CompSci 725
"Soft" Security

Clark Thomborson

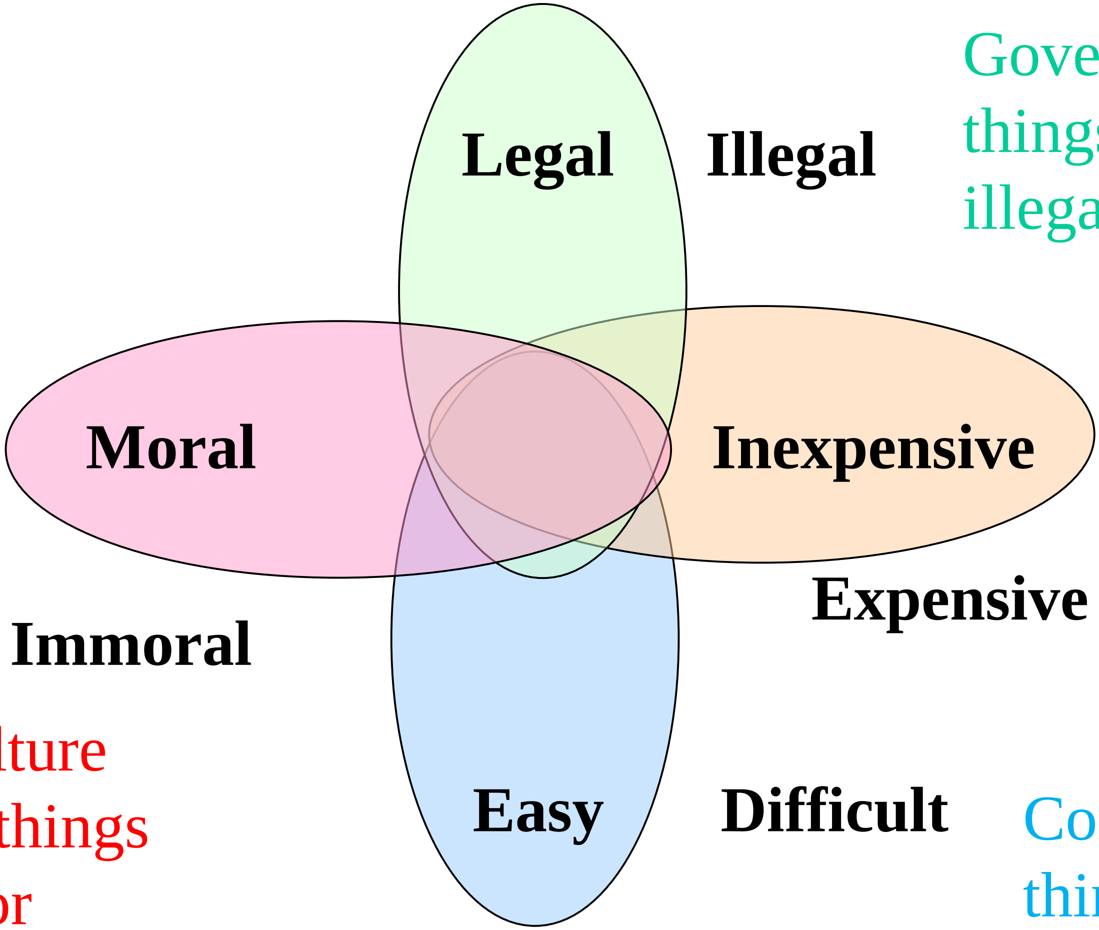
University of Auckland

v1.1 of 10 Aug 2017: slides on individualism, other isms

Real-World Security Analysis

- *Whose* security is being protected?
  - Every person, and every organised group of people, has security objectives.
  - No computer has security objectives. (Do you agree?)
- *How* could the secured entity be harmed?
  - "Security objective" e.g. loss of an asset
- *Who* might want to harm this entity?
  - "Threat agent", "threat model"
  - (How can a threat model be validated? Can it be verified?)
- Is the control *proactive* (with guards), or *reactive* (with judges)?
- Is the control *hierarchical*, or is it *democratic*?
  - Hierarchs control their organisation by administering threats and rewards. (Rule of law, or an arbitrary ruler?)
  - Peers control their society by shaming, persuading, gossiping, buying and selling. (An ethical society, or an anarchic society?)

Lessig’s Taxonomy of Control



Governments make things legal or illegal.

The world’s economy makes things inexpensive or expensive.

Our culture makes things moral or immoral.

Computers make things easy or difficult.

Ethics for IT Security (Pfleeger, 1997)

- What is ethics?
  - "Through choices, each person defines a personal set of ethical practices [when deciding right actions from wrong actions]."
  - Ethics is not law, not religion, and not universal.
- Principles of Ethical Reasoning
  - How to examine a case for ethical issues.
  - Taxonomy of ethics: consequence *vs* rule-based; individual *vs* universal.

A contradiction?

☞ You make choices every minute, are all your choices ethical?

Universal, Rule-Based Ethics

- Pfleeger suggests the following “basic moral principles” are “universal, self-evident, natural rules”:
  - – The right to know
  - – The right to privacy
  - – The right to fair compensation for work

☞ Should you expect users to obey these rules, when you are designing a security system?

☞ Should you enforce these rules in your systems?

Our Duties, from Sir David Ross

- Fidelity (truthfulness)
- Reparation (compensate for wrongful acts)
- Gratitude (thankfulness for kind acts)
- Justice (distribute happiness by merit)
- Beneficence (help other people)
- Nonmaleficience (don’t hurt other people)
- Self-improvement (both mentally and morally, *e.g.* learn from your mistakes)

☞ Which of these duties support our “rights” to knowledge, privacy and compensation?

☞ Are these universal duties, or merely “Western/Christian”?

Christian Ethics, in brief (Huston Smith, 1989)

- Moses: don’t murder, commit adultery, steal, lie.
- New Testament: faith, hope, love, charity.
- Golden Rule: “Do unto others as you would have them do unto you.”

☞ Which of these ethics support our “rights” to knowledge, privacy and compensation?

Confucian Ethics, in brief

孔 Kǒng
夫 fū
子 zǐ

仁 Rén

Ren (human-heartedness): “Measure the feelings of others by your own.”

義 Yì

Yi = zhong + shu (right conduct = doing one’s best + altruism): “How can I accommodate you?” not “What can I get from you?”

忠 Zhōng
恕 Shù

禮 Lǐ

Li (propriety): follow Confucius’ example, nothing in excess, respect for elders, …

德

De (power of moral example): leaders must show good character.

文

Wen (the arts of peace): music, poetry, painting; contrast with the arts of war and commerce.

Which of these ethics support our “rights” to knowledge, privacy and compensation?

己	Yourself,
所	what
	[you]
不	don't
欲，	want,
勿	don't
施	do
於	to
人	others.

Analects 15:23

Islamic Ethics, in brief

- Economic: don’t charge interest (but you may invest for a share of profit); all offspring should inherit; 2.5% to charity each year.
- Social: racial equality, no infanticide, women must consent to marriage.
- Military: punish wrongdoers to the full extent of injury done; honour all agreements; no mutilation of wounded.
- Religious: “Let there be no compulsion in religion.” (2:257)

☞ Which of these ethics support our “rights” to knowledge, privacy and compensation?

Individualism

- "God helps those who help themselves"
- Dale Carnegie: *How to Win Friends and Influence People*, 1936:
  - "Twelve Things This Book Will Do For You
    1. Get you out of a mental rut, give you new thoughts, new visions, new ambitions…
    4. Help you to win people to your way of thinking…
    7. Increase your earning power.
    8. Make you a better salesman, a better executive…"
- "Greed is good: A 300-year History of a Dangerous Idea", The Atlantic, 7 April 2014.

Individualism in the Chinese Tradition

- “Unlike individualism in modern European and American contexts, Chinese manifestations of “individualism” do not stress an individual’s
  - separation,
  - total independence, and
  - uniqueness from external authorities of power.
- “Rather, individualism in the Chinese tradition emphasizes
  - one’s power from within the context of one’s connection and unity (or harmony) with external authorities of power.
- “… the Western tradition tends to view the individual in an atomized, disconnected manner, whereas the Chinese tradition focuses on the individual as a vitally integrated element within a larger familial, social, political, and cosmic whole.”

[Erica Brindley, Internet Encyclopedia of Philosophy, ISSN 2161-0002, retrieved 10 August 2017]

Ethical Communism

- “Nothing in society will belong to anyone,
  - either as a personal possession or as capital goods,
  - except the things for which the person has immediate use, for either his needs, his pleasures, or his daily work.
- “Every citizen will be a public man,
  - sustained by, supported by, and occupied at the public expense.
- “Every citizen will make his particular contribution
  - to the activities of the community according to his capacity, his talent and his age;
  - it is on this basis that his duties will be determined, in conformity with the distributive laws.”

[E-G Morelli, *Code of Nature Or, The True Spirit of Laws*, 1755. Trans. A Fried and R Sanders, ed., *Socialist Thought: A Documentary History*, Columbia University Press, 1964]

Cybernetics

- “Although Wiener [1954] stated his ‘great principles’,
  - he did not assign names to them.
  - For purposes of easy reference, let us call them …
- **The Principle of Freedom**
  - Justice requires ‘the liberty of each human being to develop in his freedom the full measure of the human possibilities embodied in him.’
- **The Principle of Equality**
  - Justice requires ‘the equality by which what is just for A and B remains just when the positions of A and B are interchanged.’
- **The Principle of Benevolence**
  - Justice requires ‘a good will between man and man that knows no limits short of those of humanity itself.’

https://plato.stanford.edu/entries/ethics-computer/, retrieved 10 Aug 2017.

Is ethical analysis necessary?

- “Might makes right” (i.e. legal ≡ ethical)
  - Does a society ever have a right to rebel against an unjust ruler?
  - Does an employee ever have an ethical obligation to refuse a work assignment, to reveal a corporate secret?
- “Money is the root of all good” (Ayn Rand, *Atlas Shrugged*, 1957) (i.e. economic ≡ ethical)
  - “Until and unless you discover that money is the root of all good, you ask for your own destruction.
  - “When money ceases to become the means by which men deal with one another, then men become the tools of other men.
  - “Blood, whips and guns or dollars. Take your choice - there is no other.”
  - Aren’t there other utopias, with other choices?

Utopia

- “A utopia is an imagined community or society that possesses
  - highly desirable or nearly perfect qualities for its citizens.
- “Utopian ideals often place emphasis on
  - egalitarian principles of equality in economics, government and justice, though by no means exclusively, with the
  - method and structure of proposed implementation varying based on ideology.
- “According to Lyman Tower Sargent ‘there are
  - socialist, capitalist, monarchical, democratic, anarchist, ecological, feminist, patriarchal, egalitarian, hierarchical, racist, left-wing, right-wing, reformist, free love, nuclear family, extended family, gay, lesbian, and many more utopias’.”

[https://en.wikipedia.org/wiki/Utopia, 10 Aug 2017]

Professional Ethics

- If you, as a computer professional, design a webservice for “real world security” as defined by Lampson,
  - will your service be ethically offensive in some societies?
- Are Wiener’s “great principles” an adequate basis for ethical security in all societies?

Professional Codes of Ethics

- Most professional organisations, such as the IEEE, the ACM, and the RSNZ, have codes of ethics.
- If you transgress a professional code of ethics, your organisation may revoke your membership.
- To explore these ideas:
  - Examine the IEEE Code of Ethics. Is it congruent with Confucian ethics? With cybernetics? Explain.
  - Examine the RSNZ Code of Professional Standards and Ethics. Is it in conflict with the IEEE Code of Ethics? Explain.
  - Describe the "Ten Commandments of Computer Ethics" using Pfleeger's terminology.

Conclusion

- Because ethics are personal, and conditioned by our cultures, they won’t “always work” as a control in any security system. (But all controls are imperfect!)
- I believe security engineers must consider how their systems will affect (and be affected by) the ethics of its likely users.

Ethical Analysis of Copyright

- Samuel Johnson: “For the general good of the world,” a writer’s work “should be understood as belonging to the publick.” To which of Pfleeger’s “rights” does this argument refer?

☞ The public’s right to information.

- Richard Aston: it is “against natural reason and moral rectitude” that a government should “strip businesses of their property after fourteen years.”

☞ The publisher’s right to compensation.

Chinese Ethics of Copyright?

- In 1993, John Perry Barlow (noted cyberlibertarian) and Mitch Kapor (author of Lotus 1-2-3) visited a Hong Kong shop that specialised in “pirated” software.
  - Barlow saw “not the slightest trace of moral anxiety” in the salesclerk’s face, when Kapor informed her that he was the author of the work he was trying to purchase.
  - She said, “Yeah, but you still want a copy, right?”
  - [Charles C Mann, “Who Will Own Your Next Good Idea”, *The Atlantic Monthly*, September 1998.]
- What is “fair compensation for work”?
  - Employers might pay USD $0.50/hour for Chinese labour, and USD $10.00/hour here. Should copyright items cost 20x more in NZ than in China?
  - Confucian ethic of “Wen”: Mandarins should produce art but never sell it.
  - What were Mao’s thoughts on copyright?

My View on Copyright

- Copyright law is a delicate balance, developed over centuries, among the rights of authors, publishers and the public in Western democracies.
- Technological developments and international commerce are forcing rapid change in copyright law. There hasn’t been enough time for wisdom!

“Steal this Software”

Hillary Rosner

The Industry Standard, 26 June 2000

“Never paying for software is a point of pride among tech insiders. The Internet is making it easier for outsiders to join this jolly band of software pirates. … [Adobe] estimates that as much as 50 percent of the company’s software in use today is stolen.”

Outline

- How and why “insiders” [crackers] steal software
- How “outsiders” (like you) could steal, too.
  - Napster, Gnutella, Freenet, Hotline
- For the foreseeable future, it will be difficult for any publisher to prevent the piracy of its software products.

Software Piracy in Hotline

- “Cracked” software (“warez”) can be downloaded inexpensively, if you “go through a series of links to obtain a username and password” to a Hotline server.
- “Most Hotline servers are maintained by people
  - who have no interest in software and are just in it for the money they can make when software seekers click through the ads...
  - … The rest are college kids and anarchic programmers in it for the thrill.”

Rosner’s Ethics of Software Piracy

- “Insider’s entitlement”: if you’re clever enough to find “warez” then you deserve to have it without paying.
- If you buy any software, then you’re also in danger of buying the [Brooklyn] bridge if someone tried to sell it to you. [This is an old joke in America, making fun of naïve immigrants.]

☞ Is this an accurate description of cracker (phreak) culture?

The New Hacker’s Dictionary

- See http://www.catb.org/~esr/jargon/html/L/lamer.html
- A “lamer” is someone who “scams codes off others, rather than doing cracks or really understanding the fundamental concepts.”
- If this dictionary is an accurate reflection of cracker culture, then the warez available to non-crackers on Hotline must be pretty lame.

Ethics of Software Piracy

- If crackers only share with other crackers, who (if anyone) is harmed?
  - Legal analysis: the author and the publisher (who may assert their rights under the laws of contract, copyright, trademark or patent)
  - Ethical analysis: rights of knowledge *vs* compensation
- Is it worse if crackers post warez for lamers too?
  - Legal analysis: yes, more damage is done.
  - Ethical analysis: what rights do lamers have to this knowledge?

Rudimentary Treatise on the Construction of Locks, 1853

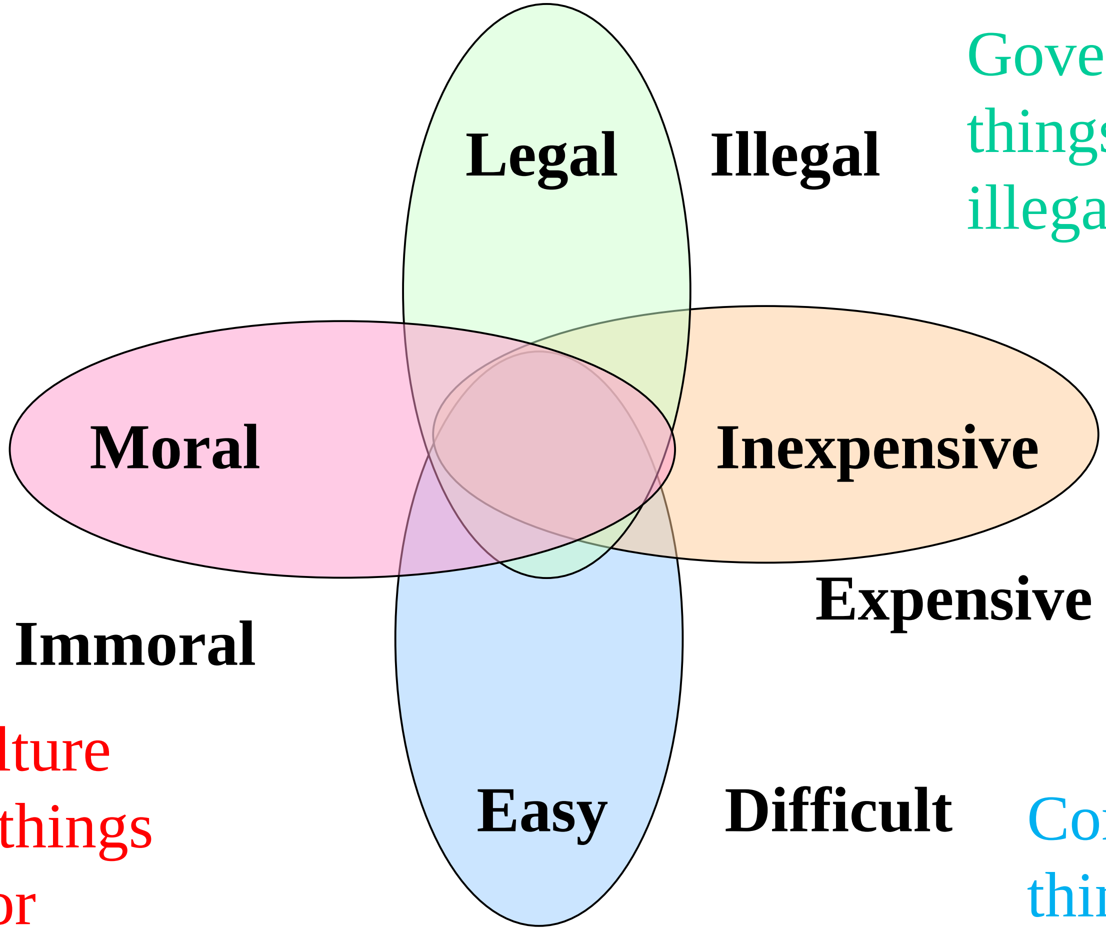
Charles Tomlinson

- “Rogues knew a good deal about lockpicking long before locksmiths discussed it among themselves.”
- “If a lock… is not so inviolable as it has hitherto been deemed to be, surely it is in the interest of *honest* persons to know this fact.”

Tomlinson’s Argument (cont.)

- “The inventor produces a lock which he honestly thinks will possess such and such qualities; and he declares the belief to the world. If others differ… the discussion, truthfully conducted, must lead to public advantage.”
- What is your ethical analysis? (Right to information *vs* ??)
- Would your analysis change if the “lock design” were protected by trade secret?

Lessig's Taxonomy of Control



Governments make things legal or illegal.

The world's economy makes things inexpensive or expensive.

Our culture makes things moral or immoral.

Computers make things easy or difficult.

An Overview of “Software Law”

- There are many types of legal controls on your activities:
  - Certain actions (theft, fraud) are **crimes**.
  - A few actions (e.g. a “duty of care”) are **obligations**: you can be punished if you don’t do them adequately.
- Every jurisdiction is **different**!
  - A first step in a legal analysis: what judiciaries have authority in this situation, and which of their laws are applicable?
  - Cross-jurisdictional generalisations are dangerous, as are naïve summaries. (I am not providing legal advice here. ;-)
- Modern states enforce **ownership rights**, making it illegal (or actionable in a civil suit) for non-owners to do certain things to an owned object.
  - An owner can sell property (if it’s “alienable”), or issue a license-to-use e.g. by lease or rental.
  - I’ll survey the “intellectual property” aspect of software, with respect to US law.

U.S. Patents, Trademarks, Copyright

- **Patent**: “the right to exclude others from making, using, offering for sale, or selling the invention in the U.S. or ‘importing’ the invention into the United States.”
- **Trademark**: “a word, name, symbol or device which is used in trade with goods to indicate the source of the goods and to distinguish them from the goods of others.”
- **Copyright**: “the exclusive right to reproduce the copyrighted work, to prepare derivative works, to distribute copies or phonorecords of [it], to perform [it] publicly, or to display [it] publicly.”

Source: US Patent and Trademark Office, “What Are Patents, Trademarks, Servicemarks, and Copyrights?”, October 2015, available http://www.uspto.gov/patents/resources/general_info_concerning_patents.jsp#heading-2.

U.S. Patents: Basics

Three types of patents:

1. **Utility** patents: "… new and useful process, machine, article or composition of matter, or any new and useful improvement thereof"
2. **Design** patents: "… new, original, and ornamental design for an article of manufacture…"
3. "**Plant** patents may be granted to anyone who invents or discovers and asexually reproduces any distinct and new variety of plant."

What is Patentable in the USA?

- New:
  - “(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for patent,” or
  - “(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country more than one year prior to the application for patent in the United States . . .”
- Useful:
  - “has a useful purpose and also includes operativeness, that is, a machine which will not operate to perform the intended purpose would not be called useful”
- Non-obvious:
  - “sufficiently different from what has been used or described before that it may be said to be nonobvious to a person having ordinary skill in the area of technology related to the invention
- “The specification must conclude with a claim or claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as the invention.”

Every country has its own laws…

- People often talk about software patents
  - what exactly do they mean?
- The term “software” is considered [by the EPO] to be ambiguous, because it may refer to
  - a program listing written in a programming language to implement an algorithm, but also to
  - binary code loaded in a computer-based apparatus, and it may also encompass
  - the accompanying documentation.
- … in place of this ambiguous term the concept of a computer-implemented invention has been introduced.

Source: “Patents and Software? European Law and Practice”, available http://www.epo.org/news-issues/issues/software.html, 11 Aug 2013.

Computer-Implemented Invention (EU)

- A computer-implemented invention is one which
  - involves the use of a computer, computer network or other programmable apparatus,
  - where one or more features are realised wholly or partly by means of a computer program.
- Under the EPC, a computer program claimed “as such” is not a patentable invention (Article 52(2)(c) and (3) EPC).
- For a patent to be granted for a computer-implemented invention, a technical problem has to be solved in a novel and non-obvious manner.

EU Non-inventions

- So-called non-inventions (those expressly excluded under Article 52 EPC, such as methods of doing business, mathematical methods or presentations of information) enter the realm of patentability in Europe
  - with the use of technical means such as a computer or a computer network.
- Computer programs for implementing a business method, nevertheless, would not be inventive since
  - they originate from non-technical constraints of particular business requirements,
  - the implementation of which on a conventional computer is obvious.

US Copyright Basics

- “[A] copyright protects ‘original works of authorship’ that are fixed in a tangible form of expression.”
  - “The fixation need not be directly perceptible so long as it may be communicated with the aid of a machine or device.”
- Covers “literary works, musical works, …sound recordings, architectural works.”
- Ineligible for copyright:
  - Unfixed works, e.g. unwritten or unrecorded speeches,
  - “Titles, names, short phrases, and slogans”,
  - “Familiar symbols or designs”,
  - “Mere listings of ingredients or contents”,
  - “Ideas, procedures, methods, systems ..., or devices, as distinguished from a description, explanation or illustration”.

Source: U.S. Copyright Office, “Copyright Office Basics”, reviewed May 2012. Available: http://www.copyright.gov/circs/circ01.pdf, 12 September 2016.

Securing a Patent or Copyright

- A patent is granted **only upon** application.
  - An examiner at the US PTO may ask questions of the inventor, before allowing or rejecting the patent.
- US copyright is **granted automatically** (to the author, or to the employer of the author) "when the work is created, and a work is 'created' when it is fixed in a copy or phonorecord for the first time."
  - A copyright notice (e.g. ©) has been optional in the USA since 1989, and is "still relevant to the copyright status of older works".
  - Copyright registration "is a legal formality intended to make a public record of the basic facts of a particular copyright... not a condition of copyright protection... [but] provides several inducements or advantages..."

NZ Copyright

- Applies to eight categories of “work or type of material”:
  - literary, dramatic, artistic, musical works;
  - sound recordings, films;
  - “communication works” (e.g. TV broadcasts);
  - “typographical arrangements of published editions”.
- Term of copyright protection depends on the type of work:
  - “Artistic works industrially applied” : 16 years
  - “Artistic craftsmanship industrially applied” : 25 years
  - Other categories: 25 to 50 years.
  - Note: US copyright lasts **much** longer than this.
    - “Life of author plus 70 years”; for works of “corporate authorship”, 120 years or 95 years after publication, whichever comes earlier”. (1998 Copyright Term Extension Act)
    - Note: Mickey Mouse was first published in 1928. 1928+95 = 2023.
    - 2019 is another important year for US copyright.

Source: MBIE, “Copyright Protection in New Zealand”, last updated 24 December 2015. Available: http://www.mbie.govt.nz/info-services/business/intellectual-property/copyright/copyright-protection-new-zealand/, 12 September 2015.

Exceptions to NZ Copyright

- There are a few exceptions to NZ copyright:
  - "Fair dealing": criticism, review, news reporting, research or private study;
  - Limited copying for educational, bibliographic or archival purposes;
  - "Subject to certain conditions, the making of a back-up copy of a computer program";
  - "time-shifting" of a television programme.
  - In 2008, a new exception was added (Sec 81A): format-shifting for audio recordings, if acquired lawfully and for personal or household use (but not for uploading onto file-sharing systems, or for friends)
- "Fair Use" in the US is a entirely different legal concept
  - NZ copyright covers **all** uses of copyright material, with the specific exceptions noted in the text of the law
  - Anyone accused of infringing US copyright has a broad (and somewhat flexible) defence called "fair use" (17 USC 107):
    - "In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include: the purpose and character of the use…"

US Copyright for Computer Programs

- Source and object code are protected as “literary works”:
  - “fiction, nonfiction, poetry, textbooks, reference works, directories, catalogs, advertising copy, compilations of information, computer programs and databases” (http://www.copyright.gov/eco/help-type.html)
- Additionally, some “non-literal elements” of a codebase are protected as “audiovisual works”. These include:
  - the “structure, sequence and organization of the programs” and their audiovisual output (Whelan v Jaslow, 1986)
  - but not the “ideas, program logic, algorithms, systems, methods, concepts or layouts.” (http://www.copyright.gov/circs/circ61.pdf)
  - “An audiovisual work is a work that consists of a series of related images that are intended to be shown by the use of a machine or device, together with accompanying sounds, if any.” (http://www.copyright.gov/eco/help-type.html)

A Brief History of (British and) American Copyright

- 1557: Stationers’ Company gains control of all printing and book sales, authors have few rights.
- 1710: Writers gain control of works, but only for 14 years (renewable once).
- 1774: House of Lords affirms that the rights of authors and publishers are temporary so that the “products of the mind always return to their real state: owned by no one, usable by everyone.”
- 1776: US declares independence, starts to develop its own laws and theories of copyright.

[Charles C Mann, “Who Will Own Your Next Good Idea”, *The Atlantic Monthly*, September 1998.]

Copyright in the French Revolution

- Prior to 1789, “privileged booksellers” were prey to pirates, and authors had few rights.
- Privilege was abolished in the Revolution.
- Culture suffered when no “serious books” or “great texts of the Enlightenment” were published.
- In 1793, authors were given power over their own work lasting until ten years after their death.

American Copyright Since 1776

- 1790: US Copyright Act passed: 14 year term with one renewal.
- 1790-1998: US Congress repeatedly extends the term of copyright
- 1998: Copyright protection is extended to databases.
- 1998: Digital Millennium Copyright Act makes it illegal (in the US) to subvert “©-chips”.

“The Age of Software Patents”

Kenneth Nichols

IEEE Computer, April 1999

“As a computer professional, it is highly unlikely that you have ever read a patent… however… patents will play a pivotal role in future software products and research.”

Outline

- Tutorials
  - Essentials of US patent law, for software
  - US trade secrets and copyright, for software
- Editorials
  - Why software is different from all other inventions
  - Why software patents don’t work
  - Software patents may be harmful

Public good of encouraging invention, versus the harm of restricting use

“… software patents are neither inherently good nor bad…”

Trade Secrets for Software

1. You write some clever software.
2. You don’t reveal your “secret” cleverness, except to people who have signed a “nondisclosure agreement” (NDA).
3. You can prosecute anyone who reveals your secret, if they have signed an NDA.
4. You have limited protection over people who “reverse engineer” your software to discover your clever idea.

What Can You Do with a Patent?

1. You may “assign” your patent to someone who will pay the (substantial) costs of filing and defending it.
2. You may sell licenses to your patent, allowing others to manufacture something containing your invention.
3. If you discover someone “infringing” your patent, you may offer to sell them a license, and you may refuse to let them use your patent.

☞ Why is your right of refusal in the public interest?

Harmful Effects of SW Patents

1. Patents that are worthless after 20 years, after allowing profitable short-term monopolies, are a bad “bargain” for society.
   - How many software patents will fall into this category?
   - “An excellent example is the group of software products designed to enhance computer performance … to ameliorate the memory limitations of the Intel 8088 processor.”
2. Because “patents amplify network effects”, firms will focus on technologies that offer a high potential for creating a monopoly.
   - “There are some signs that major software firms are neglecting certain areas of the market.”
   - Can you name one such area?

Conclusions

- All software developers should know at least a little bit about patents, copyrights and trade secrets. This article is an excellent introduction.
- I think the “jury is still out” on how much harm (and good) will be done by software patents.

Conflict-of-interest Disclosure

- My patents, published patent applications, and all other US patents and WIPO applications, can be viewed at the relevant patent office e.g. the US PTO.
  - More conveniently: Google Patents
  - Transaction System and Method, NZ Patent 533028, granted 12 January 2006, lapsed 18 May 2012.
  - Obfuscation Techniques for Enhancing Software Security, by Christian Collberg, Clark Thomborson and Douglas Low, US Patent 6,668,325, assigned to InterTrust Inc of Sunnyvale CA (USA), filed 9 June 1998, issued 23 December 2003.
  - Software Watermarking Techniques, by Christian Collberg and Clark Thomborson, US 2014/0165210 with priority to NZ 330675 of 10 June 1998. (Abandoned.)

The DMCA (1998)

- From *IEEE Computer*, Jan 2001, p. 30:
  - The DMCA made “it unlawful [in the USA] to circumvent technologies protecting access to copyrighted digital works such as software and music.”
  - The US Copyright Office “decided to permit users to bypass intellectual-property protection software only to determine which Web sites are blocked by filtering software and to work with materials protected by malfunctioning or obsolete access-control mechanisms.”
  - No other exemptions were granted.

“Hard” vs “Soft” Security

- Boaz Barak believes that all important systems should have “well-defined security”.
  - These systems can only be compromised if the analyst’s assumptions (e.g. about the secrecy of cryptographic keys) are invalid.
  - Assumptions can be checked for validity by anyone.
  - Security proofs can be validated by anyone.
  - See http://www.math.ias.edu/~boaz/Papers/obf_informal.html

Boaz’s Argument (in brief)

- “Of course, as all programmers know, using rigorously specified components does not guarantee that the overall system will be secure.
- “However, using fuzzily specified components almost guarantees *insecurity*.”

Is it Feasible to Specify Well?

- “The only problem is that it is very very difficult to build such “perfect” systems that are *large*.
- “In spite of this, with time, and with repeated testing and scrutiny, systems can converge to that bug-free state …
- “Such convergence cannot happen if one is using fuzzily secure components.”

Do you agree with Boaz?

Soft security: Necessary?

- I believe that only a few isolated, stable systems will ever converge on Boaz' ideal bug-free state.
  - Features are added and modified
  - Novel, unexpected uses: are these exploits or appropriate?
  - Systems interact with other systems in complicated, unstable, and unpredictable ways. ("Secure functional composition" is a research area, not a standard practice.)
- Do you trust your bank? Your credit card?
  - Human error is possible (e.g. Westpac Rotorua teller's misplaced decimal point)
  - Fraud is possible
  - Software is buggy, even if it is carefully verified (e.g. Ariane 5)
  - One coping strategy: "trust but verify"

My View of “Soft” Security

- Putting speedbumps on roads doesn’t stop all drivers from speeding, just as “speed bump” security (warning messages, propaganda, lamer-level defences) won’t stop a determined and skilled attacker.
- That doesn’t mean you should ignore “soft” defenses!
- If a secure system is illegal, immoral, unaffordable, or difficult to use, then it will be a target for attack by its legitimate users and its other stakeholders (e.g. the folks who are harmed by its illegal activity).
  - If a system meets Barak’s goal of “well-defined security” but is unaffordable, difficult to use, immoral, or illegal, is it a successful design? I think not…