E-COMMERCE SECURITY

Tin Trinh (tintt@uit.edu.vn)

Ecommerce Department, UIT

LEARNING OBJECTIVES

1. Understand E-commerce security essentials.
2. Identify the key security threats in the e-commerce environment.
3. Describe how technology helps secure Internet communications channels and protect networks, servers, and clients.

INTRODUCTION TO E-COMMERCE SECURITY

- Definition: Security measures taken to protect E-commerce websites, users, and transactions.
- Importance: Ensuring customer trust, protecting sensitive data, and maintaining business integrity.

Figure 4.1 The E-commerce Security Environment

KEY SECURITY THREATS FOR E-COMMERCE WEBSITES

Security Threats in the E-commerce Environment

- Three key points of vulnerability in e-commerce environment:
  - Client
  - Server
  - Communications pipeline (Internet communications channels)

Figure 4.2 A Typical E-commerce Transaction

Figure 4.3 Vulnerable Points in an E-commerce Transaction

Malicious Code

- Exploits and exploit kits
- Malvertising
- Drive-by downloads
- Viruses
- Worms
- Ransomware
- Trojan horses
- Backdoors
- Bots, botnets

Potentially Unwanted Programs

- Browser parasites
  - Monitor and change user's browser
- Adware
  - Used to call pop-up ads
- Spyware
  - Tracks users keystrokes, e-mails, IMs, etc.

KEY SECURITY THREATS FOR E-COMMERCE WEBSITES

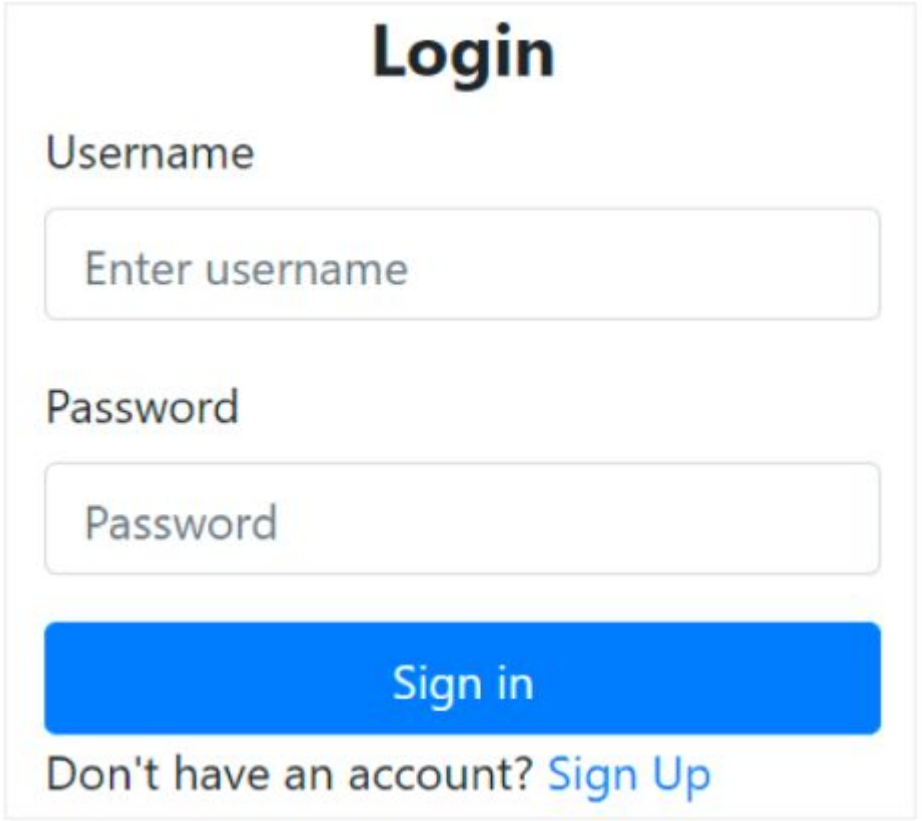
- SQL Injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Phishing Attacks
- Denial of Service (DoS) / Distributed DoS (DDoS) Attacks
- Man-in-the-Middle (MitM) Attacks
- Brute-Force Attacks

SQL INJECTION

- Definition: An attack that targets SQL databases by injecting malicious SQL statements into input fields to manipulate or access sensitive data.
- Impact: Unauthorized data access, data breaches, data modification, or even deletion.
- Prevention: Use parameterized queries, prepared statements, and input validation.

SQL INJECTION

- Sample query:
  - **SELECT * FROM users WHERE username = ' + input + ‘;**
- Retrieving data:
  - **' OR '1'=‘1’ --**
- Bypassing authentication:
  - **username = 'admin' --** (bypasses checks for username/password)
- Modifying or deleting data:
  - **'; DROP TABLE users; --**



CROSS-SITE SCRIPTING (XSS)

- Definition: An attack that injects malicious scripts into web pages viewed by other users, often targeting cookies, session tokens, or browser content.
- Impact: Data theft, hijacking user sessions, and spreading malware.
- Prevention: Use input sanitization, Content Security Policy (CSP), and proper encoding of user input.

CROSS-SITE REQUEST FORGERY (CSRF)

- Definition: An attack that tricks the user into executing unwanted actions on a web application in which they're authenticated.
- Impact: Unauthorized fund transfers, changes to user data, or manipulation of user privileges.
- Prevention: CSRF tokens, validating referrer headers, and user authentication re-confirmation.

PHISHING ATTACKS

- Definition: Deceptive emails, messages, or websites designed to steal sensitive information such as login credentials and payment details.
- Impact: Financial loss, data breaches, and user account compromise.
- Prevention: Educate users, use multi-factor authentication (MFA), and deploy anti-phishing tools.

DENIAL OF SERVICE (DOS) / DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS

- Definition: An attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.
- Impact: Website downtime, loss of revenue, and poor customer experience.
- Prevention: Use Web Application Firewalls (WAF), DDoS protection services, and rate limiting.

MAN-IN-THE-MIDDLE (MITM) ATTACKS

- Definition: An attack where the attacker secretly intercepts and potentially alters the communication between two parties.
- Impact: Data theft, including login credentials, payment data, and sensitive communications.
- Prevention: Use SSL/TLS encryption, VPNs, and secure public Wi-Fi practices.

BRUTE-FORCE ATTACKS

- Definition: An attack that attempts to gain access to user accounts by systematically trying all possible combinations of passwords.
- Impact: Unauthorized account access and data compromise.
- Prevention: Strong password policies, account lockout mechanisms, and MFA.

Social Network Security Issues

- Social networks an environment for:
  - Viruses, site takeovers, identity fraud, malware-loaded apps, click hijacking, phishing, spam
- Manual sharing scams
  - Sharing of files that link to malicious sites
- Fake offerings, fake Like buttons, and fake apps

Cloud Security Issues

- DDoS attacks
- Infrastructure scanning
- Lower-tech phishing attacks yield passwords and access
- Use of cloud storage to connect linked accounts
- Lack of encryption and strong security procedures

Internet of Things Security Issues

- Challenging environment to protect
- Vast quantity of interconnected links
- Near identical devices with long service lives
- Many devices have no upgrade features
- Little visibility into workings, data, or security

SECURING INTERNET COMMUNICATIONS AND PROTECTING NETWORKS, SERVERS, AND CLIENTS

Technology Solutions

- Protecting Internet communications
  - Encryption
- Securing channels of communication
  - SSL, TLS, VPNs, Wi-Fi
- Protecting networks
  - Firewalls, proxy servers, IDS, IPS
- Protecting servers and clients
  - OS security, anti-virus software

Figure 4.5 Tools Available to Achieve E-commerce Security

ENCRYPTION AND SECURE COMMUNICATION

- SSL/TLS Certificates: Encrypting data exchanged between the website and users.
- HTTPS Everywhere: Importance of securing all web pages.
- Data Encryption at Rest: Encrypt sensitive data in databases.

AUTHENTICATION AND ACCESS CONTROL

- Strong Password Policies: Requiring complex passwords.
- Multi-Factor Authentication (MFA): Adding an extra layer of security.
- Role-Based Access Control (RBAC): Granting the least privileges necessary.

SQL INJECTION PREVENTION

- Use of Prepared Statements and Parameterized Queries.
- Input Validation and Sanitization.
- Using Security-Oriented Frameworks and ORM Tools.
- Patching and Regular Updates.

CROSS-SITE SCRIPTING (XSS) AND CSRF PROTECTION

- Content Security Policy (CSP).
- Sanitizing User Inputs: Preventing script injections.
- Cross-Site Request Forgery (CSRF) Tokens: Adding hidden tokens for form submissions.

PAYMENT SECURITY MEASURES

- PCI-DSS Compliance: Payment Card Industry Data Security Standard.
- Tokenization: Replacing sensitive data with tokens.
- Secure Payment Gateways: Using trusted third-party payment processors.

CUSTOMER DATA PROTECTION

- Privacy Policies and Data Handling Practices.
- GDPR Compliance (General Data Protection Regulation): For customers in the EU.
- Anonymizing Data Where Possible.

REGULAR SECURITY AUDITS AND PENETRATION TESTING

- Conduct regular audits of E-commerce sites.
- Importance of vulnerability testing (internal and external).
- Working with ethical hackers for testing.

WEB APPLICATION FIREWALLS (WAFS)

- Benefits: Real-time threat protection and filtering malicious traffic.
- DDoS Mitigation Solutions.

MONITORING AND INCIDENT RESPONSE

- Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS).
- Logging and Monitoring: Tracking user activities and detecting anomalies.
- Incident Response Plan: Steps to handle a security breach.

Encryption

- Encryption
  - Transforms data into cipher text readable only by sender and receiver
  - Secures stored information and information transmission
  - Provides 4 of 6 key dimensions of e-commerce security:
    - Message integrity
    - Nonrepudiation
    - Authentication
    - Confidentiality

Symmetric Key Cryptography

- Sender and receiver use same digital key to encrypt and decrypt message
- Requires different set of keys for each transaction
- Strength of encryption: Length of binary key
- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)
- Other standards use keys with up to 2,048 bits

Figure 4.6 Public Key Cryptography: A Simple Case

Public Key Cryptography Using Digital Signatures and Hash Digests

- Sender applies a mathematical algorithm (hash function) to a message and then encrypts the message and hash result with recipient's public key
- Sender then encrypts the message and hash result with sender's private key-creating digital signature-for authenticity, nonrepudiation
- Recipient first uses sender's public key to authenticate message and then the recipient's private key to decrypt the hash result and message

Figure 4.7 Public Key Cryptography with Digital Signatures

Digital Envelopes

- Address weaknesses of:
  - Public key cryptography
    - Computationally slow, decreased transmission speed, increased processing time
  - Symmetric key cryptography
    - Insecure transmission lines
- Uses symmetric key cryptography to encrypt document
- Uses public key cryptography to encrypt and send symmetric key

Figure 4.8 Public Key Cryptography: Creating a Digital Envelope

Digital Certificates and Public Key Infrastructure (PKI)

- Digital certificate includes:
  - Name of subject/company
  - Subject's public key
  - Digital certificate serial number
  - Expiration date, issuance date
  - Digital signature of CA
- Public Key Infrastructure (PKI):
  - CAs and digital certificate procedures
  - PGP

Figure 4.9 Digital Certificates and Certification Authorities

Limitations of PKI

- Doesn’t protect storage of private key
  - PKI not effective against insiders, employees
  - Protection of private keys by individuals may be haphazard
- No guarantee that verifying computer of merchant is secure
- CAs are unregulated, self-selecting organizations

Securing Channels of Communication

- Secure Sockets Layer (SSL)/Transport Layer Security (TLS)
  - Establishes secure, negotiated client-server session
- Virtual Private Network (VPN)
  - Allows remote users to securely access internal network via the Internet
- Wireless (Wi-Fi) networks
  - WPA2
  - WPA3

Figure 4.10 Secure Negotiated Sessions Using SSL/TLS

Protecting Networks

- Firewall
  - Hardware or software that uses security policy to filter packets
    - Packet filters
    - Application gateways
  - Next-generation firewalls
- Proxy servers (proxies)
  - Software servers that handle all communications from or sent to the Internet
- Intrusion detection systems
- Intrusion prevention systems

Figure 4.11 Firewalls and Proxy Servers

Protecting Servers and Clients

- Operating system security enhancements
  - Upgrades, patches
- Anti-virus software
  - Easiest and least expensive way to prevent threats to system integrity
  - Requires daily updates

Management Policies, Business Procedures, and Public Laws

- Worldwide, companies spend more than $86 billion on security hardware, software, services
- Managing risk includes:
  - Technology
  - Effective management policies
  - Public laws and active enforcement

A Security Plan: Management Policies

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

Figure 4.12 Developing an E-commerce Security Plan

The Role of Laws and Public Policy

- Laws that give authorities tools for identifying, tracing, prosecuting cybercriminals:
  - USA Patriot Act
  - Homeland Security Act
- Private and private-public cooperation
  - US-CERT
  - CERT Coordination Center
- Government policies and controls on encryption software
  - OECD, G7/G8, Council of Europe, Wassener Arrangement

SECURITY BEST PRACTICES FOR USERS

- Educating Users: Phishing awareness, strong passwords, and secure browsing.
- Securing User Accounts: Tips for safe practices on E-commerce sites.

CASE STUDY: THE TARGET DATA BREACH 2013

- Brief overview of a notable breach (e.g., data leak).
- Lessons learned and security measures taken afterward.

EMERGING TRENDS IN E-COMMERCE SECURITY

- AI and Machine Learning for threat detection.
- Blockchain for secure transactions.
- Advances in user authentication (biometrics).

CONCLUSION

1. Understand E-commerce security essentials.
2. Identify the key security threats in the e-commerce environment.
3. Describe how technology helps secure Internet communications channels and protect networks, servers, and clients.

Q & A

The Target Data Breach (2013)

A Case Study of E-commerce Security Incident

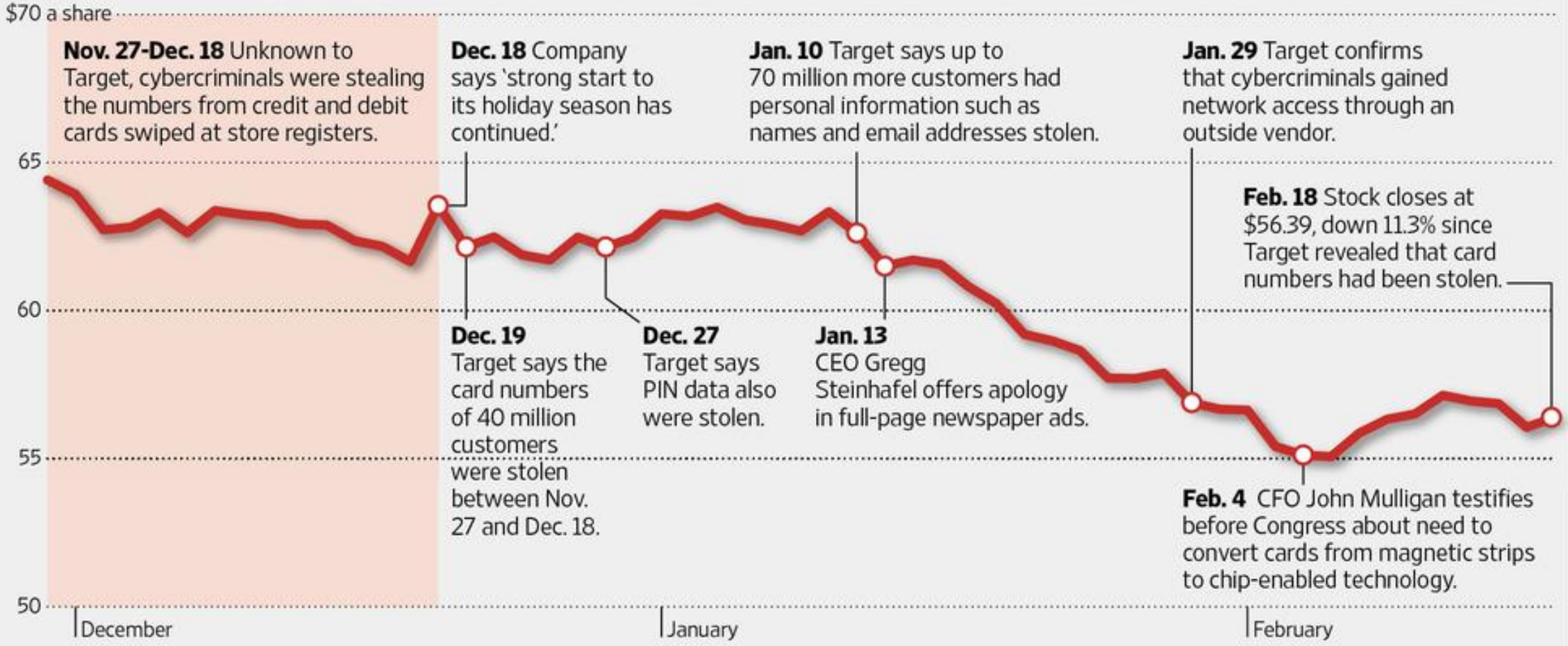
OVERVIEW OF THE INCIDENT

- Incident: Target Data Breach
- Year: 2013
- Affected Data:
  - **40 million** credit/debit card details
  - **70 million** personal records (names, addresses, phone numbers, email)
- Date Discovered: December 12, 2013
- Public Announcement: December 19, 2013

TARGET

Trying Times

Target's discovery that cybercriminals had stolen the credit and debit card numbers of about 40 million customers led to a series of difficult decisions.



Sources: WSJ Market Data Group; news reports

The Wall Street Journal

TIMELINE OF THE BREACH

- November 2013:
  - Attackers gained access through third-party vendor (Fazio Mechanical Services).
  - Malware installed on Target's point-of-sale (POS) systems.
- December 2013:
  - Attackers exfiltrated data from POS systems.
  - Target detected the breach on December 12.
  - Public notification on December 19.
- 2014:
  - Financial fallout, lawsuits, and leadership changes.

HOW THE ATTACK HAPPENED

- Step 1: Third-Party Vendor Access
  - Attackers used Fazio Mechanical Services' compromised access to Target’s internal network.
- Step 2: Malware Installation
  - Malware installed on POS systems to capture card data during transactions.
- Step 3: Data Exfiltration
  - Stolen data sent to remote servers controlled by attackers.

KEY FACTORS CONTRIBUTING TO THE BREACH

- Third-Party Vendor Vulnerability:
  - Weaknesses in vendor management allowed attackers to access sensitive systems.
- Lack of Effective Detection:
  - Security alerts ignored, breach went undetected for weeks.
- Failure to Encrypt Data:
  - Unencrypted card data made it easier for attackers to steal information.
- Delayed Response:
  - Public was not informed immediately, which extended the attack window.

IMPACT OF THE BREACH

- Financial Losses:
  - $200 million in response and recovery efforts.
- Legal Consequences:
  - Multiple lawsuits and settlements, regulatory scrutiny.
- Reputational Damage:
  - Erosion of customer trust, decline in sales during key holiday season.

Effects of the breach

TARGET

Reputational

- Lose customer trust and business

Financial

- Sales discounts that lower profit margins
- Holiday sales fall
- Reduced stock price
- Costs exceed $300M
- $116M spent in settlements

Operational

- Layoffs and hiring freeze
- CEO resigns

FOX | ITACS

LESSONS LEARNED

- Vendor Management:
  - Regular security assessments for third-party vendors.
- Detection Systems:
  - Implementing robust intrusion detection and timely response.
- Data Encryption:
  - Encrypting sensitive payment card data at all points of transaction.
- Proactive Communication:
  - Transparent and prompt communication with customers.
- Incident Response Planning:
  - Developing and testing effective incident response plans.

CONCLUSION

- Key Takeaway:
  - The Target Data Breach highlights the critical importance of securing e-commerce platforms, managing vendor relationships, and being proactive in security measures.
- Reflection for E-commerce Security:
  - Ongoing need for vigilance and continuous improvement in cybersecurity practices.