Lecture 17
Computer and Network Security

Addison-Wesley
is an imprint of
PEARSON

Participation Quiz

Which destination would you choose?

Encryption

- Method for concealing the content of a message
- Symmetric encryption:
  - Single key used to encrypt and decrypt a message
  - Problem: How does sender get key to receiver?
- Public-Key encryption (e.g., RSA):
  - Each person has two keys: public and private
  - To send ***R*** a message, encrypt it with ***R***'s public key
  - ***R*** decrypts message with ***R***'s private key
  - No need to communicate private keys
- SSL (https://...) is based on public-key encryption:
  - Upon connection, server reports its public key and a trusted certificate authority that can verify it. The client may verify the key.
  - The client encrypts a random number with the server's public key and sends the result to the server.
  - The server decrypts it with its private key.
  - From the random number, both parties generate key material for encryption and decryption.

Strong Encryption

- Strong encryption: encryption at a level that is believed not to be breakable by any other than sender/receiver
  - e.g., 256-bit AES
  - mathematical reasons to believe governments can't break it either
- Availability of strong encryption
  - Previously classified as a munition by US, regulated
  - 1991: US Senate passed a law requiring all encryption systems to include a "back door"
  - In response, Phil Zimmerman created PGP
  - Government tried to shut it down
  - 1999, 2000: courts ruled that these restrictions are illegal, encryption protects privacy and free speech
- *Questions*
  - *Should there be laws against use/distribution of strong encryption?*
  - *How should governments respond to its existence?*

Electronic Money

- Identified electronic money uses public key encryption:
  - I can verify the money came from a bank using its public key
  - The bank can verify I'm the one who took out the money
- Anonymous electronic money (digital cash):
  - No way for the bank to tell what the money was used for
  - Relies upon blind signature protocol
    - I make 100 (10,000, …) blank checks
    - You check 99 (9,999, …) of them at random
    - If they're all good, you sign the last one without seeing it
    - You have an arbitrarily high chance that the last one is good too
- *Question: As financial transactions become increasingly electronic, is it important to preserve a digital analogue to cash?*

Evil Code that can Run on Your Computer

- **Viruses**
  - What is a virus?
  - Have you ever (knowingly) gotten one?
- **Worms**
  - What is a worm? How is it different from a virus?
  - Is it wrong to distribute a virus or worm that doesn't harm anyone?
- **Trojan Horses**
  - What is a Trojan horse? How is it different from the first two?

- Do the victims of a virus/worm/Trojan horse share responsibility for being attacked if their system is not up to date?