Week 16 - Wednesday

# COMP 4290

# Last time

- What did we talk about last time?
- Review of the first half of the course

# Questions?

# Reveal Secret Messages!

# Review

# Privacy Concepts

# What is information privacy?

- Controlled disclosure
  - Right to control who knows your private data
  - Control is always diminished by sharing data with another party
- Sensitive data
  - Not all data is equally sensitive
  - Different people in different circumstances may disagree about what should be protected
- Affected subject
  - Both people and businesses have private data
  - Increasing privacy (an aspect of confidentiality) often decreases availability

# Computer-related privacy problems

- Broad data collection
- No informed consent
- Loss of control
- Ownership of the data

# Fair information policies

- In 1973, a committee advising the U.S. Department of Human Services proposed a set of principles for fair information practice:
  - Collection limitation
  - Data quality
  - Purpose specification
  - Use limitation
  - Security safeguards
  - Openness
  - Individual participation
  - Accountability

# U.S. privacy laws

- The 1974 Privacy Act is a broad law that covers all the data collected by the government
  - The law is based on the principles from the previous slide
- Laws for data collected by other organizations are for specific areas and not necessarily consistent
  - Fair Credit Reporting Act is for consumer credit
  - Health Insurance Portability and Accountability Act (HIPAA) is for healthcare information
  - Gramm-Leach-Bliley Act (GLBA) is for financial services
  - Children's Online Privacy Protection Act (COPPA) is for children's web access

# Non-US privacy

- The European Union adopted the European Privacy Directive that requires that data about individuals be:
  - Processed fairly and lawfully
  - Collected for specified, explicit, and legitimate purposes
  - Adequate, relevant, and not excessive for the purposes they were collected
  - Accurate and as up to date as necessary
  - Kept in a form that permits identification of individuals for no longer than necessary

# Authentication

# Authentication

- We have already discussed authentication from the perspective of how to do it
  - But what are we really authenticating?
- We could be authenticating any of the following three things:
  - **Individual**
    - The physical person
    - Example: you
  - **Identity**
    - A string or numerical descriptor
    - Examples: the name "Clarence", the account admin
  - **Attribute**
    - A characteristic
    - Examples: being 21, having top secret clearance

# Correlation in data mining

- Correlation is joining databases on common fields
- Privacy for correlation can be improved by making it harder to find links between related fields
- **Data perturbation** randomly swaps fields in records
  - Swapping records indiscriminately can destroy the value of the research
  - It has to add just enough randomness to the right fields

# Aggregation in data mining

- Aggregation means reporting sums, medians, counts or other statistical measures
- As we discussed in the database chapter, these can threaten privacy if we have a very small sample size
- A corresponding problem happens if we have a sample that includes almost but not quite all of the data
- For aggregates, data perturbation means adding small, random positive and negative values to each value, adding noise to the final aggregates
  - If done correctly, the aggregates may still be accurate enough for research purposes

# Privacy on the Web

# Payment

- Credit cards can easily be defrauded since you provide the critical information to stores
- Payment schemes like Venmo and PayPal give more anonymity but do not have the same consumer protection laws

# Site registration

- Virtually every site on the Internet allows (if not requires) you to register with a user name and password so that you can log in
- For the sake of privacy, you should have a different ID and password for every site
  - This, of course, is impossible
- People tend to use one or two IDs (and one or two passwords) for everything
  - Many websites encourage this behavior by forcing you to use your e-mail address as your ID
- In this way, it is easy for anyone with access to multiple databases to aggregate information about you
  - Since your e-mail address is often tied closely to you, they could find out your true identity

# Cookies

- A **cookie** is a small text file kept on your computer that records data related to web browsing
- Cookies can only be read by the site that originally stored the cookie
- The way to get around this is called **third-party cookies**
  - Networks of sites can form an alliance in which they cooperate to track all of your visits to sites in the network
- Visiting a single page could store cookies from every ad on the page (and more!)
- **Web bugs** are images that are usually 1 x 1 pixels and clear
  - They make it impossible to know how many sites could be storing cookies

# E-mail

- Regular mail cannot be opened under penalty of federal law
- Most people do not encrypt their e-mail using PGP or S/MIME
- E-mail travels from originating computer to SMTP server through the Internet to a POP server to the destination
  - Anyone can read and collect your e-mail on the way
- E-mail provides almost no guarantee of authenticity

# Privacy in emerging technologies

- **Radio frequency identification** (**RFID**) **tags** are usually small, inexpensive transmitters
  - They can be attached to almost anything
  - The infrastructure to track you everywhere may soon exist
- Electronic voting has many issues
  - It's hard to engineer a system that correctly counts votes but cannot report how someone voted
  - The software and hardware design for these systems are generally not publicized
  - Internet voting will probably increase
- VoIP
  - Privacy is in the hands of Skype, Zoom, or Teams

# Risk Management

# Parts of a business continuity plan

- A **business continuity plan** covers what will happen if a computer security problem actually happens
- These plans cover big problems
  - Catastrophic situations where large portions of the computer systems don't work
  - They must stop working for a long duration
- Assess business impact
- Develop strategy to control impact
- Develop and implement a plan

# Incident security plans

- An **incident security plan** covers the non-business parts of any security breaches
  - There should be incident security plans even for incidents that are too small to fall under a business continuity plan
- Such a plan covers:
  - The definition of an incident
  - Who is responsible for taking charge
  - What the plan of action is
- Such a plan must consider:
  - Legal issues
  - How to preserve evidence
  - How to record the progress in executing the plan
  - How to handle public relations

# Risk terminology

- **Risk** is the potential for a problem
- Risk is characterized by three factors
  1. Loss associated with the event
     - **Risk impact**
  2. Likelihood that the event will occur
     - A likelihood of 1 means there is a problem
  3. The degree to which we can change the outcome
     - **Risk control** is reducing the risk
- **Risk exposure** = risk impact × risk probability
- We can **avoid**, **transfer**, or **assume** the risk, depending on the tradeoffs

# Risk analysis

- **Risk analysis** is examining a system to find vulnerabilities and the harm they could cause
- **Risk leverage** =

$$\frac{(\text{risk exposure before reduction}) - (\text{risk exposure after reduction})}{(\text{cost of risk reduction})}$$

- Steps of a risk analysis:
  1. Identify assets
  2. Determine vulnerabilities
  3. Estimate likelihood of exploitation
  4. Compute expected annual loss
  5. Survey applicable controls and their costs
  6. Project annual savings of control

# Risk analysis pros and cons

| Pros | Cons |
| --- | --- |
| Improve awareness | False sense of confidence |
| Relate security mission to management objectives | Hard to perform |
| Identify assets, vulnerabilities, and controls | Done once and then forgotten |
| Improve basis for decisions | Lack of accuracy |
| Justify expenditures for security | |

# Physical security

- Natural disasters
  - Flood
  - Fire
  - Everything else
    - Insure and backup
- Power issues
  - Power loss
  - **Uninterruptible power supplies** (UPS)
  - Surge suppressor
- Human vandals
  - Unauthorized access
  - Theft

# Disposing of sensitive information

- Shredding paper documents
- Overwriting magnetic data
- Degaussing
- Van Eck phreaking safeguards

# Backups

- Everything should be backed up, always
- A complete backup covers the current state of all data
- Revolving backups keep the last few complete backups
- A selective (or incremental) backup stores only the files that have changed since the last backup
- Ideally, you should have an offsite backup of all your data in case of fire or flood
  - Backing up your critical data on a USB or external HD and keep it at home or school or vice versa is a good idea for you guys

# Legal and Ethical Issues

# Copyrights, patents, and trade secrets

| | Copyright | Patent | Trade Secret |
|---|---|---|---|
| **Protects** | Expression of idea, not idea itself | Invention, the way something works | A secret, a competitive advantage |
| **Protected object made public** | Yes, all about promoting publication | Filed at patent office | No |
| **Requirement to distribute** | Yes | No | No |
| **Ease of filing** | Easy, do it yourself | Complicated, usually needs lawyers | No filing |
| **Duration** | Life of author + 70 years, 95 years for corporations | 19 years | As long as you can keep it secret |
| **Legal protection** | Sue if unauthorized copy sold | Sue if invention copied | Sue if secret improperly obtained |

# Criminal vs. civil law

| | Criminal Law | Civil Law |
|---|---|---|
| **Defined by** | Statutes | Contracts<br>Common law |
| **Cases brought by** | Government | Government<br>Individuals and companies |
| **Wronged party** | Society | Individuals and companies |
| **Remedy** | Jail or fine | Damages, usually money |

# Who owns what?

- If you are paid to develop software, the company owns the software
- If you write code in your free time, it is possible that your job can still claim a piece of it (especially if you used any of their hardware or software)
- If you are a consultant who writes a program for a client and then further develop it yourself, it's complicated
- Often covered by your contract

# Patents and copyrights

- The inventor is the entity that owns the patent
  - Who is the inventor?
  - It matters whether your employer files the patent or if you do
- In general, when you create something, you hold the copyright
- The exception is a **work for hire** situation which exists when some or all of the following apply:
  - The employer has a supervisory relationship
  - The employer has the right to fire you
  - The employer arranges for the work to be done before it is created
  - A written contract states that the employer has hired you to do certain work

# Reporting flaws

- Researchers and users should report flaws to companies so that they can be fixed, but there is disagreement about how public the reporting is
- Developers want the vulnerabilities secret as long as possible so that a small number of patches can fix many vulnerabilities
- Users want more pressure on developers to fix problems quickly
- Researchers have suggested guidelines to reach a compromise between these two groups

# Computer crime

- Computer crime needs new definitions for crime
  - Traditional crime focuses on crimes against people (murder) or crimes against objects (theft)
- Copying software is not traditional theft because no tangible object is missing
- Computer trespassing has a similar problem
- Evidence of computer crime is difficult to authenticate

# Computer criminals are hard to catch

- Much of the crime is international, and there are no international computer laws
  - Although many countries cooperate to catch criminals, there are safe havens where they cannot be arrested
- Technical problems make them hard to catch
  - Attacks can be bounced through many intermediaries, each requiring their own search warrant
  - The right network administrators has to be given the warrant (and he or she might not keep good records)

# Cryptography and the law

- Many countries have controls on the use of cryptography
  - Governments want cryptography they can break so that they can catch criminals
  - Laws are hard to enforce for individuals, especially now that the instructions for coding up AES are widely available
- Until 1998, export of cryptography in the US was covered under laws preventing the export of weapons of war
  - This definition changed, although there are still export restrictions
  - There were never any restrictions on the *use* of cryptography in the US
  - Absurdly, the government said that object code was subject to export restriction, but printed source code was an idea and therefore not

# Escrowed cryptography

- The government made proposals to relax export rules for **escrowed encryption**
  - With escrowed encryption, the government is given copies of all the keys used to protect all transmissions, but promises to use them only with court authorization
- Three well known proposals for these systems were Clipper, Capstone, and Fortezza
- These proposals were not adopted because of public distrust of what the government might do with all the keys

# Laws vs. ethics

- Laws:
  - Apply to everyone
  - Courts determine which law applies or if one supersedes another
  - Laws and courts define what is right (legal) and what is wrong (illegal)
  - Laws are enforced
- Ethics:
  - Are personal
  - Ethical positions often come into conflict with each other
  - There is no universal standard of right and wrong
  - There is no systematic enforcement for ethical decisions

# Examining an ethical choice

1. Understand the situation
   - Learn all the facts about the situation first
2. Know several theories of ethical reasoning
   - There may be many ways to justify different choices
3. List the ethical principles involved
   - What different philosophies could be applied?
4. Determine which principles outweigh others
   - This is the hard part where you have to make a subjective valuation

# Ethical breakdown

| | Teleology (Consequence-based) | Deontology (Rule-based) |
|---|---|---|
| **Individual** | Based on consequences to the individual (**egoism**) | Based on rules acquired by the individual from religion, analysis, or experience |
| **Universal** | Based on consequences to society (**utilitarianism**) | Based on universal rules that everyone can agree on (but there are very few of these) |

# Upcoming

# Next time…

- There is no next time!

# Reminders

- **Final exam:**
  - **Wednesday, December 10, 2025**
  - **12:30 – 2:30 p.m.**
- Finish Project 3
  - Remember to document your attacks and explain your own system