Legal Issues and Ethics

Computer Security
1DV700

Faiz Ul Muram, Ola Flygty
Linnaeus University, Sweden
{faiz.ulmuram, ola.flygty}@lnu.se

Objectives and Contents

- Protecting Programs and Data
- Information and the Law
- Ownership Rights of Employees and Employers
- Redress for Software Failures
- Computer Crime
- Ethical Issues in Computer Security

Protecting Programs and Data

- **Copyrights**
  - Designed to protect the expression of ideas (creative works)
  - Gives the author the exclusive right to make copies of the expression and sell them to the public
- **Patents**
  - Designed to protect inventions, tangible objects, or ways to make them
  - Patents were intended to apply to the results of science, engineering, and technology as opposed to arts and writing
- **Trade secrets**
  - Information that gives one company a competitive advantage over others
  - Must be closely guarded as a secret, or legal protections are lost

Copyrights

- Copyright can be registered for **original works** of expression but **not** for **ideas**
- Copyright object is subject to "fair use" material used in a manner for which it was intended and does not interfere with the author's rights
  - e.g., new reporting, criticism, comment, teaching, scholarship, or research
- Software can be copyrighted
  - Copying the code intact is prohibited, but re-implementing the algorithm is permitted
  - If source code is not published (i.e., only compiled code is published), copyright may not apply

Copyrights

- Berne Convention is now practiced throughout the world, adopted in 1886 to deal with the protection of works and the rights of their authors
- Copyrights owner has these exclusive rights, protected against infringement:
  - **Distribution** right: the owner publicly sell, rent, lease, or lend copies of the work
  - **Modification** right: concerns modifying a work to create a new or derivative work
  - **Public-performance right**: applies mainly to live performances
  - **Public-display right**: show a copy of the work directly or by means of a film, slide, or television image

Patents

- Novelty requirement
  - Cannot be obvious to a person ordinarily skilled in the relevant field
- Must convince the patent office that the invention deserves a patent (i.e., that it is **truly novel or unique**)
- A patent holder must oppose all infringement or risk losing the patent rights
- Since 1981, patent law has extended to include computer software (USA), recognizing that algorithms are inventions, but the rules are different in different countries

Trade Secrets

- If someone obtains a trade secret improperly and profits from it, the owner can recover profits, lost revenues, damages, and legal costs
- If someone else happens to discover the secret independently, there is no infringement
- **Reverse engineering** used to uncover trade secret is **legal**!
- Trade secrets can protect secret computer algorithms from being used in other products
  - Cannot provide legal protection against software piracy
  - The challenge of using trade secrets to protect software is that software can be effectively reverse engineered

Comparing Copyrights, Patents, and Trade Secrets

	Copyright	Patent	Trade Secret
Protects	Expression of idea, not idea itself	Invention—the way something works	A secret, competitive advantage
Protected object made public	Yes; intention is to promote publication	Design filed at Patent Office	No
Requirement to distribute	Yes	No	No
Ease of filing	Very easy, do-it-yourself	Very complicated; specialist lawyer suggested	No filing
Duration	Varies by country; approximately 75–100 years is typical	19 years	Indefinite
Legal protection	Sue if unauthorized copy sold	Sue if invention copied	Sue if secret improperly obtained

Intellectual Property Issues and Computer Security

- Software programs
  - protect using copyright, perhaps patent
- Database content and arrangement
  - protect using copyright
- Digital content audio / video / media / web
  - protect using copyright
- Algorithms
  - may be able to protect by patenting

Information and the Law

- Information is a processed data, it can be pieces of objects that represent certain data and perform certain functions
- Characteristics: Information as an Object of value
  - Information is not depletable (if used it but you still have)
  - Information can be replicated, e.g., a book each person pays for a same information
  - Information has a minimal marginal cost
  - The value of information is often time dependent (outdated => less/no value)
  - Information is often transferred intangibly (transfer data through internet)
- These factors impact how information is treated under the law

Information and the Law

- The law protects personal data
- It regulates the use, development and ownership of data and software
- The law protects the secrecy, integrity and availability of data and services
- The **legal system** had to be adapted
  - But courts are not a perfect form
  - The pace of **change** is **slow**, it is not static
  - It helps to ensure that the changes that do occur are fair and well considered
  - Ethics had **not** to be **changed**

Laws: Rules adopted and enforced by governments to codify expected behavior in modern society

Ethics: Relatively fixed moral attitudes or customs of a societal group (based on cultural mores)

Different Legal Systems

- **Civil law**
  - A legal system originating in Europe, developed from Roman law, the main feature of which is that its **core principles** are codified into a referable (legal) system which serves as the primary source of law

- **Common law**
  - The intellectual framework comes from judge-made decisional law, and gives precedential authority to prior court decisions
  - Used for instance in UK and US

Different Types of Laws: Protecting Information

- **Criminal (Statutes) and Civil law**
  - Criminal law is the body of law that relates to crime (**state** prosecute)
  - The rights and duties of **individuals** amongst themselves is the primary concern of civil law
- **Tort law**
  - In common law and less in civil law, civil wrong which unfairly causes someone to suffer loss or harm resulting in legal liability for the person who commits the tortious act
    - For example, **Fraud** in which one person lies to another, causing harm
- **Contract law**
  - It involves agreed written conditions between two parties

Cybersecurity Laws

- European Council Cyber-Crime Convention
  - Empowers an international task force to oversee a range of Internet security functions
  - Attempts to improve the effectiveness of international investigations into breaches of technology law
- The Digital Millennium Copyright Act (DMCA)
  - A copyright protection is presented in the U.S.1978, which was updated in 1998 as the DMCA specifically to deal with digital object, such as music files, graphics images, data in a database, and also computer programs

In Civil Law System (like Sweden)

- **Procedural law**
  - How the legal system is working
  - A set of procedures for making, administering, and enforcing substantive law
- **Substantive laws**
  - A set of laws that governs how members of a society are to behave Criminal law
  - Hacking: Chapter 4, Section 9c,
  - Computer fraud: Chapter 9 Section 1, providing incorrect or incomplete information, modifying programmes or recording
- **Civil law**
  - Law on copyright in literary and artistic works
  - Contract law

Swedish Constitution Collection - Laws and Documents

Ownership Rights of Employees and Employers

- Ownership is a computer security concern because it relates to the rights of an employer to **protect** the **secrecy** and **integrity** of works produced by the employees
- An employment contract clarifies for both parties an employee's rights to computer products
- Ownership of a **patent**
  - An **employer** has the right to patent if the employee's job functions included **inventing** the product
- Ownership of a **copyright**
  - Similar to patent
- **Work for hire**
  - All work done by employee is owned by employer

Ownership Rights of Employees and Employers

- **Licenses**
  - In return for a fee, a programmer **grants** a company a license to use his/her program
  - The license can include many factors, such as **time period**, number of users, number of systems, and so on
- **Trade secret** protection
  - A company owns the trade secrets of its business-confidential data
  - As with copyrights and patents, an employer can argue about having contributed to the development of trade secrets

there is no registered inventor or author;
there is no registration office for trade secrets

Redress for Software Failures

- Redress = remedy or set right (an undesirable or unfair situation)
- Three example scenarios of bad software
  - Delivered through defective medium
  - Dissatisfaction (not happy)
  - Software malfunction

Always customer a right of remedy here

- If not correct then ask for refund, replacement, fixing
  - Refund: possible
  - Replacement: if this copy damaged, or improved in the meantime
  - Fixing: rarely **legally enforced**; instead, monetary awards for damages
  - **Warranty** states that the vendor will continue to search for vulnerabilities and fix these

Guarantees and returns

ON THIS PAGE

More information about

Guarantees for faulty goods

Affected by Brexit?

Under EU rules, a **trader must repair, replace, reduce the price or give you a refund** if goods you bought turn out to be faulty or do not look or work as advertised.

If you bought a **product or a service online or outside of a shop** (by telephone, mail order, from a door-to-door salesperson), you also have the right to cancel and return your order within 14 days, for any reason and without a justification.

If you're not sure which situation applies to you, you can also try our consumer rights tool to help you understand your rights when you shop in the EU.

This 2-year guarantee is your minimum right, however national rules in your country may give you extra protection.

If goods you bought anywhere in the EU turn out to be faulty or do not look or work as advertised, the seller must **repair** or **replace** them **free of charge** or give you a **price reduction or a full refund**.

You can usually only ask for a partial or full refund when it is not possible to repair or replace the goods.

You might not be entitled to a refund if the problem is minor, such as a scratch on a CD case.

Reporting Software Flaws

- There are several different viewpoint on how flaws should be reported
- **Vendor interests**
  - Vendors don’t want to react to individual flaws
  - Prefer bundle a number of flaw fixes
- **User interests**
  - Would like to have fixes quickly
- Disclosing vulnerabilities encourages vendors to develop and disseminate patches, but patching under time pressure is counter to fixing flaws completely

Vulnerability Reporting

- **Notify vendor** about a vulnerability by **reporter**
- The vendor must **agree** that the vulnerability exists
- The vendor must **inform users** of the vulnerability and any available countermeasures within 30 days/request additional time
- After informing users, the vendor may request from the reporter a **30-day quiet period** to allow users time to install patches
- After that, the vendor and reporter should agree on a date at which time the vulnerability information may be released to the general public
- The vendor should **credit** the **reporter** for locating vulnerability
- If the vendor does not follow these steps, the reporter should work with a **coordinator** to determine a responsible way to publicize the vulnerability

Software Licenses

- Software licensing strategies can be divided into three categories
- Proprietary licensing (closed)
  - agreements govern commercial software packages
  - limit the use of software according to the rights owner's business strategy
- Free and Open Source Software (FOSS) Licensing
  - to maximize openness and minimize barriers to software use, dissemination, and follow-on innovation
- Hybrid Software Licensing (also called dual- or multi-licensing)
  - some of the benefits of FOSS while also permitting creators to employ multiple business models

Computer Crime

- Separate category for computer crime is needed because special laws are required as subjects and objects of crime
- Rules of **property**
  - Most laws have evolved to **recognize data** and computer **services** as property
- Rules of **evidence**
  - Hard to prove authenticity of evidence
  - **Chain of custody**: Law enforcement track clearly and completely the order and identity of people who had access to evidence in an effort to demonstrate that no one had the opportunity to tamper

Computer Crime

- Threats to **integrity** and **confidentiality**
  - Laws have evolved to recognize breaches of privacy and damage to data as crimes
- **Value of data**
  - Digital data, from a legal perspective, is now considered to be worth what a buyer would be willing to pay for it

Examples of Computer Crime

- **Phishing:** deceiving individuals to gain private or personal information
- **Cyber Terrorism:** account hacking, threats and blackmailing towards malware (shut down computer or encrypt their files)
- **Cyber bullying or Cyber stalking:** use electronic communication**,** such as email, social media, or websites for harassing others, online harassment
- **Child Pornography:** making or distributing child pornography
- **Creating Malware:** writing, creating, or distributing malware
- **Denial of Service attack:** overloading a system with so many request it cannot serve normal request
- **Espionage:** Spying on a person or business
- **Fraud:** manipulating data (e.g., changing banking records to transfer money to an account)

Computer Crime Is Hard to Prosecute

- Lack of understanding by courts, lawyers, law enforcement, and jurors
- Lack of physical evidence but digital evidence
- Lack of recognition of assets / Complexity of cases
- Lack of political impact because direct harm to people is harder to identify
- Ages of defendants, who are more likely than many other serious criminals to be juvenile
- Even when there is clear evidence of a crime, the victim (e.g., banks) may not wish to prosecute because they may lose the trust of their customers

Comparison of Law and Ethics

- Ethics are personal choices about right and wrong actions in a given situation
- Doesn‘t have to be much adapted to computer security

Law	**Ethics**
Described by formal, written documents	Described by unwritten principles
Interpreted by courts	Interpreted by each individual
Established by legislatures representing all people	Presented by philosophers, religions, professional groups
Applied to everyone	Chosen personally
Priority determined by courts if two laws conflict	Priority determined by an individual if two principles conflict
”Right” arbitrated finally by court	Not arbitrated externally
Enforced by police and courts	Enforced by intangibles such as principles and beliefs

Ethical Issues in Computer Security

- Ethical issues
  - pertaining to or dealing with morals or the principles of morality
  - pertaining to right and wrong in conduct
  - in accordance with the **rules or standards** for right conduct or practice
  - basis of **trust** and **cooperation** in relationships with others

- Examples:
  - Should companies collect and/or sell customer data?
  - Should IT specialists monitor and report employee computer use?

Examining a Situation for Ethical Issues

- Understand the situation
- Know several theories of ethical reasoning
- List the ethical principles involved
- Determine which principles outweigh others
- Make and defend an ethical choice

- Bases of Ethical Theories
  - Consequence-based
  - Rule-based

Consequence-Based Ethics

- Consequence-based: The teleological theory of ethics focuses on the consequences of an action. Do what results in **greatest good**, least harm
- The outcome outweighs the method
- Two subtypes
  - **Egoism:** self benefits, I do what's good for me
  - **Utilitarianism:** benefits the interests of people in general, I do what's brings greatest collective good
    - For example, designing software to monitor smokestack emissions would need to assess its effects on everyone breathing

Rule-Based Ethics

- Priority is given to following the rules without undue regard to the outcome or effect
- Rules are often thought to codify principles like truthfulness, right to freedom, justice, etc.
- Exist for the benefit of society and should be followed
- Two subtypes:
  - **Pluralism/deontology** (from state, society, religion etc.)
    - stresses fidelity to a sense of duty and generally accepted principles (“never tell a lie”)
  - **Individual** (your own ideas). A set of personal rules complied from religion, experience and reflections

Ethics of Hacking or Cracking

- Ethical hacker (aka white hat hacker). Organizations often employ ethical hackers to **improve** their **system security**
- Ethical hackers adopt a strict code of conduct that protects their relationship with their clients and their client's interests
- Different curricula even propose **training** and **certifications** in order for a hacker to become a Certified Ethical Hacker (C|EH)
- The **C|EH** credentialing and training program provided by EC-Council is a respected and trusted ethical hacking program in the industry

https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/

Certified Information Systems Security Professional (CISSP)

- CISSP is considered as a quality standard in the field of information security
  - This Cyber certification is offered by International Information Systems Security Certification Consortium $(ISC)^2$ which is an international non-profit organization with more than 125,000+ certified members
  - The certification was introduced in 1994 and is the most required security certification on Linkedin
  - The exam is available in 8 languages at 882 locations in 114 countries
  - The certification **meets ISO/IEC standard 17024**
  - After exam, need to have an endorsement in subscribing to the (ISC) Code of Ethics

https://www.isc2.org/Certifications/CISSP

Are Your Ethics Contextual?

- Peoples know that downloading music or software they don't own is illegal, but do so anyway because they don't believe that it hurts the owners of the IP (intellectual property)
- You have an expectation of privacy (lockers, email, etc.) except if there is suspicion of wrong doing
- Somehow, legal doctrine must codify these complicated and contextual courses of action

Ten Commandments of Computer Ethics

Thou shalt not:

- Use a computer to harm other people
- Interfere with other people's computer work
- Snoop around in other people's computer files
- Use a computer to steal
- Use a computer to bear false witness
- Copy or use proprietary software for which you have not paid
- Use other people’s computer resources without authorization or proper compensation
- Appropriate other people’s intellectual output
- Think about the social consequences of the program you are writing or the system you are designing.
- Use a computer in ways that ensure consideration and respect for your fellow humans

Software Protection

- Software developers try to protect their software by using many different protection measures
- **Serial Numbers**: Certain software will ask the user to input a serial number when installing the software. If the number is not inputted the software will not install
- **Activation Keys**: After the software is installed, the user is required to enter some text (the activation key) so that the application will work. This activation key is usually obtained from the seller of the application, it requires product ID of the application
- **CD (or DVD) Copy Protection**: Most companies will create a special program when burning their application to the storage medium which will prevent users from copying the software
- **Hardware Keys**: In this case a hardware device (such as a USB pen) is given with the software and for the software to be functional the USB must be connected to the machine

References

- C. Pfleeger, S. Pfleeger, J. Margulies (2015),*Security in Computing, Fifth Edition*, ISBN: 9780134085043, Pearson Education

- M. E. Whitman, H. J. Mattord (2014). *Principles of Information Security, Fourth Edition*, Cengage Learning

- A. Morin1, J. Urban, P. Sliz (2012), A Quick Guide to Software Licensing for the Scientist-Programmer, PLoS computational biology

Assignment 3

Information Security

Computer Security
1DV700

- You will continue to work with the company Loco News
- Your group now is to investigate the **information security of the company**
- The teaching assistants (acting CTO) will be your contact persons for the company
- **Please interact with TA by email/slack/tutoring sessions**
- Read provided material
  - ISO/IEC 27002 standard
  - Loco New Information Security
  - Other material uploaded on MyMoodle

- **Task 1**
- Study the ISO/IEC 27002 standard
- Discuss all the areas of controls that the standard covers
- Divide them between the group members (each member having at least **two areas** each, possibly with some overlap)

- Write an individual 2 pages summary of the security controls that you are responsible of
- Include only around 8-10 questions to be directed to company personnel in your summary
- Upload pdf

- **Deadline: 12 December**

- **Task 2**
- Interact with TA (CTO) by email/slack/tutoring sessions
- Request any material you need and ask questions
- Prepare the policy document for the specific security control that he/she is responsible for
- Then combine their work and generate one complete INFOSEC (information security) policy document
- All of team members have to agree on the document
- Team leader of the group should submit the 1 report in pdf format
- You can check the policy document template on the following link:

Security Policy Document Template

- **Deadline: 16 January**

Lnu.se