Lecture notes for 10.5-10.6, Freenet, & Tor

Online privacy
- Advertising cookies (doubleclick.net) track visited sites (via ads on each site)
- Spyware: Malicious software that records your computer use
- Keylogger, clicklogger
- Installed with other software (e.g. Kazaa)
- Adware displays pop-up ads (gator toolbar)
- Drive-by downloads
  - Exploit browser flaw to install
  - Obscure installation dialog popup box text to entice users to click OK
- Retailers give different price quotes to different customers based on prior history of purchases

Email privacy
- Emails sent in clear, no evidence of tamper or access
  - Very different from physical mail security
- Encryption, anonymization

Anonymization
- Recall traffic analysis (sigint)
  - Information in who-talks-to-who
- Who wants to evade traffic analysis?
  - Govt agents talking to handlers
  - Prosecutors talking to whistle-blowers
  - Parties engaging in sale of CC dumps
  - Citizens accessing web sites banned by repressive govts
- Def: removal of identifying information
  - Here, from endpoint of communication

Anonymizers
- Email: remailers
- Web: proxies (anonymouse)
  - Drawback: proxy could deanonymize
- Web: mix networks
- Web: onion routing (tor)
  - Entry & exit points know actual start or finish
  - Long enough circuit prevents correlation

- General: anonymizing overlay networks (freenet)
    - P2P plausible deniability: don't know if computer is requesting information for itself or on behalf of a peer

Proxy

- [Draw picture, one hop proxy, intentional MITM]
- Drawback: proxy knows deanonymizing information

Mixnets

- [Draw picture, internet cloud, multiple clients, multiple servers, mixnet cycles the traffic]
- Drawback: arbitrary slowdown in the mixnet
- Attack: match input flow with output flows, ignore mixnet entirely

Tor / Onion routing

- [Draw picture, client, multiple routers in the cloud, server]
- Client creates a circuit:
    - Think source routing
    - Client chooses subset of servers
    - Wraps data for server in layers of one-hop routing information (layers of the onion)
    - Each server unwraps one layer
- Attack: traffic flow correlation?
- [Tor demo]

Freenet / P2P overlay network

- [Draw p2p picture, all nodes equal]
- Censorship-resistant
    - Data replicated across nodes
    - Nodes have no information about data they are storing
- Anonymous (?)
    - Nodes know peer IPs
    - Nodes do not know if request from peer originated at that peer or if peer is forwarding request
        - Plausible deniability
- Designed to disseminate suppressed info, particularly to china & middle-east
- Attack: simply identify machines participating in the network?