Physical Threats

- By and large, the physical world is a safe place
  - Very few people are attacked each day
  - Very few businesses are robbed
  - But the nightly news plays up each such event
  - ...and for those involved, there are serious implications

Digital Threats

- This is also true for Cyberspace
  - Most of my e-mail doesn’t contain viruses/worms
  - Most of the web pages I visit aren’t infected
  - Most traffic on the net isn’t DDOS traffic
- But, like the physical world, there are significant attacks and they do make headlines
Are Electronic Attacks Different?

- Not really
  - The motivations are the same
    - Greed, boredom, vengeance, …
  - The underlying crime is the same
    - Robbery, blackmail, espionage, child porn…
  - The laws are already there!
- This reinforces our point that technology is only part of SA.

But Are They the Same?

- Again, not quite
- The difference isn’t in the motivation, or the base crime, it’s in the approach and the effect
- Consider the spread of NIMDA or Code Red
- The ability to infect/affect a vast majority of the world gives one pause
- Worm/Warhol Worm/Flash Worm (see web site for reference to Flash Worms)

Why Attacks Will be Different

- Automation
- Reach
- Propagation
## Automation

- **Look at a couple of physical attacks**
  - **Counterfeit coins**
    - I could make perfect phony quarters, but it would be too expensive, and too hard to use
    - Phone phreaking (Cap’n Crunch)
  - **Lock picking**
    - I can learn to pick locks, and there are even lock picking “guns,” but there’s no machine to pick all the locks in my building by itself

## Automation II

- **What about cyber attacks?**
  - **419 scams**
  - **Make Money Fast!!!**
  - **Spam Spam Spam Spam...**
  - **Success rates can be low**
    - What if you had a 1/100,000 chance of success for an advertisement/attack/con?
    - Not feasible in the physical world; no problem in the virtual world
  - **Many, many minuscule attacks are now feasible (e.g., Salami attacks)**

## A Digression: Face Recognition

- Suppose a 1% false positive, and a 0% false negative (unrealistically optimistic)
- 1,000,000 passengers per day; 1 terrorist on a given day (this would be a high average!)
- 10,000 false positives for the 1 true positive.
- Is this acceptable?
Privacy Attacks

- Certain information has always been a matter of public record
- But accessing the public record has not always been easy
- Correlation is the key (data mining)
- DoubleClick
- Wegman’s/Dick’s frequent shopper programs
- Amazon’s recommendation pages
- Kevin Du: Privacy-preserving data mining
- Much, MUCH more on this later…

Reach

- There are no borders
- For physical crimes, location is important: I can’t break into your home if I’m in the next country
- Local laws have meaning
- But in Cyberspace, I can sit on an island or in a remote country and attack anyone/anywhere that I want to

It’s also Reach Back

- I can reach out and touch you, but can you prosecute me?
- International treaties (or lack thereof) make it extremely difficult to obtain warrants, etc., internationally
- Cuckoo’s Egg
- FBI’s activities
Other Jurisdictional Issues

- Where does a crime take place?
- Where the criminal is?
- Where the data/server is?
- Where is the data?
- This cuts both ways
  - Convictions of BBS operators in Tennessee
  - Nigeria...

Propagation

- How long does it take to break into a computer, then attack another?
- For a human, the first time, it can take many minutes or hours.
- Once a hole is found, a program can be written to exploit it
- That program can then be used
- Script kiddies (Kiddiez)

The Immune System Analogy

- Some people model assurance on the human immune system
  - Self, non-self
  - Adaptive
  - We know that it works in real life
- But...
  - Immune systems “learn,” and that takes time
  - Intelligence
  - Species vs. individual (evolution)
### Problems with the Internet

- 90% of the world’s computers run a single vendor’s OS
  - Monoculture—a single, or small number of attacks can be devastating
- Unlike the immune system, we don’t have adaptive, learning defenses
- Time is on the attackers’ side

---

### Nimda, Warhol, and Flash

- Nimda used an initialized list of hosts to attack, and then they attacked more, and then they attacked more…tree
- Warhol worm: taking over the net in 15 minutes
- Flash worm: take over the net in seconds
- Homework: read Warhol and Flash papers and write 1-page summary (Due: Friday).