Network Privacy

- Mostly issues of preserving privacy of data flowing through network
- Start with encryption
  - With good encryption, data values not readable
- So what's the problem?

Traffic Analysis Problems

- Sometimes desirable to hide that you're talking to someone else
- That can be deduced even if the data itself cannot
- How can you hide that?
  - In the Internet of today?

A Cautionary Example

- VoIP traffic is commonly encrypted
- Researchers recently showed that they could understand what was being said
  - Despite the encryption
  - Without breaking the encryption
  - Without obtaining the key

How Did They Do That?

- Lots of sophisticated data analysis based on understanding human speech
  - And how the application worked
- In essence, use size of encrypted packets and interarrival time
  - With enough analysis, got conversation about half right

Location Privacy

- Mobile devices often communicate while on the move
- Often providing information about their location
  - Perhaps detailed information
  - Maybe just hints
- This can be used to track our movements

Cellphones and Location

- Provider knows what cell tower you're using
- With some effort, can pinpoint you more accurately
- In US, law enforcement can get that information just by asking
  - Except in California

Other Electronic Communications and Location

- Easy to localize user based on hearing 802.11 wireless signals
- Many devices contain GPS nowadays
  - Often possible to get the GPS coordinates from that device
- Bugging a car with a GPS receiver not allowed without warrant
  - For now . . .

Implications of Location Privacy Problems

- Anyone with access to location data can know where we go
- Allowing government surveillance
- Or a private detective following your moves
- Or a maniac stalker figuring out where to ambush you . . .

Another Location Privacy Scenario

- Many parents like to know where their children are
- Used to be extremely difficult
- Give them a smart phone with the right app and it's trivial
- Good or bad?

A Bit of Irony

- To a large extent, Internet communications provide a lot of privacy
  - "On the Internet, no one knows you're a dog."
- But it's somewhat illusory
  - Unless you're a criminal

Why Isn't the Internet Private?

- All messages tagged with sender's IP address
- With sufficient legal authority, there are reliable mappings of IP to machine
  - ISP can do it without that authority
- Doesn't indicate who was using the machine
  - But owner is generally liable

Web Privacy

- Where we visit with our browsers reveals a lot about us
- Advertisers and other merchants really want that information
- Maybe we don't want to give it to them
  - Or to others
- But there are many technologies to allow tracking
  - Even to sites the tracker doesn't control

Do Not Track

- Wouldn't it be nice if we could ensure that web sites don't track us?
- Enter the Do Not Track standard
- A configurable option in your web browser
- Which, by enabling, you might think prevents you from being tracked

The Problems With Do Not Track

- First, it's voluntary
  - Web server is supposed to honor it
  - But will they?
- Second, and worse, it doesn't mean what you think it means
  - Based on current definitions of the option

What Do Not Track Really Means

- What it really means is “I’ll track you anyway”
- “But I won’t provide you anything helpful based on the tracking”
- So they know what you’re doing
  - And they do whatever they want with that data
- But you don’t see targeted ads
- So what’s the point of Do Not Track?
  - A good question

Privacy and the Law

- US law has long recognized a Constitutional right to privacy
  - Many of the legal decisions related to sex
  - But also areas like education choice, medical decisions, marital issues
  - Not well settled law
- Some state constitutions enumerate a right to privacy (e.g., California's)

Privacy Laws Related to Data Compromise

- Many US states have laws compelling businesses to divulge data loss
  - When such loss involves compromise of users' personal info
  - E.g., CA SB 1386
- Continuing attempts to pass a national version of this kind of law

US Medical Data Privacy Law

- In the HIPAA laws regulating health insurance
- Seeks balance between
  - privacy of medical info and
  - benefits of sharing among health care providers
- Strong limits on who can be given your medical information

European Law and Privacy

- EU Data Protection Directive provides broad privacy protections
- Specifically in the context of computer data
- Offers wide and powerful protections against privacy invasions
- Generally Europeans have particular sensitivity to privacy issues

Other Nation's Legal Stands

- Some nations (e.g., China) have limited constitutional privacy rights
- Some have derived rights, like the US (e.g., India)
- Some have non-constitutional legal frameworks (e.g., Russia)
- In many countries, what the laws say and what actually happens might differ

The Relevance of Privacy Laws

- Typically, one nation's privacy laws not necessarily honored by others
  - Exception: EU shares laws among its member nations
- Governments not always committed to enforcing them
- The fact you're supposed to keep info private can help hide compromises