Distributed-Application Security
Spam

Spams

- Spam referred to unsolicited bulk email
- Spam emails contain advertisement, viruses, malware
- Spams emails are used to gather information about the victim

Harvesting email addresses:

- Spidering is a process that crawl the web and collect email addresses
Spam

• Sending Spam email include the following methods:
  • Spoofing the FROM field of the message, but the IP of the SMTP server is still included in the message header
  • Sending spam via a third party by using open relays and proxies
  • Spammer can use proxies to hide the true origin of the messages
Spams

**CAPTCHAs** (Completely Automated Public Turing test to tell Computer and Human Apart). Such a task is easily solved by a human but difficult to solved by a computer

- Spammer circumvent some of these CAPTCHAs using websites that required visitors to solve CAPTCHA to gain access
- User provided solution are then used to register a webmail account for sending spam and automate the registration process.
- **Computer infected** with malware are also used to send spam
- It is estimated that 80% of spams are generated from botnets
Electronic Payment Schemes

- Schemes for electronic payment are **multi-party protocols**
- Parties include:
  - Payer (customer)
  - Payee (merchant)
  - Bank
Transactions

• Transactions in an electronic payment scheme typically include:
  • **Withdrawal** of coins by customer from the bank
  • **Payment** of coins by customer to merchant
  • **Deposit** of coins by merchant into bank

• Online scheme:
  • The bank participates in the payment transaction

• Offline scheme
  • The bank does not participate in the payment transaction
Digital Cash

- Digital cash provide anonymity and un-traceability
- Electronic coin has several security properties:
  - **Privacy.** Coin can not be trace back to the payer
  - **Integrity.** Coin can not be forged or duplicated
  - **Accountability.** Transaction can not be denied at a later date
Payment with Digital Signatures

- Coins are random identifiers digitally signed by the bank at the time of withdrawal
- The merchant verifies the signature by the bank
- The bank honors deposit of valid coins
- Security and privacy issues:
  - Customer can copy coin and double spend
  - The bank learns about every transaction by customer and merchant
Digital cash and Blind Signatures
Social networking

Attacks vectors

• Social networking site provide many communication channels between users.
• Attackers can utilized these channel to gather information
• Social networking site are highly interactive, third party application can be executed on these sites which provide new attack vectors
• Social networking site are vulnerable to cross-site scripting attacks to distribute malware, worms, and viruses

Privacy

1. User must be given complete control over what personal information is available to what parties
2. Security and privacy configuration options must be simple and easy to execute
3. Privacy setting must be assigned to restrictive default values to protect users who are unwilling to change their own privacy preferences
Voting Systems

- Electronic voting systems is a multiparty computation system

**Security Goals for voting systems**

- Accuracy
- Availability
- Secrecy
- Verifiability
- Usability

**Casting Votes**

- The three ballot is a computational voting scheme, designed by Ron Rivets
- A voter is given three ballots, each with a unique identifier
- The voter is instructed to cast two votes for his preferred candidate and one exactly vote for the remaining candidates
Vote Tallying and Verification

Tallying
- When all ballots are collected, the ballots are posted publicly
- If a candidate receives $v$ votes and $n$ is the total number of voters.
- The above candidate receives $v + n$

Verification
- The receipt allows a voter that one of her ballots is included in the tally
- Attempts to alter a ballot has a chance of $1/3$ of being detected
- Example:
  - $m$ ballots has been modified
  - The fraction of voters that verify their receipts is $f$
  - The probability that the tempering goes undetected is

\[ (1 - f/3)^m \]