Prolog to Lecture 18
CS 236
On-Line MS Program
Networks and Systems Security
Peter Reiher

Privacy vs. Surveillance

- Increasingly governments are demanding increased surveillance
  - For law enforcement
  - For national security
  - In some cases, to control citizens
- How does that affect privacy?

The Obvious Issue

- If they prevail, you get no privacy from your government
  - To the extent they push it
- At best, you hope they will "behave well"
- Many past cases of governments not behaving well

Technology Solutions

- Some tech companies are pushing extreme privacy solutions
- Effectively making it impossible for governments to compromise privacy
  - Since literally no one can
- Typically based on crypto
- Often supported by hardware
- Apple iPhone controversy, for example

Government Response?

- Require tech companies to be able to breach consumer privacy
  - At least under special circumstances
- What's the implication?
  - Companies can breach privacy, obviously
- There are implications . . .

One Implication

- The company can obtain your private data
  - Not necessarily with any kind of due process
  - They, after all, must have the ability to do so
  - And who's watching them?
- Will they behave well?
- Who will make them?

Another Implication

- If the company can breach privacy, probably others can
- Privacy breaches are likely since the company has useful secrets
- If those secrets are learned by others, those others can breach privacy
- So others will try
- Experience suggests they'll sometimes succeed

An Example

- A smart phone that encrypts all data
- How could the company breach that privacy?
- They have (or can obtain) the key to decrypt
- Where is it?
- Who else can get it?
- Can it be stolen?
- What if the company goes bankrupt?

The Technologist's Argument

- Either a system is safe from everyone
- Or it's really safe from no one
- Maybe we can build security that the manufacturers themselves can't crack
- But if they can crack it, so can someone else
- Safer to build something no one can crack

The Government's Argument

- There have never before been secrets that the government can't get
  - Except those only in people's heads
- Warrants open safes and safety deposit boxes, invalidate confidentiality agreements, etc.
- Why should computers or phones be different?
- What bad things might happen if they are?

So . . .?

- This is a major public policy debate
- In the US and Europe, currently
- Likely everywhere, eventually
- I won't tell you what to think about it
- But I suggest you do think about it
- Chances are you're more knowledgeable about the issues than 99.9% of everyone
  - Including some of those who will make the decisions