Last time

• Administering Security
  – Security planning
  – Risk Analysis
This time

- Physical security
- Legal and ethical issues
  - Intellectual property
Physical security

- All the firewalls in the world won't help you defend against an attacker who physically steals your laptop off your desk
  - See the Data Loss archive from last week for many examples of personal information being lost in incidents just like this

- We need to protect the physical machines, as well as the software and data
Physical threats

- There are two major classes of physical threats:
  - Nature, e.g.:
    - Fire
    - Flood
    - Blackouts
  - Human, e.g.:
    - Vandals
    - Thieves
    - Targetted attackers

- What are the major differences in the security controls needed to protect against these two classes?
Physical controls against humans

- Last time, we looked at being able to recover from natural disasters
  - Many of these techniques will also be useful against thefts, etc.

- This time, we will discuss what additional measures are necessary to protect against humans
  - Need to not only recover from the loss, but also deal with the release of potentially sensitive data
Vandals

- Some human attacks aren't actually after the data
- Sir George Williams (later Concordia U) “Computer Centre Incident” of 1969 — the largest student uprising in Canadian history

- How would you control this kind of threat?
Thieves

• Most thefts are after what?
  - Hardware?
  - Software?
  - Data?

• We've already talked about controls against theft of software and data

• What about hardware?
Targetted attackers

• What if the thieves are actually targeting you?

• Now what are they most likely to be after?
  – Hardware?
  – Software?
  – Data?
Protecting offline data

- We have a good sense of how to protect data on an active machine hooked up to a network.

- What about data sitting on a shelf?
  - Backup tapes / disks
  - Printouts / reports

- What happens after they're on the shelf?

- Why is offline data like this attractive to attackers?
Protecting offline data

- It's obviously harder for a network-based attacker to get at that kind of data

- But what about a physical attacker?
  - Thief
  - Insider

- How do you safely dispose of data?
  - Paper
  - Magnetic media
  - Optical media
Putting it together

• So now we know how to protect:
  – Programs
  – Operating Systems
  – Networks
  – Internet applications
  – Databases
  – Physical computers and data

• How can we test if we've done it right?
Tiger teams

- Tiger teams are teams of security professionals

- You can hire them to try to break into your site, systems, networks, etc.
  - And tell you what's wrong
Legal protections

• Remember this from lecture 1:

• How can we defend against a threat?
  – Prevent it: block the attack
  – Deter it: make the attack harder or more expensive
  – Deflect it: make yourself less attractive to attacker
  – Detect it: notice that attack is occurring (or has occurred)
  – Recover from it: mitigate the effects of the attack

• In addition to (sometimes instead of, unfortunately) using technological defences, we can also use legal defences
Legal protections

• The most obvious legal protections are against threats to hardware

• If someone steals a laptop, it's completely straightforward that he can be charged with a crime

• What if someone copies the laptop's hard disk, but leaves the laptop where it is?

• This is much newer law, and is often less clear
  - Caveat: IANAL; this course does not constitute formal legal advice. :-}
Overview of IP

• In contrast to real property, so-called “intellectual property” (IP) differs in important ways:
  - It is non-depletable
  - It is replicable
  - It has minimal marginal cost

• So the laws for IP differ from the laws for real property, and indeed are much more complicated

• Four kinds of IP concern us:
  - Trade secrets, trademarks, patents, and copyrights
Overview of IP

• These four kinds of IP:
  – Cover different kinds of intangibles
  – Convey different rights
  – Have different durations
  – Have different registration requirements
  – (But are nonetheless often confused for each other!)

• Note: IP law is similar, but not identical, in Canada and the US; we will make note of the most important differences
Trade secrets

- This is the simplest kind of IP

- You want to protect some secret information
  - The formula for Coca-Cola
  - The method for computing how many airline seats to oversell
  - Your new O(n) sorting algorithm

- Just don't tell anyone, and call it a trade secret
  - Unfortunately, you have to tell someone, or it's not useful
  - You get legal protection if that person passes it on
Reverse engineering

- Reverse engineering is the process of taking a finished product, and taking it apart to figure out how it works
  - If someone successfully does this, you've lost your trade secret protection
  - General rule for trade secrets: it has to be a secret

- A similar rule applies to software, with some caveats we'll see later

- RC4 was originally a trade secret, but it was reverse engineered in 1994
Trademarks

• Even though the RC4 algorithm was no longer protected, its name was!

• Trademarks protect names, brands, logos

• To get one, make a legal filing showing that you are using the name in commerce
  – This lets you sue others who use that name in a confusing manner

• Domain names are often protected under trademark law
Patents

• Applies to inventions, which must be:
  – Novel
  – Useful
  – Nonobvious

• The bargain is that:
  – You tell everyone how your invention works
  – In exchange, you get to have a monopoly over it for 20 years

• The most difficult form of IP to obtain
Cryptography patents

- Many cryptographic algorithms are (or were) patented
- Notably:
  - Diffie-Hellman (expired 1997)
  - RSA (expired 2000)
  - IDEA (block cipher used in early PGP, expires 2012)
  - Lots of patents on elliptic curve cryptography
- Since 2000, you could pick a good unpatented example of each type of crypto
Recap

- Physical security
- Legal and ethical issues
  - Intellectual property
Next time

• Legal and ethical issues
  – Copyright and paracopyright
  – Computer crime
  – Redress for software failures
  – Codes of professional ethics