Prolog to Lecture 2
CS 236
On-Line MS Program
Networks and Systems Security
Peter Reiher

What's This Prolog Stuff?

- When I can, I will add a short presentation to each lecture
- Discussing application of material from the previous or recent lectures
- Generally stuff that's pretty timely

Do We Really Care About Security?

- Security gets a lot of lip-service
- But is the community out there really behind it?
  - Particularly the industrial community that builds our software?
- Two recent stories suggest maybe not

1. Fun With Firewire

- Many computers have firewire interfaces
  - Especially laptops
- These interfaces allow **direct** access to memory
  - No access control
  - No nuthin'

What's That Mean?

- Anyone who hooks up a firewire device to your laptop doesn't need to log in
- He can just read and alter the memory
- Proof-of-concept tool[1] allows you to own Windows machine in seconds
  - [1]http://www.darkreading.com/document.asp?doc_id=147713&f_src=drweekly

What's the Response?

- "Well, duh, that's what Firewire is supposed to do"
- In other words, we designed your computer to let anyone take it over
  - If they have physical access
- All this login stuff is just window dressing to impress the rubes

2. Backdoor Processors

- Many devices come with complete processors "hidden" inside
  - Printers, routers, storage devices, etc.
- They're installed with complete OSes
  - Often very badly configured
- Allowing anyone access
- E.g., Cisco had an undocumented test interface in wireless APs and routers (2013)
  - Allowed attacker to run anything on them

The Implications

- If attacker knows about these,
- And you don't,
- He's got a hidden backdoor into your system
- Often these processors have network capabilities
- And can access the CPU you already knew you had

What's That Mean?

- The people who put these processors in neither knew nor cared about security
- System management (the purpose of them) was more important
- They didn't care enough to even mention they were there

The General Lesson

- Just because people say they care about security doesn't mean they do
- Many decisions seem to be made without even considering security implications