Last time

- Physical security
- Legal and ethical issues
  - Intellectual property

This time

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

Copyright

- Copyright is the most well-known kind of IP
- No filing requirement
  - But you can get additional benefits if you do file
- Protects expressions of ideas in a tangible medium
  - But not ideas themselves!
- Lasts a “limited time”
  - Currently: life+70 years in the US, life+50 in Canada
- The copyright holder has monopoly rights over certain uses of the work; primarily, making copies

Legal copying

- Even the rights granted to the copyright holder aren't absolute
  - Anyone can copy a work without permission in certain circumstances
- In the US, these circumstances are broad, but loosely defined
  - It's sometimes not obvious when they apply
- In Canada, there are very specific (but narrow) circumstances

Fair use

- In the US, these exceptions are called fair use
  - For purposes such as criticism, comment, news reporting, teaching, scholarship, or research
  - Four tests:
    - the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
    - the nature of the copyrighted work;
    - the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
    - the effect of the use upon the potential market for or value of the copyrighted work

Fair dealing

- In Canada, the fair dealing exception to copyright law is more limited

- It applies to private study, research, criticism, review, and news reporting
  - This is an exhaustive list!
  - It does not apply to things like parody, or even time-shifting (i.e. using a VCR), which are protected in the US under fair use

Private copying

- Canada has another exception to copyright:
  - You are allowed to copy a sound recording “onto an audio recording medium for the private use of the person who makes the copy”
  - In exchange, everyone pays a levy (about 21 cents) on blank audio recording media like tapes and blank CDs
- Some people argue this makes the downloading of songs over a P2P network legal in Canada
  - But uploading still probably isn't!

Paracopyright

- In 1998, the US passed the Digital Millennium Copyright Act (DMCA)
- It didn't make any additional acts of making copies illegal; rather, it made illegal the manufacture, selling, or “traffic” of devices that might help you make copies
  - For example, by circumventing any technological copy protection mechanisms that might be in place
- Problem: this applies even when the device is used to make a “fair use” copy!
- Canada has no such law; Bill C-60 had some similarities, but never got passed
  - A new Canadian copyright law may be just around the corner, though

Computer crime

- We talked last time about how laws regarding intellectual property differ from those about real property

- Similarly, laws about unauthorized access of computers, networks, or services differ from those about trespass
  - But until those new laws came about, courts had to make really stretched analogies to handle such events

Computer crime

- Early on, there were bizarre rulings:
  - The value of stolen data was the value of the paper it was printed on
  - The value of a stolen manual was the value of the equipment it was the manual for
- Things seem to have settled down somewhat
  - At least as long as (para)copyright doesn't get involved
- But there are still many recent and active issues!
  - If your ISP keeps a copy of your incoming email, is that wiretapping?

Rules of evidence

- Another problem with prosecuting computer crime is producing evidence admissible in court
  - "Chain of custody"
- Should the log files of the machine that was broken into be admissible?
- How should you preserve electronic evidence from the time of the intrusion to the time of a possible trial?
  - And there's usually no physical evidence at all to speak of!
  - Computer forensics replace regular forensics

Cybercrime treaty

- Worse, computer crime is often international
- Rules of evidence, police powers, etc. in one country don't usually carry over to another
- The Council of Europe cybercrime treaty (to which Canada and the US are also signatories) stipulates that member countries should pass laws making it easier for law enforcement to access telecommunications traffic (including voice, data, and Internet)
  - Canada's version of this law hasn't passed yet
  - We're still working out what it should look like

Scope of “Lawful Access”

- Who will be covered?
  - Phone companies
  - ISPs
  - Web server operators?
  - Wireless Nomad?
  - Coffeeshops with free Wi-fi?
  - Anyone who has Wi-fi at home?
    - Will you have to have a Wi-fi router with a “back door”?

Dangers of building in “back doors”

- From a technical point of view, adding the ability for anyone to surreptitiously intercept communications is designing in a weakness
- These dangers have been known since the Clipper Chip days, back before the turn of the century
- Remember that the technology can't tell whether any oversight requirements are met

Dangers of building in “back doors”

- If there's a back door built into the system, the bad guys will find a way to use it
  - Technical means (hacking in)
  - Social engineering
- This isn't just a hypothetical concern!

Greek wiretapping scandal

- Many senior Greek government officials had copies of their calls routed to a bank of throwaway cell phones
- Unknown people used CALEA interception capabilities built into phone switches to comply with US law
  - But this was in Greece!

Harmonization

- Industry prefers to only build one thing, not one thing for each jurisdiction
  - "Any new technical requirements must be based on international standards" (Information Technology Association of Canada submission to Customer Name and Address consultation)
- So we tend to end up with the biggest "back doors" required anywhere

Regulation of Investigatory Powers

- Example of a big back door required elsewhere:
- In the UK, Part III of the RIP Act went into effect last month
- You can be served notice to:
  - Decrypt data
  - Hand over decryption keys
  - Don't tell that this has happened

Redress for software failures

- If flaws are discovered in most products you buy, you can get a new one (with the flaw repaired), or at least a refund
  - Not so with software
- Why is that?
- Note that embedded software usually doesn't have this problem: flaws in embedded software (in things like cars, for example) are usually fixed by the manufacturers

Reporting flaws and failures

- What should you do if you discover a flaw or failure in a software product?
  - Especially a security flaw
- Vendors prefer that you tell them, and no one else
  - And then they can tell no one else, and the problem is solved?
  - Some vendors will even back up this preference by suing you (or having you arrested!) if you publicly disclose a security flaw in their products

Full disclosure

- Some people (but not usually vendors) prefer full disclosure
  - When you find a problem, post it to a full disclosure mailing list of security professionals (like Bugtraq)
  - The reasoning is that by the time you (the good guys) have found the problem, the bad guys probably have as well, and may be actively exploiting it
  - You need to plug the hole as quickly as you can, until the vendor comes up with an official fix
  - Further, without disclosure, vendors sometimes have little incentive to fix the problem at all

Responsible disclosure

- Vendors countered with responsible disclosure:
  - If you find a security flaw, tell the vendor
  - Tell no one else for at least 30 days
  - If the vendor hasn't announced the flaw, with credit to you, and hopefully with a fix, in that 30 days, you should contact a coordinating centre like CERT to decide what to do next
- There is ongoing debate (see link on UW-ACE) as to which way is best
  - Best for whom?

Codes of professional ethics

- As a computer security professional (or even not specifically in security), you will be expected to uphold certain ethical standards
  - Note: ethics != law
- You will probably be a member of one or more professional societies
  - Association for Computing Machinery (ACM)
  - Institute of Electrical and Electronics Engineers (IEEE)
  - Canadian Information Processing Society (CIPS)
- These organizations have codes of professional ethics
  - Linked to on UW-ACE

Example: CIPS

- Most professional codes of ethics have similar flavours, with some difference in detail

- These are the high-level bullets from CIPS' code:
  - Protect Public Interest and Maintain Integrity
  - Demonstrate Competence and Quality of Service
  - Maintain Confidential Information and Privacy
  - Avoid Conflicts of Interest
  - Uphold Responsibility to the IT Profession

Recap

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