Tutorial 11

Aims

- To highlight the main issues in Internet-based banking
- Have a basic understanding of cybercrime

Questions

1. Credit cards are used in most Internet-based commerce.
   (a) You are purchasing a product on the Internet, and you pay using your credit card. Explain the participants in the transaction and the steps of the payment process.
   Participants
   - Customer: card holder
   - Issuer: Issues the bankcard, maintains the customer's account
   - Merchant: sells goods, receives payment, **does not** have access to financial information – uses a payment terminal (gateway) to communicate with the Acquirer
   - Acquirer gateway: provides payment processing services to merchant, credits the merchant's account after communicating with the issuer

   Payment process: merchant initiates the following steps
   - Authorization:
     - checks (i) credit card validity (ii) availability of sufficient funds
     - holds the funds for later capture (for an "honour period" of about 3-5 days)
   - Capture
     Transfer of funds from the customer's account to the merchant's (after delivery of goods)

   (b) How is credit card information secured in an Internet transaction? Are there any vulnerable points in a transaction?
   Encryption is securing information in transit.
   Endpoints are the main vulnerability, particularly on the merchant side (card skimming, spyware on personal computers etc). Acquirer sites are attractive targets to criminals due to the large amount of data stored and processed, and have been victims of successful attacks (e.g. transaction processing services)

   (c) Is an ATM more secure for financial transactions than a user PC?
   An ATM is a dedicated machine with one application running only, and having special peripherals to deal with the task (simplified keyboard, special display etc.)
   On the other hand, they are just PCs running Windows, mainly XP, Windows 7 was certified for it only in early 2013.

2. What is a smart card? How does it differ from an ordinary bankcard, what are the advantages and disadvantages?

Smart card: Information to be processed is stored on the card, not only authentication information.
Uses microchip: built-in memory (bankcards also use it)
Contains a security system: cryptoprocessor, secure file system etc
Uses near-field communication or contacts to microchip, not magnetic stripe
Advantage: more capable
Disadvantage: more harm if compromised

3. What are the basic flaws that early malware was exploiting?
   Buffer overflow: Buffer copy without checking size of input
   Missing authentication for critical function
   Execution with unnecessary privileges
   Injection: Improper neutralization of special elements used in an input

4. What are malware toolkits? What do they provide?
   Provide tools to run and spread malware.
   Require no expertise to run and perform malicious activities (are often rented out
   Automated
   discovery and exploitation of vulnerabilities in commonly used software. Can run its own web server (e.g. Blackhole does)
   launch of attacks (e.g. DDoS)