Lecture notes for 11.1-11.4 Intellectual Property

If it's property, why don't we pay property tax on it?

Intellectual Property
- A creation that requires significant resources to initially create, few resources to duplicate
- Examples: software, media, books

Threat
- User of the system is attacker
- Hardware may be malicious
- OS may be malicious
- Apps may be malicious
- Extremely challenging threat model: only one user need be sufficiently skilled to defeat checks, then they distribute cracked copy to everyone else

Common protection
- License files & checks in software
- DRM checks in media viewers/players

Defeating protections
- Generate duplicate / fake license files
  - Producers make software call home (windows genuine advantage)
- License checks & DRM checks are just code
  - Identify & remove code / overwrite with nops
  - Def: Cracked software: new version of a formerly protected piece of software with protections removed
  - Producers try to make removal highly difficult

Software protections
- Self-checksumming
  - [Explain self-checksumming with an example]
  - [Explain attack using malicious OS playing games with page tables]
- Code obfuscation
  - Makes software difficult to analyze, hard to find protection code

- Examples: indirect control flows, opaque predicates, return address manipulation

Watermarking
- Def: embedded information in a digital file that identifies unique copies of the file but cannot be easily identified, altered, or removed
- Provides attribution for copies
- Software watermarking
  - Variable names
  - Code layout
- Does not prevent distribution, allows identification & prosecution of leaker

Hidden functionality (Old Macs)
- http://www.folklore.org/StoryView.py?project=Macintosh&story=Stolen_From_Apple.txt&sortOrder=Sort%20by%20Rating&detail=medium
- http://img516.imageshack.us/img516/5517/stolenfromapple3zv.jpg

Media protections
- Watermarking
  - Similar to covert channel
  - Distort data in ways not visible to human
  - Must be robust to media transformations (resizing, etc)
- Program that enforces protections on media
  - [… so software protections matter, too]

Trusted hardware (TCG)
- [Draw picture vertical stack, verifying upwards]
- [Idea: verification will ensure that next layer does not have malicious software... has only known software that people know doesn't break license checks]