Lecture 9: Security and Privacy

Privacy

- **Privacy**: The right of people to choose freely under what circumstances and to what extent they will reveal themselves, their attitude, and their behavior to others.
- Two basic threats to privacy: government and business organizations.
- Should government have access to certain types of information?
  - Privacy vs. safety (counter-terrorism)
- Business access to information: good or bad?
  - Targeted advertisements
- US has pretty weak privacy regulation

How could the information be used?

- When a store obtains the customer's personal information during a transaction, there are four main possibilities:
  1. **No uses**. The information out to be deleted when the store is finished with it (for example, when a check has cleared the bank), because there can be no further use of it.
  2. **Approval**. The store can use it for other purposes, but only if you approve the use.
  3. **Objection**. The store can use it for other purposes, but not if your object to a use.
  4. **No limits**. The information can be used any way the store chooses.
- If the transaction took place in Europe, New Zealand, Australia, Canada, Hong Kong, and etc., the law and standards would place it between (1) and (2).
- If the transaction took place in United States, the law and standards are in between (3) and (4).

Cookies

- Cookies are small text files, stored on your computer by a server.
- Cookies are used to maintain information across multiple page requests to the server. E.g. to maintain the contents of your shopping cart, when go backward and forward different catalog pages.

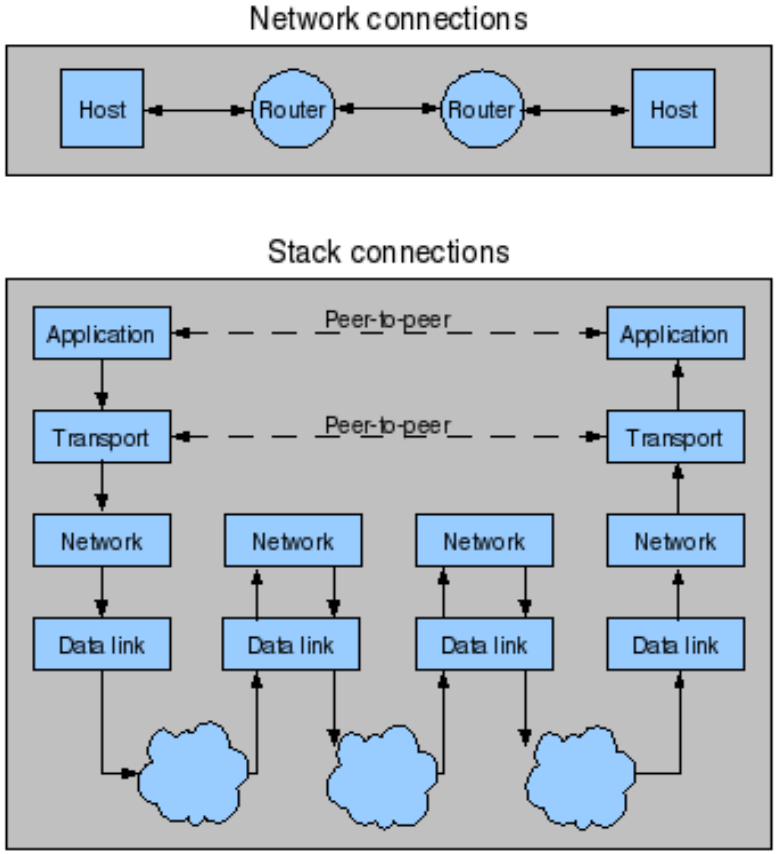
Problem with cookies

- Third-party cookies
  - A web site may contract with an ad agency to place ads on its page.
  - When you visit the server, it sends a request to the ad agency to display an ad, but then it is suddenly allowing that ad company to place cookie on your computer, without your realizing it.
  - If you later visit a different web server that contracts with the same ad agency, it will be able to retrieve those cookies and the ad agency will now know which other companies you interacted with.
- You can change the browser settings to deny cookies, or to warn you when cookies are being stored. The cost is that some good web pages which requires cookies won't work for you.

E-Commerce – Secure Tansactions

- Information sent over the Internet can be intercepted by a third party, so, for example, credit car numbers might be collected. To keep information secure, it must be **encrypted**.
- **SSL** – Secure socket layer protocol for secure transactions. The communication between the browser and the web server is **encrypted**. Web pages using this protocol are accessed using **https**.
- SSL uses certificates to verify that a web server is really what it claims to be.
- Email is not secure. PGP can be used to encrypt email messages.

TCP/IP protocols



- Data link layer – e.g. Ethernet
- Network layer – e.g . IP packet exchanging
- Transport – e.g. TCP connections
- Application – e.g. HTTP

The Network Functions Layering

1. http_deliver(url, html_file)
   - Figure out the **IP address** and the **port number** of the receiving software
   - Call tcp_deliver with the IP address and port number, and the message is the html file

   1.5. SSL: https_deliver(url, html_file) sits between http_deliver and tcp_deliver if "https://" is used instead of "http://" in the URL.

- tcp_deliver(ip_address, port, message)
  - Break the message into packets
  - For each packet, call ip_deliber(ip_address, ip_packet)

1. ip_deliver(ip_address, ip_packet)
   - Routing through the networks by looking up the routing table
   - In each network, figure out the mac_address which corresponds to the ip_address, and assemble the ip_packet into frame_packet
   - Call Ethernet_deliver(mac_address, frame_packet)
2. Ethernet_deliver(mac_address, frame_packet)

Summary

- Privacy
- Cookies
- E-commerce – secure transactions