，可以同時兼顧易用性和安全性.

Part II:

Security Threats in the E-Commerce Environment

1. Security Threats

安全威脅

- From a technology perspective, three key points of vulnerability in e-commerce environment:

  從技術角度看，電子商務中有三個關鍵的薄弱點:

  - Client

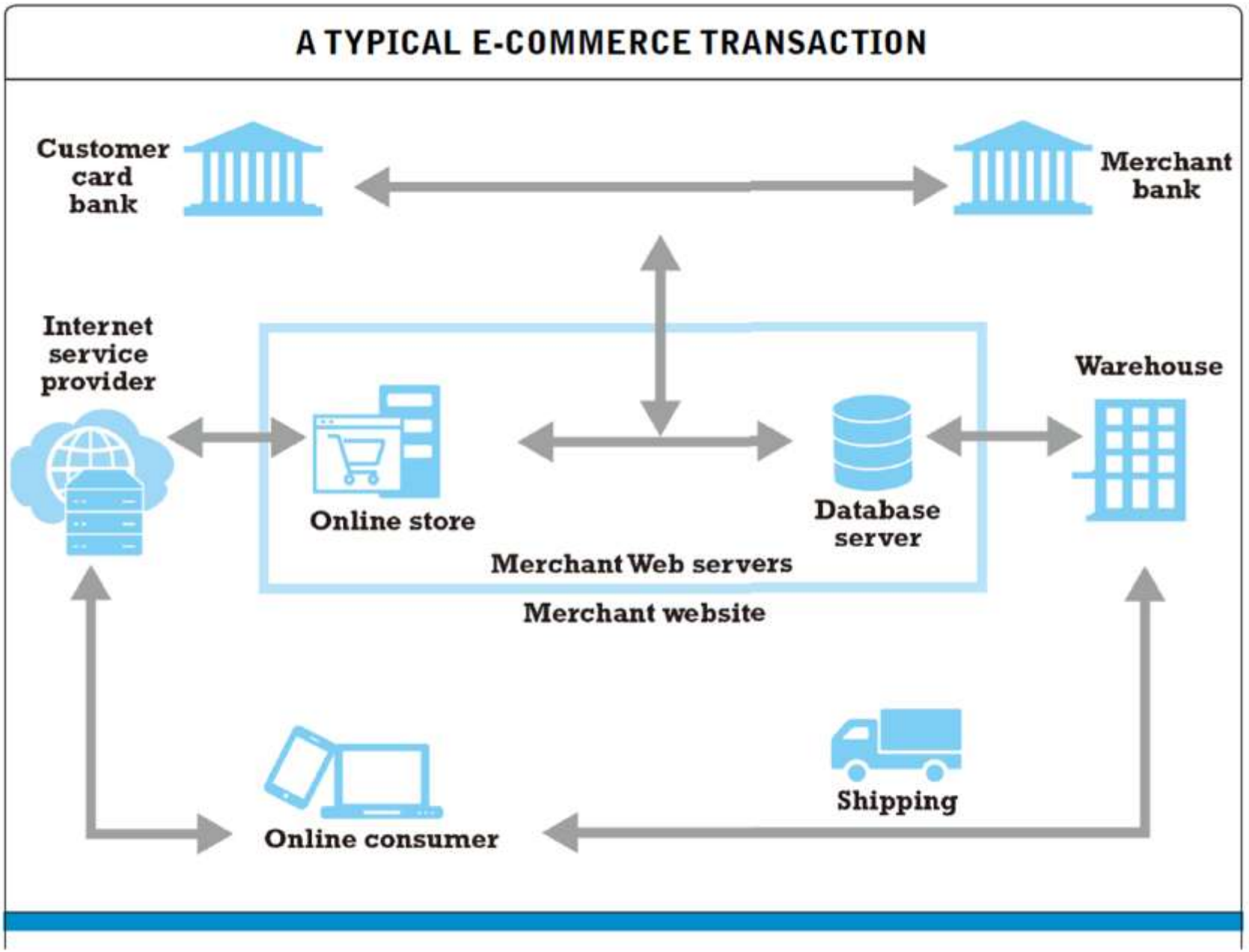
    客戶機

  - Server

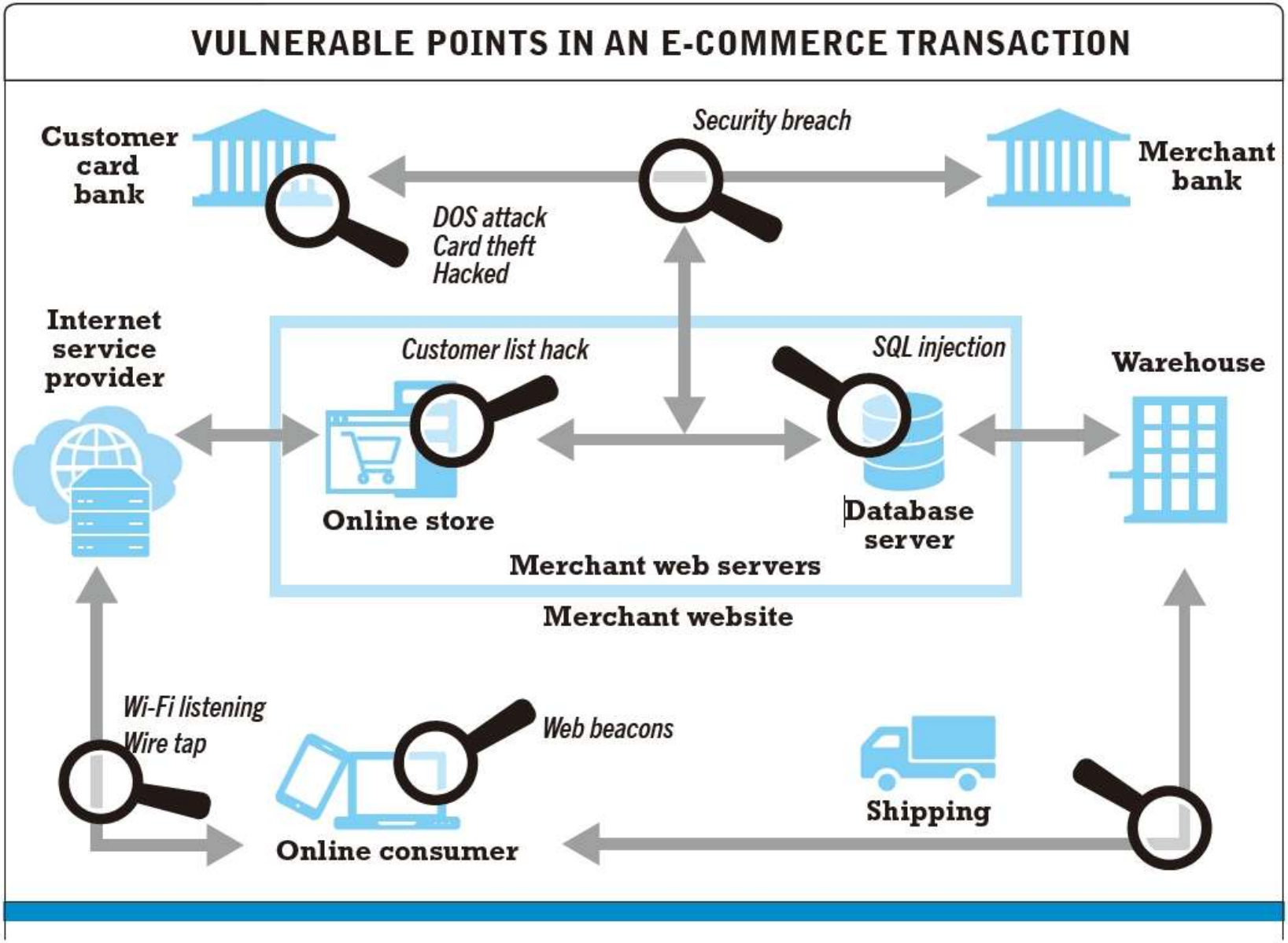
    服務器

  - Communications pipeline: Internet communications channels

    通信信道：互聯網通信渠道



In a typical e-commerce transaction, the customer uses a bank card and the existing payment system.



There are three major vulnerable points in e-commerce transactions: Internet communications, servers, and clients.

1. Security Threats

安全威脅

- The most common and most damaging forms of security threats to e-commerce consumers and site operators: malicious code, potentially unwanted programs, phishing, hacking and cybervandalism, data breaches, bank card fraud/theft, spoofing, pharming, spam websites, identity fraud, Denial of Service (DoS) and DDoS attacks, sniffing, insider attacks, and poorly designed server and client software, as well as security issues with respect to social networks, the mobile platform, cloud computing, the Internet of Things (IoT), and the metaverse.

對電子商務消費者和網站運營商來說最常見和最具破壞性的安全威脅：惡意代碼、潛在不必要程序、網絡釣魚、黑客攻擊和網絡破壞、數據泄露、銀行卡欺詐/竊取、電子欺騙、網址嫁接、垃圾網站、身份欺詐、拒絕服務攻擊和分布式拒絕服務攻擊、網絡竊聽、內部攻擊、設計不當的服務器和客戶端軟件、社交網絡安全問題、移動平台網絡安全問題、雲計算網絡安全問題、物聯網網絡安全問題和元宇宙安全問題

1. Security Threats

安全威脅

Malicious Code 惡意代碼

- **Malicious code** (sometimes referred to as “malware”) includes a variety of threats such as viruses, worms, Trojan horses, ransomware, and bots. Some malicious code, sometimes referred to as an exploit, is designed to take advantage of software vulnerabilities in a computer’s operating system, web browser, applications, or other software components. In the past, malicious code was often intended to simply impair computers and was often created by amateur hackers, but increasingly it involves a group of hackers (or a nation-state-supported group), and the intent is to steal e-mail addresses, logon credentials, personal data, and financial information.

惡意代碼（有時稱爲“惡意軟件”）包括各種威脅，例如病毒、蠕蟲、特洛伊木馬、勒索軟件和僵尸程序. 某些惡意代碼（有時稱爲漏洞）旨在利用計算機操作系統、web瀏覽器、應用程序或其他軟件組件中的軟件漏洞. 過去，惡意代碼通常由一個單獨的黑客編寫，用於損害計算機，但現在越來越多的惡意代碼涉及一群黑客甚至是一個國家支持的團體，目的是竊取電子郵件地址、登錄信息、個人數據和財務信息.

1. Security Threats

安全威脅

Malicious Code 惡意代碼

- **Exploit kits** are collections of exploits bundled together and rented or sold as a commercial product, often with slick user interfaces and in-depth analytics functionality.

  漏洞利用工具包是捆綁在一起的漏洞利用工具集合，被作爲商業産品出租或出售，通常具有流暢的用戶界面和深入的分析功能.

- Use of an exploit kit typically does not require much technical skill, enabling novices to become cybercriminals easily.

  使用漏洞利用工具包通常不需要太多技術技能，這使新手也能容易的成爲網絡犯罪分子.

1. Security Threats

安全威脅

Malicious Code 惡意代碼

- Malware is often delivered in the form of a malicious attachment to an e-mail or is embedded as a link in the e-mail. Malicious links can also be placed in innocent-looking Microsoft Word or Excel documents. The links lead directly to a malicious code download or websites that include malicious code.

  惡意鏈接通常以惡意附件形式發送到電子郵件中，或作爲鏈接嵌入電子郵件中. 惡意鏈接也可以放置在看起來無害的Microsoft Word或Excel文檔中. 這些鏈接直接指向惡意代碼下載或包含惡意代碼的網站.

- A **drive-by download** is malware that comes with a downloaded file that a user intentionally or unintentionally requests. Drive-by downloads are now one of the most common methods of infecting computers.

  路過式下載是指用戶有意或無意請求的下載文件中附帶了惡意代碼. 現在，路過式下載是感染計算機的最常見方法之一.

1. Security Threats

安全威脅

Malicious Code 惡意代碼

- Another method for malicious code distribution is to embed it in the online advertising chain (known as malvertising). As the ad network chain becomes more complicated, it becomes increasingly difficult for companies to vet ads placed on their websites and apps to ensure they are malware-free. One way users can combat malicious ads is by installing ad blockers. .

  惡意代碼分發的另一種方法是將其嵌入在綫廣告鏈（稱爲惡意廣告）. 隨著廣告網絡鏈變得越來越複雜，網站審核放置在其網站上的廣告以確保它們不含惡意代碼的難度越來越大. 用戶可以對抗惡意廣告的一種方法是安裝廣告攔截器.

1. Security Threats

安全威脅

Malicious Code 惡意代碼

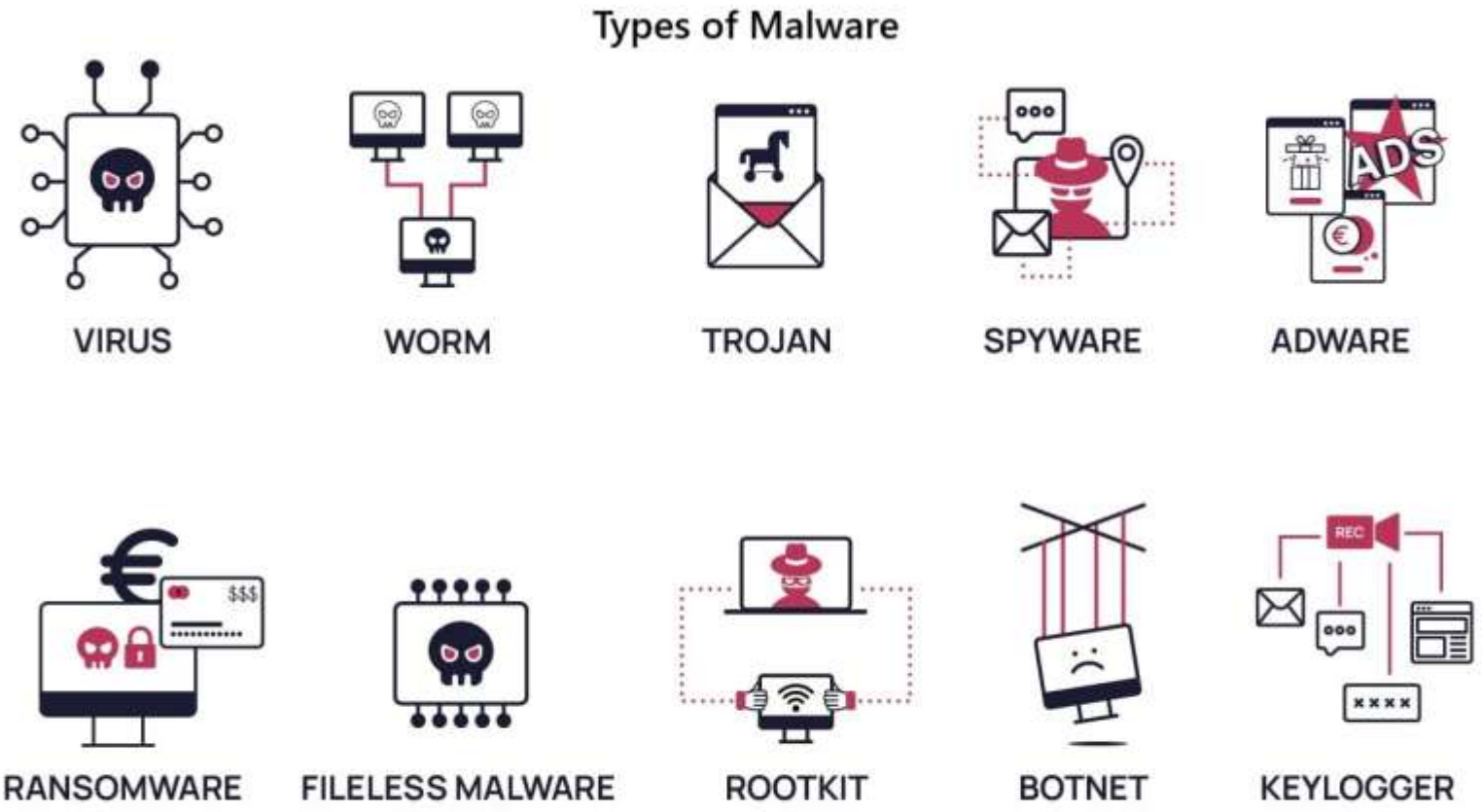
- Much of the malvertising in past years was in the form of drive-by downloads that exploited the frequent zero-day vulnerabilities that plagued Adobe Flash, which was often used for online advertisements. As a result, the Internet Advertising Bureau urged advertisers to abandon Adobe Flash in favor of HTML5, and Mozilla Firefox, Apple's Safari, and Google's Chrome browser all now block Flash advertisements from autoplaying. Adobe no longer distributes or updates the Flash Player.

  過去幾年中的許多惡意廣告都是以路過式下載的形式傳播的，利用了Adobe Flash中頻繁出現的零日漏洞，其中Adobe Flash常用於在綫廣告. 因此，互聯網廣告局敦促廣告商放弃Adobe Flash，轉而使用HTML5，而Mozilla Firefox、蘋果的 Safari 和穀歌的 Chrome瀏覽器現在都禁止了 Flash 廣告的自動播放. Adobe 不再發佈或更新 Flash Player.

1. Security Threats

安全威脅

Malicious Code 惡意代碼



1. Security Threats

安全威脅

Malicious Code 惡意代碼

- A **virus** is a computer program that can replicate or make copies of itself and spread to other files. In addition to the ability to replicate, most computer viruses deliver a "payload." The payload may be relatively benign, such as the display of a message or image, or it may be highly destructive—destroying files, reformatting the computer's hard drive, or causing programs to run improperly.

  病毒是一種具備自我複製能力並能够傳播到其他文件中的計算機程序. 除了具有自我複製能力外，大多數計算機病毒還具有"有效載荷". 有效載荷可能是相對良性的，例如消息或圖像的顯示，也可能具有很强的破壞性，會損害文件、格式化計算機的硬盤驅動器或導致程序運行不正常.

Virus

1. Security Threats

安全威脅

Malicious Code 惡意代碼

Some common types of computer viruses

- **Polymorphic virus:** By regularly mutating, these viruses nimbly avoid detection.
  多態病毒：通過定期變异，這些病毒可以靈活地逃避檢測.
- **Multipartite virus:** This computer virus simultaneously infects the boot sector and files, performing unauthorized actions to spread.
  混合型病毒：這種計算機病毒同時感染引導扇區和文件，執行未經授權的操作以及進行傳播.
- **Boot sector virus:** Often transmitted via a malicious USB drive, this virus typically targets the Master Boot Record.
  引導扇區病毒：該病毒通常通過惡意 USB 驅動器傳播，通常以主引導記錄爲目標.
- **File infector:** Also known as a file-infecting virus, a file infector generally attaches to executable files or command extensions.
  文件感染程序：也稱爲文件感染病毒，文件感染程序通常附加到可執行文件或命令擴展.
- **Browser hijacker:** A browser hijacker redirects your browser to malicious websites.
  瀏覽器劫持者：瀏覽器劫持者會將您的瀏覽器重定向到惡意網站.

Virus

1. Security Threats

安全威脅

Malicious Code 惡意代碼

Some common types of computer viruses

- **Web scripting virus:** Hiding in the coding of links, images, ads, videos, and websites, a web scripting virus can infect systems through downloads or visits to an infected website.
  網頁脚本病毒：網頁脚本病毒隱藏在鏈接、圖像、廣告、視頻和網站的編碼中，可以通過下載或訪問受感染的網站來感染系統.
- **Network virus:** A network virus travels through the network and replicates via network packets.
  網絡病毒：網絡病毒通過網絡傳播並通過網絡數據包進行複製.
- **Macro virus:** Often transmitted via an infected Microsoft Word or Excel file, macro viruses are written in the same macro language as the software and frequently spread through email attachments.
  宏病毒：宏病毒通常通過受感染的 Microsoft Word 或 Excel 文件傳播，其使用與軟件相同的宏語言編寫，並且經常通過電子郵件附件傳播.
- **Overwrite virus:** This computer virus overwrites file content with its own code to destroy system elements.
  覆蓋型病毒：這種計算機病毒用自己的代碼覆蓋文件內容以破壞系統元素.

Virus

1. Security Threats

安全威脅

Malicious Code 惡意代碼

- **Viruses** are often combined with a worm. Instead of just spreading from file to file, a worm is designed to spread from computer to computer. A worm does not necessarily need to be activated by a user or program in order to replicate itself.

  病毒通常與蠕蟲結合. 蠕蟲不僅可以在文件之間傳播，還可以在計算機之間傳播. 蠕蟲不是必須由用戶或程序激活才能自我複製.

Worm

1. Security Threats

安全威脅

Malicious Code 惡意代碼

Ransomware

- **Ransomware** is a type of malware (often a worm) that locks your computer or files to stop you from accessing them. For example, CryptoLocker, it encrypts victims' files with a virtually unbreakable asymmetric encryption and demands a ransom to decrypt them, often in Bitcoins. If the victim does not comply within the time allowed, the files will never be able to be decrypted. Other variants include CryptoDefense and Cryptowall. The growth of ransomware is also related to the growth of the virtual currency Bitcoin. Hackers often demand victims pay using Bitcoin so their transactions are hidden from authorities.

勒索軟件是一種惡意軟件（通常是蠕蟲），它會鎖定你的計算機或文件，阻止你訪問它們. 比如CryptoLocker，它使用幾乎牢不可破的非對稱加密來加密受害者的文件，並要求贖金來解密，通常使用比特幣. 如果受害者在允許的時間內不支付，文件將永遠無法解密. 其他變體包括CryptoDefense和Cryptowall. 勒索軟件的增長也與虛擬貨幣比特幣的增長有關. 黑客經常要求受害者使用比特幣付款，以便對官方隱瞞他們的交易.

1. Security Threats

安全威脅

Malicious Code 惡意代碼

Trojan horse

- A **Trojan horse** is software that appears to be benign but then does something other than expected. The Trojan horse is not itself a virus because it does not replicate but is often a way for viruses or other malicious code such as bots or rootkits (a program whose aim is to subvert control of the computer's operating system) to be introduced into a computer system. In today's world, Trojan downloaders and droppers (Trojans that install malicious files into a computer they have infected by either downloading them from a remote computer or from a copy contained in their own code) are a common type of malware.

  特洛伊木馬表面上看起來是無害的，但會產生令人意想不到的後果. 特洛伊木馬本身不是病毒，因爲它不能複製，但通常是病毒或其他惡意代碼（例如僵尸程序或rootkits（旨在破壞計算機操作系統控制的程序））感染計算機的一種工具. 在當今世界，特洛伊木馬可能會僞裝成游戲，但實際上隱藏了一個可以竊取你的密碼並將其通過電子郵件發送給其他人的程序. 各種各樣的特洛伊木馬以及特洛伊木馬下載器和釋放器（將從遠程計算機或其自身代碼包含的副本中下載的惡意文件安裝到其感染的計算機上的木馬程序）是常見的惡意代碼.

1. Security Threats

安全威脅

Malicious Code 惡意代碼

Backdoor

- **A backdoor** is a feature of viruses, worms, and Trojans that allows an attacker to remotely access a compromised computer. Downadup is an example of a worm with a backdoor, while Virut, a virus that infects various file types, also includes a backdoor that can be used to download and install additional threats.
  後門是病毒、蠕蟲和特洛伊木馬的一個功能，允許攻擊者遠程訪問受感染的計算機. Downadup是帶有後門的蠕蟲的一個示例，而感染各種文件類型的病毒 Virut 也有後門，可用於下載和安裝其他病毒.
- Besides, the backdoor refers to the access of the software or hardware of a computer system without being detected. The backdoor can be created by the developer themselves so that they can quickly and easily make changes to the code without the need to log in to the system.
  此外，後門是指在不被發現的情況下訪問計算機系統的軟件或硬件. 後門可以由開發者自己創建，這樣他們就可以快速輕鬆地對代碼進行更改，而無需登錄系統.

1. Security Threats

安全威脅

Malicious Code 惡意代碼

- **Bots** (short for robots) are a type of malicious code that can be covertly installed on your computer when attached to the Internet. Once installed, the bot responds to external commands sent by the attacker; your computer becomes a "zombie" and is able to be controlled by an external third party (the "bot-herder"). **Botnets** are collections of captured computers used for malicious activities such as sending spam, participating in a DDoS attack, stealing information from computers, and storing network traffic for later analysis. The number of botnets operating worldwide is not known but is estimated to be well in the thousands, potentially controlling millions of computers. Bots and bot networks are significant threats because they can be used to launch very large-scale attacks using many different techniques.

Bot

僵尸程序（robots的縮寫）是一種惡意代碼，當連接到互聯網時可以秘密安裝在計算機上. 一旦安裝後，僵尸程序響應外部攻擊者發送的命令，計算機將成爲"僵尸"，並可由外部第三方（"僵尸程序托管者"）進行控制. **僵尸網絡**是一系列被感染的計算機的集合，這些計算機被用於惡意活動，例如發送垃圾郵件，參與DDoS攻擊，從其他計算機中竊取信息以及存儲網絡流量以供以後分析. 世界範圍內運行的僵尸網絡的數量不詳，但估計有數千個，控制著數以百萬計的計算機. 僵程序和僵尸網絡是互聯網和電子商務面臨的重要威脅，因爲它們可以使用許多不同的技術來發起大規模的攻擊.

1. Security Threats

安全威脅

Malicious Code 惡意代碼

Good vs. evil bot uses

GOOD BOTS	BAD BOTS
Chatbot for a customer service application	DDoS bots that overwhelm a system with malicious traffic
Bots that automate news content and headlines	Keylogger bots that track a user's keystrokes
Social bots for measuring customer engagement	Spam bots that pester users into clicking on malicious links
Monitoring bots that track the health of the system	Email bots that send messages without the user's permission
Web crawlers that gather indexes for search engines	Web crawlers that scour the web for a user's personal information

1. Security Threats

Virus **病毒**	A computer program that has the ability to replicate or make copies of itself, and spread to other files. A virus generally require a host program 一種能够複製或自我複製並傳播到其他文件的計算機程序. 病毒通常需要宿主程序
Worm **蠕蟲**	Instead of just spreading from file to file, a worm is designed to spread from computer to computer. A worm does not need a host program 蠕蟲不僅可以在文件之間傳播，還可以在計算機之間傳播. 蠕蟲不需要宿主程序
Ransomware **勒索軟件**	A malware that prevents you from accessing your computer or files and demands that you pay a fine 阻止您訪問計算機或文件並要求您支付罰款的惡意軟件
Trojan horse **特洛伊木馬**	It appears to be benign, but then does something other than expected. Often a way for viruses or other malicious code to be introduced into a computer system 看起來是良性的，但隨後做了一些超出預期的事情. 通常是將病毒或其他惡意代碼引入計算機系統的一種方式
Backdoor **後門**	It is a feature of viruses, worms, and Trojans that allows an attacker to remotely access a compromised computer 病毒、蠕蟲和特洛伊木馬的一個功能，允許攻擊者遠程訪問受感染的計算機
Bot **僵尸程序**	Is a type of malicious code that can be covertly installed on a computer when connected to the Internet. Once installed, the bot responds to external commands sent by the attacker 連接到Internet時可以秘密安裝在計算機上的惡意代碼類型. 安裝後，機器人程序會對攻擊者發送的外部命令做出響應
Botnet **僵尸網絡**	They are collections of captured bot computers 捕獲的用於惡意活動的計算機的集合

1. Security Threats

EXAMPLES OF MALICIOUS CODE

NAME	TYPE	DESCRIPTION
Emotet	Trojan/Botnet	Described by Europol as the world's most dangerous malware. Initially used to steal bank login credentials by surreptitiously capturing people's keystrokes. Later versions added malware delivery services, including other Trojans and ransomware, and were spread via botnet. In January 2021, an internationally coordinated effort took down many Emotet botnets, but by November 2021, Emotet had once again resurfaced, indicating how difficult it is to fully eradicate.
WannaCry	Ransomware/ worm	Exploits vulnerabilities in older versions of Windows operating systems, encrypts data, and demands a ransom payment to decrypt them.
Cryptolocker	Ransomware/ Trojan	Hijacks users' data such as photos, videos, and documents, encrypts them with virtually unbreakable asymmetric encryption, and demands ransom payment for them.
Zeus	Trojan/botnet	Sometimes referred to as the king of financial malware. May install via drive-by download and evades detection by taking control of web browser and stealing data that is exchanged with bank servers.
Conficker	Worm	First appeared in 2008 and still a problem for users of older, unpatched Windows operating systems. Uses advanced malware techniques. Had nearly 10 million computers worldwide under its control.
Slammer	Worm	Launched in 2003. Caused widespread problems.
Melissa	Macro virus/ worm	First spotted in 1999. At the time, the fastest-spreading infectious program ever discovered. It attacked Microsoft Word's Normal.dot global template, ensuring infection of all newly created documents. It also mailed an infected Word file to the first 50 entries in each user's Microsoft Outlook Address Book.

1. Security Threats

安全威脅

Malicious Code 惡意代碼

- *Malicious code is a threat at both the client and the server levels, although servers generally have the benefit of much more thorough anti-malware protection than do consumers. At the server level, malicious code can bring down an entire website, preventing millions of people from using the site. Such incidents are relatively infrequent. Much more frequent malicious code attacks occur at the client level, and the damage can quickly spread to millions of other computers connected to the Internet.*

  惡意代碼在客戶機和服務器層面均構成威脅，儘管服務器通常比客戶機具有更多的反惡意代碼優勢. 在服務器層面，惡意代碼可以入侵整個網站，從而阻止數以百萬計的人使用該網站. 此類事件相對少見. 在客戶機層面，被惡意代碼攻擊的頻率更高，並且損害可以迅速蔓延至連接到互聯網上的數百萬台其他計算機.

1. Security Threats

安全威脅

Potentially Unwanted Programs 潛在不必要程序

- **Potentially unwanted programs** (PUPs) are application programs such as adware, browser parasites, spyware, and other applications, that install themselves on a computer, such as rogue security software, toolbars, and PC diagnostic tools, typically without the user's informed consent. Such programs are increasingly found on social network and usergenerated content sites where users are fooled into downloading them. Once installed, these applications are usually exceedingly difficult to remove from the computer.

潛在不必要程序是指通常在未經用戶知情同意的情況下自行安裝在計算機上的諸如廣告軟件、瀏覽器寄生蟲、間諜軟件等應用程序，例如流氓安全軟件、工具欄和計算機診斷工具. 此類程序越來越多地出現在社交網絡和用戶生成內容網站上，導致用戶被誤導下載它們. 一旦安裝，這些應用程序通常很難從計算機中刪除.

1. Security Threats

安全威脅

Potentially Unwanted Programs 潛在不必要程序

- Browser parasites 瀏覽器寄生蟲
  - Monitor and change user's browser

    監視和更改用戶瀏覽器的設置的程序

- Adware 廣告軟件
  - Typically used to call for pop-up ads to display when the user visits certain sites.

    在用戶訪問網站時調出彈出式廣告

- Spyware 間諜軟件
  - used to obtain information such as a user's keystrokes, copies of e-mail and instant messages, and even take screenshots (and thereby capture passwords or other confidential data)..

    用於獲取信息，例如用戶的鍵盤記錄、電子郵件和即時消息的副本，甚至截取屏幕截圖（從而捕獲密碼或其他保密數據）.

1. Security Threats

安全威脅

Phishing 網絡釣魚

- **Phishing** is any deceptive, online attempt by a third party to obtain confidential information for financial gain. Phishing attacks typically do not involve malicious code but instead rely on straightforward misrepresentation and fraud, so-called "social engineering" techniques.

  網絡釣魚是第三方爲獲得經濟利益而進行的任何欺騙性的網絡行爲. 網絡釣魚攻擊通常不涉及惡意代碼，而是依賴於直接的虛假陳述和欺詐，即所謂的"社會工程"技術.

- **Social engineering** relies on human curiosity, greed, gullibility, and fear in order to trick people into taking an action that enables a hacker to gain access to a computer system or results in the target downloading malware.

  社交工程利用人類的好奇心、貪婪、輕信和恐懼，誘騙人們進行可能導致惡意代碼下載的行爲，從而使黑客能够訪問計算機系統或導致目標下載惡意軟件.

1. Security Threats

安全威脅

Phishing 網絡釣魚

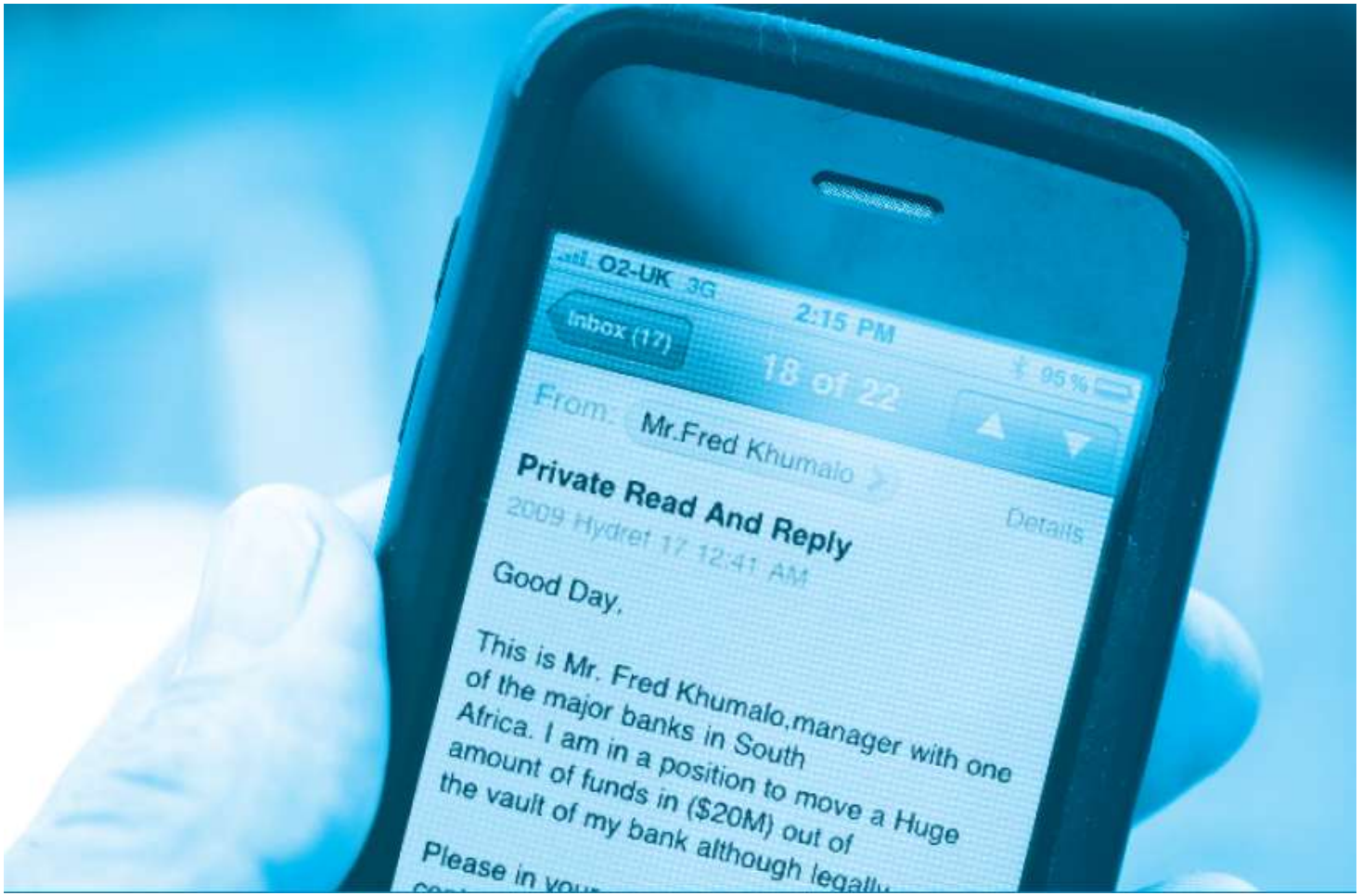
- Phishers rely on traditional “con man” tactics but also use e-mail or other forms of online communication, such as social media or text messaging, to trick recipients into voluntarily giving out financial access codes, bank account numbers, credit card numbers, and other personal information. One newer technique makes use of a fake chatbot to build trust with potential victims. Often, phishers create (or “spoof ”) a website that purports to be a legitimate institution and cons users into entering financial information, or the site downloads malware such as a keylogger to the victim’s computer..

網絡釣魚者依靠傳統的“贏得受騙人信任”的詐騙策略，使用電子郵件或其他形式的在綫交流工具（例如社交媒體或短信）來誘騙收件人自泄露銀行賬號、信用卡號和其他個人信息.通常，網絡釣魚者創建（或假裝）一個聲稱是合法機構的網站誘使用戶輸入財務信息，或者該網站將諸如鍵盤記錄程序之類的惡意代碼下載到用戶的計算機上.

1. Security Threats

安全威脅

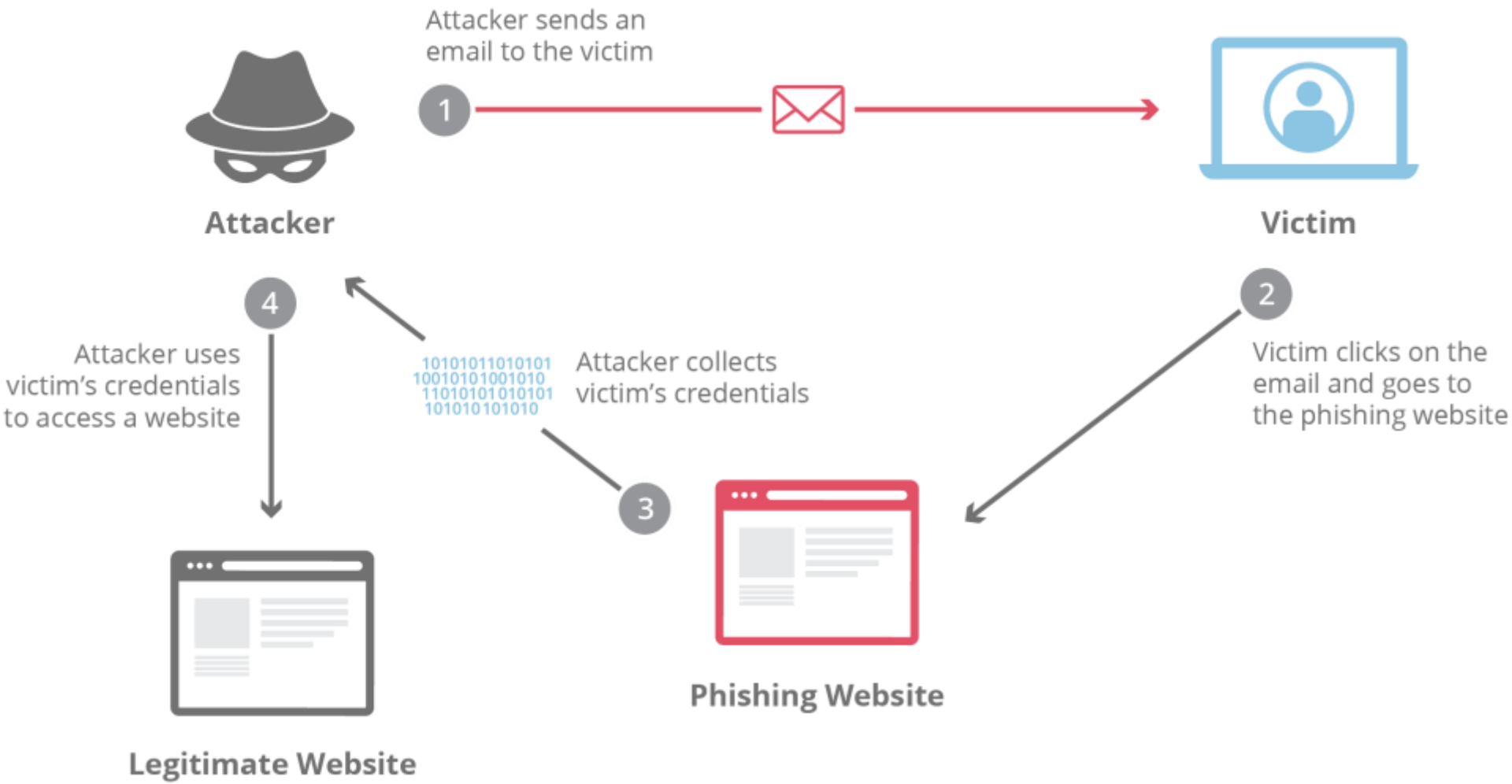
Phishing 網絡釣魚



1. Security Threats

安全威脅

Phishing 網絡釣魚



1. Security Threats

安全威脅

Phishing 網絡釣魚

- **BEC (business e-mail compromise) phishing:** In BEC phishing, an attacker poses as a high-level employee of a company and requests that another employee transfer funds to what is actually a fraudulent account. One specific type of BEC phishing that has also become prevalent involves requests for employee information sent to payroll or human resources personnel by scammers impersonating high-level company executives.

  商業電子郵件詐騙網絡釣魚：在BEC網絡釣魚中，攻擊者冒充公司的高級員工，要求另一位員工將資金轉入虛假賬戶.BEC網絡釣魚已變得非常普遍，其中包括騙子冒充公司高層管理人員要求財務人員或人力資源管理者提供員工報稅表信息.

1. Security Threats

安全威脅

Phishing 網絡釣魚

- Other phishing scams involve hackers sending e-mails that are purportedly from a trusted organization such as eBay, PayPal, or Wells Fargo and that ask for account verification (known as **spear phishing**, or targeting a known customer of a specific business). Click on a link in the e-mail, and you will be taken to a website controlled by the scammer and then prompted to enter confidential information about your accounts, such as your account number and PIN codes. On any given day, millions of these phishing attack e-mails are sent, and, unfortunately, some people are fooled and disclose their personal account information.

網絡釣魚攻擊還使用其他欺詐手段，其中有一些僞裝成eBay、PayPal或Wells向人們進行賬戶驗證（如**魚叉式網絡釣魚**，或針對特定銀行或其他類型企業的特定客戶）.點擊電子郵件中的鏈接，你將進入一個由詐騙者控制的網站，網站會提示你輸入有關你賬戶的機密信息，例如賬號和密碼.每天數以百萬計的此類網絡釣魚被發送，但不幸的是，有些人被欺騙並泄露了他們的個人賬戶信息.

1. Security Threats

安全威脅

Phishing 網絡釣魚

- **Spear phishing** is a type of phishing attack that targets a specific individual, group or organization. These personalized scams trick victims into divulging sensitive data, downloading malware or sending money to an attacker. Like all phishing scams, spear phishing involves manipulating victims through fake stories and fraudulent scenarios. Spear phishing attacks can be conducted through email messages, text messages, chat apps or phone calls.

  魚叉式網絡釣魚是一種網絡釣魚攻擊，它以組織內的特定個人或群體爲目標，試圖誘騙他們泄露敏感信息、下載惡意軟件或在不知情的情况下向攻擊者發送授權付款. 與所有網絡釣魚詐騙一樣，魚叉式網絡釣魚可以通過電子郵件、短信或電話進行. 不同之處在於，魚叉式網絡釣魚者不是采用全面的“批量網絡釣魚”計策來針對數千或數百萬潜在受害者，而是通過基於廣泛研究的個性化詐騙來針對特定個人或個人群體.

1. Security Threats

安全威脅

Hacking, Cybervandalism, and Hacktivism 黑客攻擊、網絡破壞和黑客行動主義

- A **hacker** is an individual who intends to gain unauthorized access to a computer system. Within the hacking community, the term **cracker** is typically used to denote a hacker with criminal intent, although in the public press, the terms hacker and cracker tend to be used interchangeably.
  黑客是企圖在未經授權的情況下訪問計算機系統的人. 在黑客社區中，**駭客**一詞通常用於表示具有犯罪意圖的黑客，儘管在公共媒體中，黑客和駭客往往可以互換使用.
- Hackers and crackers gain unauthorized access by finding weaknesses in the security procedures of websites and computer systems. In the past, hackers and crackers typically were computer aficionados excited by the challenge of breaking into corporate and government websites. Today, most hackers have malicious intentions to disrupt, deface, or destroy sites (cybervandalism) or to steal personal or corporate information they can use for financial gain (data breach).
  黑客和駭客常常利用互聯網作爲開發系統便於使用的特性，通過發現網站和計算機系統安全程序中的弱點來進行未經授權的訪問. 過去，黑客通常是計算機狂熱愛好者，他們對進入公司和政府網站的挑戰感到興奮. 有時，他們僅僅因能訪問電子商務網站的文件而感到興奮. 如今，大多數黑客惡意擾亂、破壞、摧毀網站（網絡破壞行爲），或竊取可用於牟利的個人或公司信息（數據泄露）.

1. Security Threats

安全威脅

Hacking, Cybervandalism, and Hacktivism 黑客攻擊、網絡破壞和黑客行動主義

- **Hacktivism** adds a political twist to hacking. Hacktivists typically attack governments, organizations, and even individuals for political purposes, employing the tactics of cybervandalism, DDoS attacks, data thefts, and doxing (gathering and exposing personal information of public figures, typically from e-mails, social network posts, and other documents). They often strongly believe that information should be free, so sharing previously secret information is part of their mission.
  黑客行爲主義具有政治色彩. 黑客行爲主義者通常出於政治目的，采用網絡破壞行爲策略、分布式拒絕服務攻擊、數據盜竊（收集和公開公衆人物的個人信息，通常來自電子郵件、社交網絡帖子以及其他文件）的方式攻擊政府、組織甚至個人. 他們通常堅信信息應該是免費的，因此共享以前的秘密信息是他們任務的一部分.
- Organizations sometimes hire ethical hackers to try to break into their systems from the outside in order to test their security measures. These types of hackers do their work under an agreement with the target firms that they will not be prosecuted for their efforts to break in.
  組織有時會雇傭正義黑客從外部入侵其系統，以測試自己的安全措施. 這些類型的黑客與目標公司簽訂了協議，他們不會因闖入而受到起訴.

1. Security Threats

安全威脅

Hacking, Cybervandalism, and Hacktivism 黑客攻擊、網絡破壞和黑客行動主義

- There are also hackers who believe they are pursuing some greater good by breaking in and revealing system flaws. These hackers discover weaknesses in a system's security and then publish the weaknesses without disrupting the site or attempting to profit from their finds. Their only reward is the prestige of discovering the weaknesses. Their actions are suspect, however, especially when such hackers reveal security flaws that make it easier for other criminals to gain access to a system.

  也有一些黑客認爲，他們通過入侵並揭示系統缺陷來追求更大的利益. 這些黑客發現了系統安全性方面的弱點，然後在不破壞站點或嘗試從其發現中獲利的情況下公布這一弱點. 他們唯一的回報就是因發現弱點而獲得的“威望”. 但是，他們的行爲令人懷疑，尤其是當此類黑客發現安全漏洞使其他罪犯更容易獲得系統訪問權限時.

1. Security Threats

安全威脅

Hacking, Cybervandalism, and Hacktivism　　黑客攻擊、網絡破壞和黑客行動主義

- **Main Types of Hackers**

White Hat Hacker

Gray Hat Hacker

Black Hat Hacker

1. Security Threats

安全威脅

Hacking, Cybervandalism, and Hacktivism 黑客攻擊、網絡破壞和黑客行動主義

- **Main Types of Hackers**

- **White hats**, "good" hackers, help organizations locate and fix security flaws. White hats do their work under contract, such as Apple, Microsoft, Intel, HP, and many others pay bounties of $25,000 to $250,000 to white hat hackers for discovering bugs in their software and hardware (Warren, 2018).

  白帽子，“好的”黑客，幫助組織定位和修復安全漏洞，簽訂合約工作，例如蘋果、微軟、英特爾、惠普和許多其他公司會向白帽黑客支付25,000到250,000美元的獎金，以獎勵他們發現軟件和硬件中的漏洞（沃倫，2018）.

1. Security Threats

安全威脅

Hacking, Cybervandalism, and Hacktivism 黑客攻擊、網絡破壞和黑客行動主義

- **Main Types of Hackers**
- **Black hats** are hackers who engage in the same kinds of activities but without pay or any buy-in from the targeted organization, and with the intention of causing harm. They break into websites and reveal the confidential or proprietary information they find.

黑帽子是從事相同類型活動，但不會得到任何被入侵企業的報酬，因爲他們的行爲具有破壞企圖. 他們入侵網站，泄露他們發現的機密或私人信息.

1. Security Threats

安全威脅

Hacking, Cybervandalism, and Hacktivism　　黑客攻擊、網絡破壞和黑客行動主義

- **Main Types of Hackers**
- Somewhere in the middle are the **grey hats**, hackers who believe they are pursuing some greater good by breaking in and revealing system flaws. Grey hats discover weaknesses in a system's security, and then publish the weakness without disrupting the site or attempting to profit from their finds. Their only reward is the prestige of discovering the weakness.

  介於兩者間的是**灰帽子**，他們認爲入侵並尋找系統缺陷可以得到更大的利益. 灰帽會發現系統安全中的弱點，然後在不破壞網站或不利用其獲利的情況下發布網站的弱點. 他們唯一的回報是發現弱點所贏得的聲望.

1. Security Threats

安全威脅

Hacking, Cybervandalism, and Hacktivism 黑客攻擊、網絡破壞和黑客行動主義

- **Other Types of Hackers**
- There are generally many types of hackers, after the main 3 types, they are:
  - Script Kiddie
  - Green Hat Hacker
  - Blue Hat Hacker
  - Red Hat Hacker
  - Hacktivist
  - Malicious Insider or Whistleblower

1. Security Threats

安全威脅

Hacking, Cybervandalism, and Hacktivism 黑客攻擊、網絡破壞和黑客行動主義

- **Other Types of Hackers**

- Script Kiddie: A Script kiddie is an unskilled person who uses scripts or downloads tools available for hacking provided by other hackers. They attempt to attack computer systems and networks and deface websites. Their main purpose is to impress their friends and society. Generally, Script Kiddies are juveniles who are unskilled about hacking.

  脚本小子：脚本小子是指那些沒有技術能力，却利用他人編寫的脚本或下載其他黑客提供的工具來進行攻擊的人. 他們試圖攻擊計算機系統和網絡，篡改網站. 他們的主要目的是給朋友和社會留下深刻印象. 通常，脚本小子是對黑客技術知之甚少的青少年.

1. Security Threats

安全威脅

Hacking, Cybervandalism, and Hacktivism 黑客攻擊、網絡破壞和黑客行動主義

- **Other Types of Hackers**

- Green Hat Hacker: Green hat hackers are also amateurs in the world of hacking but they are bit different from script kiddies. They care about hacking and strive to become full-blown hackers. They are inspired by the hackers and ask them few questions about. While hackers are answering their question they will listen to its novelty.

綠帽黑客：綠帽黑客也是黑客世界中的新手，但與脚本小子有所不同. 他們對黑客技術充滿熱情，並努力成爲真正的黑客. 他們受到黑客的啓發，會向黑客請教一些問題. 當黑客回答他們的問題時，他們會認真聆聽其中的新奇之處.

1. Security Threats

安全威脅

Hacking, Cybervandalism, and Hacktivism 黑客攻擊、網絡破壞和黑客行動主義

- **Other Types of Hackers**

- Blue Hat Hacker: Blue hat hackers are much like the white hat hackers, they work for companies for security testing of their software right before the product launch. Blue hat hackers are outsourced by the company unlike white hat hackers which are employed by the (part of the) company..

  藍帽黑客：藍帽黑客與白帽黑客非常相似，受雇於公司，負責在產品發布前進行軟件安全測試. 與公司內部的白帽黑客不同，藍帽黑客是公司外包的安全專家.

1. Security Threats

安全威脅

Hacking, Cybervandalism, and Hacktivism 黑客攻擊、網絡破壞和黑客行動主義

- **Other Types of Hackers**

- Red Hat Hacker: Red hat hackers are those who are appointed by the government to provide them cybersecurity and to gain confidential information from other countries to stay at the top or to avoid any kind of danger to the country. They are highly paid government workers.

  紅帽黑客：紅帽黑客也被稱爲鷹眼黑客. 與白帽黑客一樣，紅帽黑客的目標也是阻止黑帽黑客. 但他們的操作方式有很大不同. 他們在對付黑帽黑客的惡意行爲時毫不留情. 紅帽黑客會持續對黑客進行猛烈攻擊，以至於黑客可能不得不更換整個系統.

1. Security Threats

安全威脅

Hacking, Cybervandalism, and Hacktivism　　黑客攻擊、網絡破壞和黑客行動主義

- **Other Types of Hackers**

- Hacktivist: These are also called the online versions of the activists. Hacktivist is a hacker or a group of anonymous hackers who gain unauthorized access to government's computer files and networks for further social or political ends.

  黑客行動主義者：他們也被稱爲網絡版的行動主義者. 黑客行動主義者是指那些未經授權訪問政府計算機文件和網絡的黑客或匿名黑客團體，他們的目的是推動社會或政治目標.

1. Security Threats

安全威脅

Hacking, Cybervandalism, and Hacktivism 黑客攻擊、網絡破壞和黑客行動主義

- **Other Types of Hackers**

- Malicious Insider or Whistleblower: A malicious insider or a whistleblower could be an employee of a company or a government agency with a grudge or a strategic employee who becomes aware of any illegal activities happening within the organization and can blackmail the organization for his/her personal gain.

  惡意內部人員或告密者：惡意內部人員或告密者可能是公司或政府機構的員工，他們心懷不滿，或者是瞭解組織內非法活動的戰略員工，並可能以此敲詐組織以謀取個人利益.

1. Security Threats

安全威脅

Data Breaches 數據泄露

- A data breach occurs when organizations lose control over corporate information to outsiders.

  當組織對外部人員失去對公司信息的控制時，數據泄露就發生了.

- Data breaches are also an enabler for credential stuffing attacks. Credential stuffing is a brute force attack that hackers launch via botnets and automated tools using known username and password combinations (referred to as combo lists) obtained from data breaches.

  數據泄露也是撞庫攻擊的促成因素.撞庫是一種蠻力攻擊，黑客通過僵尸網絡和自動工具使用從數據泄露中獲得的特定用戶名和密碼組合(稱爲組合列表).

- Leading causes
  - Hacking 黑客攻擊
  - Employee error/negligence 員工錯誤/疏忽
  - Accidental e-mail/Internet exposure 意外電子郵件/互聯網泄露
  - Insider theft 內部盜竊

1. Security Threats

安全威脅

Bank Card Fraud 銀行卡欺詐

- Lost or stolen bank card
  銀行卡丟失或被盜
- Theft of customer identities (criminals applying for cards using false identities)
  盜竊客戶身份信息（犯罪分子使用虛假身份卡片）
- Hacking and looting of corporate servers
  黑客攻擊和劫持公司服務器
- Central security issue: establishing customer identity
  核心安全問題：確立客戶身份
  - E-signatures 電子簽名
  - Multi-factor authentication 多因素認證
  - Fingerprint identification 指紋識別

1. Security Threats

安全威脅

Identity Fraud 身份詐欺

- Unauthorized use of another person's personal data for illegal financial benefit

  即未經授權使用他人的個人數據，以獲取非法經濟利益

  - Identity card number 身份證號碼
  - Driver's license 駕駛執照
  - Credit card numbers 信用卡號碼
  - Usernames/passwords 用戶名和密碼

1. Security Threats

安全威脅

Spoofing, Pharming, and Spam (Junk) Websites

電子欺騙、網址嫁接和垃圾網站

- Spoofing 電子欺騙
  - Attempting to hide true identity by using someone else's e-mail or I P (Internet Protocol) address

    指通過使用別人的電子郵件或IP地址企圖隱藏自己的真實身份
- Pharming 網址嫁接
  - Automatically redirecting a web link to a different address, to benefit the hacker

    自動將網絡鏈接鏈接重定向到其他地址，使黑客受益
- Spam (junk) websites 垃圾網站
  - Offer collection of advertisements for other sites, which may contain malicious code

    爲可能包含惡意代碼的其他網站提供廣告集合

1. Security Threats

安全威脅

Spoofing, Pharming, and Spam (Junk) Websites

電子欺騙、網址嫁接和垃圾網站

- Spoofing 電子欺騙
  - Spoofing involves attempting to hide a true identity by using someone else's e-mail or IP address. For instance, a spoofed e-mail will have a forged sender e-mail address designed to mislead the receiver about who sent the e-mail. IP spoofing involves the creation of TCP/IP packets that use someone else's source IP address to give the impression that the packets are coming from a trusted host. Most current routers and firewalls can offer protection against IP spoofing.

    電子欺騙包括嘗試通過使用他人的電子郵件或IP地址來隱藏真實身份. 例如，僞造的電子郵件具有僞造的發送者電子郵件地址，該地址旨在誤導接收者對於電子郵件發送者的判斷. IP電子欺騙涉及創建和使用其他人的源IP地址的TCP/IP數據包，這些數據包來自受信任的主機. 當前大多數路由器和防火墻都可以提供針對 IP電子欺騙的保護.

1. Security Threats

安全威脅

Spoofing, Pharming, and Spam (Junk) Websites

電子欺騙、網址嫁接和垃圾網站

- Pharming 網址嫁接
  - Spoofing a website sometimes involves pharming, automatically redirecting a web link to an address different from the intended one, with the site masquerading as the intended destination. Links that are designed to lead to one site can be reset to send users to a totally unrelated site—one that benefits the hacker.

    網站欺騙有時也被稱爲網址嫁接，即通過把網站僞裝成目標地址，把網站鏈接重定向到與預期地址不同的地址. 這種用來重定向到某一網站的鏈接設計可以通過重置，將用戶定向到一個完全不相關的站點，使黑客從中受益.

1. Security Threats

安全威脅

Spoofing, Pharming, and Spam (Junk) Websites

電子欺騙、網址嫁接和垃圾網站

- Although spoofing and pharming do not directly damage files or network servers, they threaten the integrity of a site. For example, if hackers redirect customers to a fake website that looks almost exactly like the true site, they can then collect and process orders, effectively stealing business from the true site. Or if the intent is to disrupt rather than steal, hackers can alter orders—inflating them or changing the products ordered— and then send them on to the true site for processing and delivery. Customers become dissatisfied with the improper order shipment, and the company may have huge inventory fluctuations that impact its operations. In addition to threatening integrity, spoofing also threatens authenticity by making it difficult to discern the true sender of a message. Clever hackers can make it almost impossible to distinguish between a true and a fake identity or web address.

雖然電子欺騙和網址嫁接不直接破壞文件或網絡服務器，但他們會威脅網站的完整性. 例如，如果黑客將客戶重定向到看起來與真實網站幾乎完全相同的假網站，則他們可以收集和處理訂單，從而從真實網站那裏搶走業務. 或者，如果其目的是破壞而不是竊取，則黑客可以更改訂單(如增加訂單數量或更改訂購的產品)，然後將其發送到真實的站點進行處理和交付. 這樣消費者就會對錯誤的訂單發貨感到不滿意，而商家的庫存波動可能會影響其正常運營. 除了威脅網站的完整性之外，電子欺騙還會通過讓人難以辨別消息的真實發件人來威脅真實性. 聰明的黑客能够做到讓人幾乎無法辨別發件人的身份和網址的真僞.

1. Security Threats

安全威脅

Spoofing, Pharming, and Spam (Junk) Websites

電子欺騙、網址嫁接和垃圾網站

- Spam (junk) websites 垃圾網站
  - Spam (junk) websites (also sometimes referred to as link farms) are a little different. These are sites that promise to offer some product or service but, in fact, are just a collection of advertisements for other sites, some of which contain malicious code. For instance, you may search for "[name of town] weather" and then click on a link that promises the local weather, but then you discover that all the site does is display ads for weather-related products or other websites. Junk or spam websites typically appear on search results pages and do not involve e-mail. These sites sometimes cloak their identities by using domain names similar to legitimate firm names and redirect traffic to known spammer-redirection domains.

    垃圾網站（有時也稱爲鏈接工廠）略有不同. 這些網站承諾提供某些產品或服務，但實際上只是其他網站廣告的集合，其中一些網站包含惡意代碼. 例如，你可以搜索"[鎮名]天氣"，然後單擊一個看似提供了這一信息的鏈接，但隨後發現該站點所呈現的只是與天氣相關的產品或其他網站的展示廣告. 垃圾網站通常會出現在搜索結果中，並不涉及電子郵件. 這些網站有時通過使用類似於合法公司的域名來掩飾其身份，並引入流量..

1. Security Threats

安全威脅

Sniffing and Man-In-The-Middle Attacks

網絡竊聽和中間人攻擊

- Sniffer 網絡竊聽器
  - A type of eavesdropping program that monitors information traveling over a network

    一種竊聽程序，用於監視通過網絡傳輸的信息
  - When used legitimately, sniffers can help identify potential network troublespots

    合法使用時，網絡竊聽器可以幫助識別潛在的網絡故障點
  - When used for criminal purposes, sniffers can be damaging and very difficult to detect.

    當用於犯罪目的時，網絡竊聽器可能具有破壞性並且很難被發現
  - Can be used by criminals to steal proprietary information

    可被犯罪分子用來竊取專有信息

1. Security Threats

安全威脅

Sniffing and Man-In-The-Middle Attacks

網絡竊聽和中間人攻擊

- Sniffer 網絡竊聽器
  - A type of eavesdropping program that monitors information traveling over a network

    一種竊聽程序，用於監視通過網絡傳輸的信息
  - When used legitimately, sniffers can help identify potential network troublespots

    合法使用時，網絡竊聽器可以幫助識別潛在的網絡故障點
  - When used for criminal purposes, sniffers can be damaging and very difficult to detect.

    當用於犯罪目的時，網絡竊聽器可能具有破壞性並且很難被發現
  - Can be used by criminals to steal proprietary information, including passwords, e-mail messages, company files, and confidential reports, from anywhere on a network

    可被犯罪分子用來竊取專有信息，包括密碼、電子郵件、公司文件和機密報告.

1. Security Threats

安全威脅

Sniffing and Man-In-The-Middle Attacks

網絡竊聽和中間人攻擊

- E-mail wiretaps 電子郵件竊聽
  - E-mail wiretaps are a variation on the sniffing threat. An e-mail wiretap is a method for recording or journaling e-mail traffic generally at the mail server level from any individual.
    電子郵件竊聽是網絡竊聽器的一個變體. 電子郵件竊聽是一種通常在郵件服務器層記錄來自任何個人的電子郵件通信的方法.

- Man-in-the-middle attack 中間人攻擊
  - Attacker intercepts and changes communication between two parties who believe they are communicating directly
    攻擊者截獲並更改雙方之間的通信，而這兩方認爲他們在直接通信

1. Security Threats

安全威脅

Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

拒絕服務攻擊和分布式拒絕服務攻擊

- Denial of service (DoS) attack 拒絕服務攻擊
  - Flooding website with pings and page requests

    發送無用的通信來淹沒網絡
  - Overwhelm and can shut down site's web servers

    拒絕服務攻擊可以造成網絡關閉
  - Often accompanied by blackmail attempts

    拒絕服務攻擊通常都伴隨著敲詐
  - Increasingly, DoS attacks involve the use of bot networks and so-called "distributed attacks" built from thousands of compromised client computers

    拒絕服務攻擊越來越多地涉及使用僵尸網絡和由數千台受感染的客戶端計算機構建的所謂"分布式攻擊"

1. Security Threats

安全威脅

Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks

拒絕服務攻擊和分布式拒絕服務攻擊

- Distributed Denial of Service (DDoS) attack 分布式拒絕服務攻擊
  - Uses hundreds or thousands of computers to attack target network

    使用數百甚至上千台計算機從不同的節點攻擊目標網絡
  - Can use devices from Internet of Things, mobile devices

    可以使用物聯網設備、移動設備
  - DoS and DDoS attacks are threats to a system's operation because they can shut it down indefinitely

    DoS 和 DDoS 攻擊都會對系統運行的造成威脅，因爲它們可以無限期地關閉系統

1. Security Threats

安全威脅

Insider Attacks 內部攻擊

- Largest threat to business institutions come from insider embezzlement

  商業機構面臨的最大威脅來自內部人貪盜用.

- Employees have access to privileged information, and, in the presence of sloppy internal security procedures, they are often able to roam throughout an organization's systems without leaving a trace.

  員工有機會獲得機密信息，並且由於內部安全程序的漏洞，他們往往能够訪問整個組織系統而不留痕迹.

- In some instances, the insider might not have criminal intent but inadvertently exposes data that can then be exploited by others. Companies must be equally concerned about accidental/unintentional data breaches resulting from user carelessness as they are about data breaches resulting from malicious insiders

  在某些情况下，內部人員可能沒有犯罪意圖，但無意間公開了可供他人利用的數據. 公司必須同樣關注因員工粗心大意而造成的偶然或無意的數據泄露

1. Security Threats

安全威脅

Poorly Designed Software 設計不當的軟件

- Many security threats prey on poorly designed software, sometimes in the operating system and sometimes in the application software, including browsers. The increase in complexity and size of software programs, coupled with demands for timely delivery to markets, has contributed to an increase in software flaws or vulnerabilities that hackers can exploit.

  許多安全問題源自設計不當的軟件，有時是操作系統設計不當，有時是應用程序(包括瀏覽器)設計不當. 軟件的複雜性、規模的持續擴大以及對及時交付的市場要求，導致黑客可以利用的軟件缺陷或漏洞也逐漸增多.

1. Security Threats

安全威脅

Poorly Designed Software 設計不當的軟件

- **SQL injection (SQLi) attacks** take advantage of vulnerabilities in poorly coded web application software that fails to properly validate or filter data entered by a user on a web page to introduce malicious program code into a company's systems and networks. An attacker can use this input validation error to send a rogue SQL query to the underlying database to access the database, plant malicious code, or access other systems on the network. Large web applications have hundreds of places for inputting user data, each of which creates an opportunity for an SQLi attack. A large number of web-facing applications are believed to have SQLi vulnerabilities, and tools are available for hackers to check web applications for these vulnerabilities

SOL注入攻擊利用了編碼不良的網絡應用程序中的漏洞，這些漏洞無法正確驗證或過濾用戶在網頁上輸入的數據，從而將惡意程序代碼引入公司的系統和網絡. 攻擊者可以使用此輸入驗證錯誤將惡意SQL查詢發送到基礎數據庫，以訪問數據庫並植入惡意代碼或訪問網絡上的其他系統. 大型網絡應用程序具有數百個用於輸入用戶數據的位置，每個位置都爲SQL注入攻擊創造了機會. 人們相信大量面向網絡的應用程序都有SQL注入漏洞，並且黑客可以使用工具來檢查網絡應用程序是否存在這些漏洞.

1. Security Threats

安全威脅

Poorly Designed Software 設計不當的軟件

- Zero-day vulnerability is one that has been previously unreported and for which no patch yet exists.

  零日漏洞是以前沒有發下且目前還未開發出補丁的漏洞.

- Heartbleed bug: The vulnerability allowed hackers to decrypt an SSL (Secure Sockets Layer) session and discover user names, passwords, and other user data.

  Heartbleed漏洞：該漏洞允許黑客解密安全套接層會話並發現用戶名、密碼和其他用戶數據.

1. Security Threats

安全威脅

Social Network Security Issues

社交網絡安全問題

- Social networks like TikTok, Instagram, LinkedIn, and Pinterest provide a rich and rewarding environment for hackers. Viruses, site takeovers, identity fraud, malware-loaded apps, click hijacking, phishing, and spam are all found on social networks.
  TikTok、Instagram、領英、和Pinterest等社交網絡爲黑客提供了豐富而有回報的環境. 社交網絡上出現了病毒、網站接管、身份欺詐、惡意代碼加載的應用程序點擊劫持、網絡釣魚和垃圾郵件.
- Common types of scams on social networks include manual sharing scams, in which victims unwittingly share videos, stories, and pictures that include links to malicious sites, and fake offerings that invite victims to join a fake event or group with incentives such as free gift cards and that require users to share their information with the attacker. Other techniques include fake Reactions buttons that, when clicked, install malware and post updates to the user's Newsfeed (further spreading the attack), and fake apps. By sneaking in among our friends, hackers can masquerade as friends and dupe users into scams.
  社交網絡上的常見騙局類型包括手動共享騙局，受害者在不經意間共享視頻、故事和圖片，這些視頻、故事和圖片包括指向惡意網站的鏈接以及虛假產品，以誘使受害者參加一些虛假的活動或團體，如提供免費禮品卡，要求用戶向攻擊者共享他的信息. 其他技術包括僞造的響應按鈕（單擊該按鈕會安裝惡意代碼並將更新發布到用戶的動態消息中，進一步傳播攻擊）以及虛假的應用程序. 通過潛入我們的社交網絡，黑客可以僞裝成朋友，並對用戶實施欺詐.

1. Security Threats

安全威脅

Social Network Security Issues

社交網絡安全問題

- *Social network firms have thus far been relatively poor policers because they have failed to aggressively weed out accounts that send visitors to malware sites. Social networks are open: Anyone, even criminals, can set up an account. Most attacks are social engineering attacks that tempt visitors to click on links that seem authentic. Social apps downloaded from either the social network or an external website are not certified by the social network to be clean of malware. It's "clicker beware.".*

  到目前爲止，社交網絡的安全保護相對薄弱，因爲它們沒有積極清除將訪問者送到惡意代碼網站的賬戶. 社交網絡是開放的:任何人都可以創建個人頁面，甚至犯罪分子也可以. 大多數攻擊是社交工程攻擊，誘使訪問者點擊看起來合理的鏈接. 從社交網絡或外國網站下載的社交應用程序沒有經過認證，也缺乏"點擊者要小心"的提示.

1. Security Threats

安全威脅

Mobile Platform Security Issues

移動平台的安全

- The explosion in mobile devices has broadened opportunities for hackers. Mobile users are filling their devices with personal and financial information, and using them to conduct an increasing number of transactions, from retail purchases to mobile banking, making them excellent targets for hackers. In general, mobile devices face all the same risks as any Internet device as well as some new risks associated with wireless network security. For instance, public Wi-Fi networks that are not secured are very susceptible to hacking. A flaw in an older version (WPA2) of the Wi-Fi security protocol allowed hackers to intercept passwords, e-mails, and other traffic on Wi-Fi networks.

  移動設備的爆炸式增長爲黑客提供了更多機會. 移動用戶可以在手機中存儲個人和財務信息，並使用它們進行越來越多的交易，從零售購買到移動銀行，這成爲黑客的絕佳目標. 通常，移動設備面臨與聯網設備相同的風險，以及與無綫網絡安全性相關的一些新風險. 例如，不受保護的公共 Wi-Fi非常容易遭到黑客攻擊. 較舊版本的 Wi-Fi安全協議(WPA2)中的一個漏洞使黑客能够在 Wi-Fi上攔截密碼、電子郵件和其他通信.

1. Security Threats

安全威脅

Mobile Platform Security Issues

移動平台的安全

- There are many mobile malicious installation packages, mobile banking Trojans, and mobile ransomware Trojans. Madware—innocent-looking apps that contain adware that launches pop-up ads and text messages on your mobile device—accounts for the largest share of detected threats. The majority of mobile malware still targets Android devices, which are much more likely to be infected with malware compared to iOS devices. This is due in part to the fact that Android users can download apps from third-party stores that are poorly regulated, whereas Apple users are confined to the more tightly controlled App Store.

  移動惡意安裝包、移動銀行木馬程序以及移動勒索軟件木馬. 其中，廣告軟件——即那些看似無害但包含廣告軟件的應用程序，會在您的移動設備上彈出廣告和發送短信——占據了檢測到的威脅中的最大比例. 大多數移動惡意軟件仍然針對 Android 設備，與 iOS 設備相比，Android 設備更容易感染惡意軟件. 這在一定程度上是由於 Android 用戶可以從監管較松的第三方商店下載應用程序，而Apple用戶則僅限於管控更爲嚴格的App Store.

1. Security Threats

安全威脅

Mobile Platform Security Issues

移動平台的安全

- Beyond the threat of rogue apps, smartphones of all types are susceptible to **browser-based malware**, often received via unsafe wireless networks. In addition, attackers have also developed methods of hijacking phones using weaknesses in SIM cards. The defects allow hackers to obtain the encryption key that guards users' personal information, granting hackers nearly complete access over the phone in the process.

  除了恶意應用程序的威脅外，各類智能手機都容易受到**基於瀏覽器的恶意軟件**攻擊，這些恶意軟件通常通過不安全的無綫網絡傳播. 此外，攻擊者還開發了利用SIM卡漏洞劫持手機的方法. 這些缺陷使黑客能够獲取保護用戶個人信息的加密密鑰，從而在此過程中幾乎完全訪問手機.

1. Security Threats

安全威脅

Mobile Platform Security Issues

移動平台的安全

- Vishing refers to fraudulent phone calls or voice messages designed to trick victims into providing sensitive information, like passwords or bank details. In vishing scams, attackers pretend to be from reputable organizations (such as the victim's bank, the IRS, or a package delivery service) and make unexpected phone calls. They might use toll-free numbers or use voice over Internet protocol (VoIP) technology to appear as trusted organizations.

  網絡釣魚是指是指欺詐性電話或語音消息，旨在誘騙受害者提供敏感信息，如密碼或銀行詳細信息. 在語音網絡釣魚詐騙中，攻擊者假裝來自信譽良好的組織（例如受害者的銀行、國稅局或包裹遞送服務）並撥打意外電話. 他們可能會使用免費電話號碼或使用互聯網協議語音技術冒充受信任的組織.

1. Security Threats

安全威脅

Mobile Platform Security Issues

移動平台的安全

- **Smishing attacks** exploit SMS/text messages. Compromised text messages can contain e-mail and website addresses that can lead the innocent user to a malware site. Smishing attacks are effective because users have become conditioned to quickly open and read SMS/text messages, and many tend to be less suspicious of texts than they are of e-mail. In addition, smishing attacks are inexpensive to develop and deploy. Criminal SMS spoofing services have emerged, which conceal the cybercriminal's true phone number by replacing it with a false alpha-numeric name. SMS spoofing can also be used by cybercriminals to lure mobile users to a malicious website by sending a text that appears in the From field to be from a legitimate organization and suggesting the receiver click on what is actually a malicious URL hyperlink to update an account or obtain a gift card.

短信釣魚攻擊利用短信/文本消息. 被篡改的短信可能包含電子郵件和網站地址，誘使用戶訪問惡意軟件站點. 短信釣魚攻擊之所以有效，是因爲用戶已經習慣於快速打開和閱讀短信，而且許多人對短信的警惕性往往低於電子郵件. 此外，短信釣魚攻擊的開發成本低且易於實施. 一些非法的短信僞造服務已經出現，這些服務通過用虛假的字母數字名稱替換網絡犯罪者的真實電話號碼來隱藏其身份. 網絡犯罪分子還可以利用短信僞造技術，通過發送一條顯示爲來自合法組織的短信，引誘移動用戶點擊實際上是惡意URL的鏈接，以更新賬戶或領取禮品卡.

1. Security Threats

安全威脅

Cloud Security Issues 雲安全問題

- The move of so many Internet services into the cloud also raises security risks. From an infrastructure standpoint, DDoS attacks threaten the availability of cloud services on which more and more companies are relying. Companies that have hybrid networks, with their applications scattered among public clouds, private clouds, and on-premises systems, are most at risk.

  將如此多的互聯網服務遷移到雲中也增加了安全風險. 從基礎架構的角度來看DDoS攻擊威脅著越來越多的公司所依賴的雲服務的可用性. 擁有混合網絡的公司面臨的風險最大, 其應用程序分散在公共雲、私有雲和本地系統中.

- Lack of encryption and strong security procedures.

  缺乏加密和强大的安全程序.

1. Security Threats

安全威脅

Internet of Things Security Issues 物聯網安全問題

- IoT involves the use of the Internet to connect a wide variety of sensors, devices, and machines and is powering the development of a multitude of smart connected things, such as home electronics (smart TVs, thermostats, home security systems, and more), connected cars, medical devices, and industrial equipment that supports manufacturing, energy, transportation, and other industrial sectors. IoT raises a host of security issues that are in some ways similar to existing security issues but are even more challenging, given the need to deal with a wider range of devices that operate in a less controlled, global environment and that have an expanded range of attack. In a world of connected things, the devices, the data produced and used by the devices, and the systems and applications supported by those devices can all potentially be attacked.

物聯網涉及使用互聯網連接各種傳感器、設備和機器，並推動了衆多智能互聯設備的發展，例如家用電子產品（智能電視、恒溫器、家庭安全系統等）、聯網汽車、醫療設備以及支持製造、能源、交通和其他工業領域的工業設備.物聯網引發了一系列安全問題，這些問題在某些方面與現有的安全問題類似，但由於需要應對在控制較少、全球化的環境中運行的更廣泛設備，並且攻擊面更大，因此更具挑戰性.在一個互聯設備的世界中，設備本身、設備產生和使用的數據，以及這些設備支持的系統和應用程序，都有可能成爲攻擊目標.

1. Security Threats

安全威脅

Internet of Things Security Issues 物聯網安全問題

INTERNET OF THINGS SECURITY CHALLENGES

CHALLENGE	POSSIBLE IMPLICATIONS
Many IoT devices, such as sensors, are intended to be deployed on a much greater scale than are traditional Internet-connected devices, creating a vast quantity of interconnected links that can be exploited.	Existing tools, methods, and strategies need to be developed to deal with this unprecedented scale.
Many instances of IoT consist of collections of identical devices that all have the same characteristics.	Magnifies the potential impact of a security vulnerability.
Many IoT devices are anticipated to have a much longer service life than typical equipment has.	Devices may "outlive" the manufacturer, leaving them without long-term support, which creates persistent vulnerabilities.
Many IoT devices are intentionally designed without the ability to be upgraded or the upgrade process is difficult.	Raises the possibility that vulnerable devices cannot or will not be fixed, leaving them perpetually vulnerable.
Many IoT devices do not provide the user with visibility into the workings of the device or into the data being produced, and do not alert the user when a security problem arises.	Users may believe an IoT device is functioning as intended when, in fact, it may be performing in a malicious manner.
Some IoT devices, such as sensors, are unobtrusively embedded in the environment such that a user may not even be aware of the device.	Security breaches might persist for a long time before being noticed.

1. Security Threats

安全威脅

Metaverse Security Issues 元宇宙安全問題

- Malware is also likely to be targeted at the 3-D virtual reality environment known as the metaverse as the metaverse develops further. The hardware needed for virtual reality and augmented reality platforms will create new endpoints that hackers will seek to exploit. Attackers could potentially manipulate platforms to create physical dangers. Participants in the metaverse may also be subject to various forms of harassment by malicious actors. Identities can be stolen, as can digital currencies that are used to pay for goods and services. All of the security issues currently being experienced with today's Internet are likely to continue to persist in the metaverse. The privacy of participants and the security of their personal information are also concerns. These issues are particularly acute because metaverse companies may track and retain user biometric data, as well as data about users' actual actions, and ultimately may be able to learn how users uniquely think and act.

隨著元宇宙的發展，惡意軟件也可能將目標對準被稱爲元宇宙的3D虛擬現實環境. 虛擬現實和增强現實平台所需的硬件將創造新的終端，黑客將試圖利用這些終端進行攻擊. 攻擊者可能會操縱平台，製造物理危險. 元宇宙的參與者也可能面臨惡意行爲者的各種形式的打擾. 身份可能被盜，用於支付商品和服務的數字貨幣也可能被盜. 當前互聯網所面臨的所有安全問題很可能在元宇宙中繼續存在. 參與者的隱私及其個人信息的安全也是令人擔憂的問題. 這些問題尤其嚴重，因爲元宇宙公司可能會跟踪和保留用戶的生物識別數據，以及用戶實際行爲的數據，並最終可能能够瞭解用戶獨特思維和行爲方式.

Exercise (Part I)

1) Confidentiality is sometimes confused with:
A) privacy
B) authenticity
C) integrity
D) nonrepudiation

2) _____ refers to the ability to ensure that e-commerce participants do not deny their online actions.

3) _____ refers to the ability to identify the person or entity with whom you are dealing on the Internet.

Exercise (Part I)

4) _____ refers to the ability to ensure that an e-commerce site continues to function as intended.

5) _____ refers to the ability to ensure that messages and data are only available to those authorized to view them.

6) Which of the following has the Internet Advertising Bureau urged advertisers to abandon?
A) HTML
B) HTML5
C) Adobe Flash
D) Adobe Acrobat

Exercise (Part I)

7) Accessing data without authorization on Dropbox is an example of which of the following?
A) social network security issue
B) cloud security issue
C) mobile platform security issue
D) sniffing

8) Which of the following is the leading cause of data breaches?
A) theft of a computer
B) accidental disclosures
C) hackers
D) DDoS attacks

9) Software that is used to obtain private user information such as a user's keystrokes or copies of e-mail is referred to as:
A) spyware
B) backdoor
C) browser parasite
D) adware

Exercise (Part I)

10) Malware that comes with a downloaded file requested by a user is called a:
A) Trojan horse
B) backdoor
C) drive-by download
D) exploit

11) _____ typically attack governments, organizations, and sometimes individuals for political purposes.
A) Crackers
B) White hats
C) Grey hats
D) Hacktivists

12) Which of the following statements is *not* true?
A) Typically, the more security measures added to an e-commerce site, the slower and more difficult it becomes to use
B) A worm does not need to be activated by a user for it to replicate itself
C) A Trojan horse appears to be benign, but then does something other than expected
D) Spoofing a website is not a threat to the integrity of the website

Exercise (Part I)

13) Which of the following is *not* an example of a PUP?
A) adware
B) browser parasite
C) drive-by download
D) spyware

14) Automatically redirecting a web link to a different address is an example of:
A) sniffing
B) social engineering
C) pharming
D) DDoS attack

15) Which of the following statements is *not* true?
A) Exploit kits are often rented or sold as a commercial product
B) Vishing attacks exploit SMS messages
C) Factoring Attack on RSA-Export Keys (FREAK) is an example of a software vulnerability
D) A sniffer is a type of eavesdropping program that monitors information traveling over a network

Exercise (Part I)

16) _____ is *not* an example of malicious code.
A) Scareware
B) A Trojan horse
C) A bot
D) A sniffer

17) Which dimension(s) of security is spoofing a threat to?
A) integrity
B) availability
C) integrity and authenticity
D) availability and integrity

18) Bitcoins are an example of:
A) digital cash
B) virtual currency
C) a stored value payment system
D) an EBPP system

Exercise (Part I)

19) Which of the following is an example of an online privacy violation?
A) Your e-mail being read by a hacker
B) Your online purchasing history being sold to other merchants without your consent
C) Your computer being used as part of a botnet
D) Your e-mail being altered by a hacker

20) Which of the following is an example of an integrity violation of e-commerce security?
A) A website is not actually operated by the entity the customer believes it to be
B) A merchant uses customer information in a manner not intended by the customer
C) A customer denies that he or she is the person who placed the order
D) An unauthorized person intercepts an online communication and changes its contents

21) Which of the following statements about Denial of Service (DoS) attack is *not* true?
A) Flooding website with pings and page requests
B) Often unaccompanied by blackmail attempts
C) Overwhelm and can shut down site's web servers
D) Increasingly, DoS attacks involve the use of bot networks and so-called "distributed attacks" built from thousands of compromised client computers

What is malicious code? Provide at least 5 types of malicious code and briefly explain their meanings.