Security and Privacy

Xin Liu
Computer Science
University of California, Davis
What is network security?

Confidentiality: only sender, intended receiver should “understand” message contents
- sender encrypts message
- receiver decrypts message

Authentication: sender, receiver want to confirm identity of each other

Message integrity: sender, receiver want to ensure message not altered (in transit, or afterwards) without detection

Access and availability: services must be accessible and available to users
Friends and enemies: Alice, Bob, Trudy

- well-known in network security world
- Bob, Alice (lovers!) want to communicate “securely”
- Trudy (intruder) may intercept, delete, add messages
Who might Bob, Alice be?

• ... well, *real-life* Bobs and Alices!
• Web browser/server for electronic transactions (e.g., on-line purchases)
• on-line banking client/server
• DNS servers
• routers exchanging routing table updates
• other examples?
There are bad guys (and girls) out there!

**Q:** What can a “bad guy” do?

**A:** a lot!

- *eavesdrop:* intercept messages
- actively *insert* messages into connection
- *impersonation:* can fake (spoof) source address in packet (or any field in packet)
- *hijacking:* “take over” ongoing connection by removing sender or receiver, inserting himself in place
- *denial of service:* prevent service from being used by others (e.g., by overloading resources)
A few security tools

- Crypto
  - Public key structure
  - Symmetric key structure
  - Certificate authentication
- Firewall
- WLAN security
A certificate contains:

- Serial number (unique to issuer)
- info about certificate owner, including algorithm and key value itself (not shown)

[Image showing a certificate with detailed information]

- info about certificate issuer
- valid dates
- digital signature by issuer
Phishing

• an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication (definition from wikipedia)

• Defense:
  – Social response
  – Technical response: filtering, identify legitimate site, browser alert, augment password
Spamming

- indiscriminately send unsolicited bulk messages
- Email, phone, IM, cellular phone, etc.
- How do spammers gather the addresses?
- Anti-spam
  - Bayesian filter, white list, black list, collective filtering, keyword filtering
Computer Virus

• a computer program that can copy and propagate itself without permission or knowledge of the computer user

• How does computer virus spread:
  – Attachment
  – Exploring bugs in existing software systems
  – Active content code: HTML virus

• Counter measure:
  – Antivirus software,
  – Software update
  – Be conscious
Spyware

• A software that intercepts or takes partial control over the user's interaction with the computer, without the user's informed consent.

• Adware

• Where does it come from?
  – Piggybacking,
  – trick users to install
  – Security hole

• Counter measure
  – Anti-spyware software
  – Be conscious
Practical issues

- http vs. https
- Open WiFi networks (and automatic connection)
- Multi factor authentication
- Change password on your home router
- Using the same password on multiple accounts
- Password vs. passphrase
  - John081595, asdf1234 (how is this password?)
  - Change the last digit of password
  - Dictionary attack and big data

- Bottom line: convenience vs. security
Practical Tips

- [http://software.ucdavis.edu](http://software.ucdavis.edu)
- Click on Antivirus software
- Sophos
- 360 Security (PC and Android)
- Cleanmaster for mobile devices
Practice tips

• Security patches
  – OS, Office, Adobe, etc.
• Password management
  – Is it safe to let the browser save passwords for you?
  – Good password/passphrase
• Email
  – Never ever send your SSN/login/password and other sensitive information through email
  – Be cautious when you open attachment, even from people you know
  – Use other online tools to open attachment for you (e.g., google)
• Warnings about websites that may cause harm to your computer
• Close the browser after sensitive transactions
• BE CAUTIOUS: security is as strong as the weakest link
• Anything else you can think of?
Privacy

• Hard to define, easy to identify
• Bits on the Internet NEVER EVER disappear
  — Even if you delete it.
• Privacy on social networks
• What do they know about us?
  — they: Facebook, Google, Yahoo, Amazon, etc.
• It is fairly common for potential employers or dates to check out a candidate on Facebook, Linkedin, etc.