Prolog to Lecture 13
CS 236
On-Line MS Program
Networks and Systems Security
Peter Reiher

Where Malware Lives

- Most people expect malware in only one place –
  - Somewhere on your hard drive
- Maybe also on flash drives, CDs, DVDs
- *Perhaps* in boot sector
- But that's it, right?

Malware and Firmware

- Proof of concept recently showed malware stored in peripherals
  - In their firmware
- Malware writes itself into their firmware
- Virus detection stuff doesn't look there
  - Nor does most cleaning code
- So it's unlikely to be found or removed

The Implications

- Anything with writable memory might harbor malware
- Need device specific scanning and analysis code
- If device has its own processing capabilities, problem is even worse
- Obviously, much harder to clean devices this way

Let's Look in Another Dimension

- Spatial
- We are moving to a world of embedded devices
- They're too small and weak to host virus detection software
- What will be the problems there?

Malware Problems of the Ubiquitous Future

- Millions of evil little nodes
  - All around us
  - Hard to detect
  - Hard to clean
- But they are limited devices
  - Can we leverage that for protection?
  - Or at least to limit the damage?

Another Example

- What if someone writes malware to live in a network device?
  - Like a printer
    - Recently, HP and Samsung had printer security problems
- Doesn't have to have large footprint in other machines
- Printer software wakes up and takes over other machines when needed
- Who's going to bother checking the printer?

Malware in Our Smart Phones

- Smart phones are essentially portable computers
- Widely deployed
- Poorly administered
- With access to useful personal data
- Criminals are very interested in them

Protecting the Ubiquitous Future

- If computers are everywhere, how can we prevent malware from being everywhere?
- The few advantages we have with classic computers don't apply
- What's our strategy for keeping these machines safe?