COSC130 Lecture notes

Week 1

Some Quotes

Always assume someone will fuck you up dawg

Cybersecruity through obscurity is very bad practice - If you are relying on someone not knowing your system or how to attack it, they will figure it out and you will be DESTROYED.

We must except that today we understand that we have to accept some uncertainty, we cannot run completely unhackable services

Amateurs hack systems, professionals hack people

If something is for free, you're not the customer, but the product

What can go wrong

Ransom attack - If an attacker can get access to your computer they can encrypt all your data and lock your computer down until you pay for the decryption key, if you don't, they can delete it all. Never a good idea to pay ransom, as you can assume you'll get your stuff back

Identify Theft - somebody learns enough personal information about you that they can do things in your name pretending to be you, get loans, etc

Digitally Disappearing - It is possible to remove people from pics and videos

Deepface - the opposite of disappearance, create fake videos, recordings of you, etc

What is cybersecurity?

Your system is only as secure as your weakest link.

Computers require automated software tools to protect data and other resources(assets)

Use of networks and communication links that requires measures to protect data during transmission… THE INTERNET can be used as an entry point to your system, you can be hacked and data can be taken, intercepted, etc.

Define Cyberspace
Cybersecuiry refers to any technology measures of preventing cyberattacks or mitigating Their impact - IBM

Safety is about natural disasters including earthquake, floods, etc also know as benign attacks

Security is concerned with malicious actions designed to cause harm.

Cybersecurity is well known for inconsistent terminology, therefore understanding the concepts and not get confused with the terminology. Or Information(data) security plus system security

Computer Security - Generic name for the collection of tools designed to protect data and other resources(aka assets) and to thwart hackers.

Data security - Refers to the protection of data from unauthorized disclosure, destruction and alteration.

Network (Internet) Security - Deter, provent, detect and correct violations that involve transmission of information

Data - is basically what you stored in your computer and information is what can be learned from that data.

We need a systematic way to identify sec requirements and how they can be satisfied

Security services - Goals, objectives, what we want to achieve
Security mechanisms - how we can achieve them
Security attack - ways in which adversaries can harm the system
Security vulnerabilities - weaknesses in the system that facilitate attacks

Cybersecuiry is about preventing security attacks, or failing that, detecting and mitigating and recovering from them

Security attack - Any action that compromises the security of the system and of information or data owned by an organization.

Security Mechanisms - A process or a device that is designed to detect, prevent recover from a security attack

Security service

A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. tTHe services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service.

CIA Triad:

Confidentiality - data should be accessible only be authorized users

From stallings Crypto book

Confidentiality covers two related concepts:

- Data confidentiality - assume that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy - assume that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Integrity - data can be modified only by authorized users (Should also mention the system not just data)

From stallings Crypto book

Integrity covers two concepts

- Data integrity - Assures that information (both stored and in transmitted packets) and programs are changed only in specified and authorized manner.
- Systems integrity - Assures that a system performs it intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

Availability - computer assets are available to authorized users when needed

From stallings Crypto book

Availability Assures that systems work promptly and services and data is not denied to authorized users.

Authenticity - the origin of an electronic document can be correctly identified

From stallings crypto book

Authenticity - The property of being genuine and being able to be verified and trusted, confidence in the validity of a transmission, am message, or message originator. This means that users are who they say they are and that each input arriving at the system came from a tufted source.

Non-**Repudiation** - neither the sender nor the receiver of the message can deny the transmission

Anonymity - individuals can remain anonymous (if they choose to do so)

Accountability - The security goal that generates the requirements for actions to be traced uniquely to that entity. This supports **non-repudiation, deterrence, fault isolation, intrusion detection** and **prevention** and after action recovery and legal action. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or aid in transaction disputes.

Service is what we want to achieve

Security Mechanisms

There is no single security mechanism that can support all the required security services, you should use all the mechanisms in combination, or atleast all that apply.

Cryptographic techniques do provide many of security mechanisms in one.

Access Control - We can say that this file can be read by these people access to these people and so on.

Backups - We can and always should make back ups

Traffic Padding - So that nobody can monitor traffic between us and other people, sometimes it is enough to know that two people are communicating.

And so on, ADD ONES FROM TEXTBOOK

From recommended reading
Chapter 1 Introduction
C. P. Pfleeger, S. L. Pfleeger and J. Margulies. (2015). Security in Computing, 5th Edition, Pearson Education.

Defences

Proactive approaches

- Preventative controls eg Firewalls, stops a hacking from entering your system
  Ensure that an attack against a target is not possible or not successful

- Deterrence eg 2fa, make it hard for the attacker
  Merely increases the effort for an adversary, aiming to make the target unattractive.

- Deflection eg deploying honeypots on your system, make other targets look pretty but obtain no useful information.
  The goal of the defender is to redirect the efforts of an adversary to another target

Reactive approaches

- Detection Controls eg logs, see the attack as it happens or post mortem
  Can focus either on real-time notifications or on documentation.

- Mitigation eg Network segmentation, not have one network of the whole company in one accessible place, break it al up with different access
  Reduces the impact of an attack. A frequently deployed mitigation control is network segmentation.

- Recovery eg backups, self explanatory
  Helops revert the effects of an attack as fast as possible and resume operation.

Secruity Design Principles

Continuous improvement - people say that security is a process and not a state

Least privilege - Lowest amount of access needed by users

Defense in depth - A single mechanism should not be relied on, multiple mechanisms to provide security

Open design - mechanism should not rely on the fact that adversaries do not know their design - no security by obscurity

Chain of control - Only trustworthy software should be executed whenever possible and non trustworthy components should be restricted - An adversary can attack you not directly but from your supplier

Transitive Trust - If A trusts B and B trusts C then A may also trust C - if you trust somebody and they trust somebody else then you will trust them

Deny by default - If you have to have a permission to do something if nothing is specified it is denied

Trust but verify - only using trustworthy suppliers and software bt still verify

Separation of duty - If something is critical it will not be done by the same person in the company you will split it between different sections or people

The principle of the least astonished - Systems should be easy to use, people should be able to use the security system. They should be intuitive in design and in consequence

Threats and attacks

Threat

a potential for violation of security which exists when there is a circumstance, capability or action or event that could breach security and cause harm. That is a threatt id possible danger that might exploit a vulnerability.

Attack

An assault on a system's security that derives from an intelligent threat is an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system.

Passive attacks - do not change anything on a system and are harder to detect, eavesdropping on a system, monitoring traffic and flows

Active attacks - you modify the system, the data of configuration

- Masquerade of one entity as some other
- Reply previous messages
- Modify messages in transit
- Denial of service

Who is attacking

If you want a successful attack then an attacker needs three things

- Method of how to attack
- An opportunity
- And a motive

Looking at the below motives can tell us whats going on.

Amatuers

Script Kiddies - Usually have limited or no skills, use readily available tools

Hackitivsts - motivated by ideology, fighting against climate change, etc Want to create publicity to further their cause

Rouge hackers - motivated by curiosity but still doing illegal things.

Hacking for **personal gain** - Normally still an amatur, usually for financial gain

Professional

White hat hackers - people who are ethical hackers who are doing it to help improve systems

Grey hats - kinda have good intentions but are still not doing it legally

Black hats - are malicious

Corporate spies - Want to obtain commercial secrets

Cyber criminals - financial gain, ransom attacks, exploiting

Nations state - want to influence other states or extend their power, well resourced and capable of creating advanced persistent threat

Another way to look at attackers

- Unauthorized users
- Authorized users having unauthorized access
- Authorized users using authorized access to obtain access to data they should not have access to.

Vulnerabilities

Two preconditions for a successful attack

Exposure - The system must be exposed to the attacker, they must be able to reach a system other wise they cannot attack

Exploitability - The system has to contain a vulnerability otherwise it cannot be successfully attacked

Vulnerability - Not every weakness is a vulnerability. vulnerability is a weakness that can be exploited to cause harm. And the weakness can be in the system design, or the implementation, maybe made with a bug or in management, maybe the system was misconfigured.

Zero day vulnerability -

Talking about exposure and exploitability, together, gives us the likelihood of the attack of the attacker, how much exposure there is and how much exploitability there is. Anotherimportant variable is the impact of the attack. The likelihood and the impact together determine the severity of the risk

Risks can be:

- Avoided
- Mitigate - by reducing the likelihood or the impact
- Transferring, for example purchasing insurance or externalizing the cost, passing it onto the users of the system
- Accepted, for example just knowing its there and covering the cost when it comes up

Stages of an attack

Reconnaissance - First the attacker needs to learn about you or the company, what software are they using to learn emails of employees for hacking
Weaponization - weaponizing something like a word doc to embed malware
Delivery - could sent an email attachment is a typical one, usb flash drive if you cant do it over the network, websites, links.
Exploitation - Now the malware is there, it runs,
Installation - when the malware is able to hack into the authentication control system and allow access to the adversary to the system
Command and control - similar to above, connecting hacked computer to own server and now have access
Actions - can do whatever they want to do, read commercial secrets, delete data.

If they are able to conduct an attack like this, they are able to create a persistent threat on the company.

Pre quiz questions I want to be able to answer

Define cyber security - Cybersecurity refers to any technological measures used to prevent attacks or mitigate their impact.

What is Information security - The Three information goals with infosec, they are the triad bruh
Name da triad and explain da triad bruh

- Confidentiality - prevent unauthorized information gain
- Integrity - Prevent or detect unauthorized modification of data
- Availability - Prevent unauthorized deletion of disruption

These apply to both data at rest and data in transit

Authenticity - prevents actors from impersonating someone by providing a means to verify.
Nonrepudiation - Is a strong form of authenticity, which prevents actors from deny they sent a message, good for law and courts.

What is systems security - is designing systems so that they protect the data stored on them or are able to continue providing their normal service.

What is the difference between safety and security - Safety is making sure systems can remain up and running during times of natural disasters, security refers to human threats in particular malicious acts such as cyber attackers or random attacks like phising.

Security Service - Is a service used to enhance or provide help in protecting or mitigating attacks on the system and to make sure data remains safe and systems function as intended, they deploy one or more security mechanisms to achieve this

Security mechanisms - Are techniques or physical devices used in helping to protect data or system services. Normally used in tandem with one another to create defense in depth

Name as many security mechanisms (Briefly describe)

- Cryptographic techniques - highly useful tools for encrypting data, proving signatures, etc
- Access controls - preventing who can access which data or which parts of a system
- Traffic padding - protecting against actors from monitoring traffic between people

What is a threat - A threat is something that could stop your system from running as usual or your data being compromised or identity stolen, many different threats.

Security attacks - Attacks are malicious assaults on a system on individual to gain access to data or stop a system from usual process.

Name as many security attacks (Briefly describe)

- DDos - taking down a system or services by flooding it with requests
- Ransome - gainiing access to your data and locking it up with encryption and forcing you to pay money if you want it back
-

Name as many different attackers, explain?

- Script kiddies - use pre made tools often shored on online forums, easiest to detect but can also cause serious damage
- Hacktivists - Motivated by their cause, often trying to drum up media attention and spotlight on their cause
- Rogue hackers- Simply curious actors seeing either what they can do or how things work.
- Cyber criminals - Exploiting people, companies, systems for financial gain, often classified as professional hackers
- State actors - Used in cyber warfare, well funded, can carry out advanced persistent threat attackers, usually aimed at other state actors to gain secrets or shut down services or infrastructure
- White hat - Ethical hackers who find problems in systems and can help fix them
- Grey hat - Not good nor bad but not legally hacking
- Black hat - hackers with malicious motives
- Corporate spies - looking for commercial or trade secrets

Name proactive defenses and reactive defenses and explain each

Proactive

- Preventive controls ensure that an attack against you is not successful but manipulating exposure and exploitability
- Deterrence merely makes it harder for an adversary to gain access of control, 2fa is a fine example of this
- Deflection - aims at providing a more lucrative looking target on your system to draw attackers to it instead of critical information, honeypots bby

Re

- Detection controls - provide live monitoring of the hack to see what they are doing or helpful in post mortem when analyzing what went wrong
- Mitigating - Reduce the impact of an attack usually by splitting the network up so systems are not easily connected or new access would be needed to be gained
- Back up - Keep back ups so incase of attack you can restore and return services quickly

Name Some security design principles and explain

- Continuous improvement - security is a process and not a state
- Defense in depth - use multiple mechanisms in tandemjh to provide better coverage and more security
- Least privilege - users should only be able to access what is needed as to control the access points into your system

- Open design - You should not build a system that tries to hide its weaknesses, someone will find them.
- Chain of control - only use trustworthy software whenever possible
- Transitive trust - If A trusts B and B trusts C, A can also Trust C, build a strong trustworthy network
- Deny by default - unless needed, no access should be granted
- Trust by verify
- Separation of duty - Critical task should be split up across different people or teams as to make it harder for a critical attack on a single system or person, or place
- The principle of least astonishment - systems should be intuitive so as the end user with no experience can understand what is going on, what is happening, and what security problem may arise.

Name the steps for hacking into a secured network

- Reconnaissance - Research target
- Weaponization - Loading a word document or file with the malicious software
- Delivery - transmitting the weapon either via email, usb drive, etc
- Exploitation - after it is delivered the software can be triggered and begin the attack
- Installation - installs remote access for the hacker
- Command and conquer - Compromised host connects to hackers server where they have complete control
- Actions - intruder can take whatever actions they want in this last step

Week 2:

Ethics

“Informally ethics is a system of moral principles that can be adhered to in order to so what is right and good”

Our model for analysis:

1. It is always possible to identify a person or group that makes a decision
2. Those who are making decisions understand that they are making a decision and have the authority to do so
3. Decision makers are not coerced into making a particular decision
4. Each decision is made in isolation independently of the other decisions
5. Decision makers are aware of constraints under which they are making decisions.

Metaethics - the study about ethics
- Where do our ethics come from
- Are ethics innate or learnt

Normative Ethics - determining moral standards that regulate right or wrong

Applied Ethics - Examine controversial decisions.

Objectivist - Born knowing right from wrong
Relativists - learn ethics from our surroundings and culture

The golden rule - “Do unto others as you would have them do unto you”

To decide if something is morally correct or not, one has to ask what would happen if everyone was doing it

Ethical theories

Teleological - Consequentialist ethics. The rightness or wrongness of an act is a function solely of the consequences of the act.

- An act is morally right if it has a good consequence
- Results based thinking
- Ends justifies the means

Utilitarianism focuses on happiness of the greatest number for the outcome

The main advantage of consequentialism is that uses a simple and objective algorithm the calculation of the utility can easily be automated

The main criticism is that always subjecting an individual's right to a group interests can be seen as authoritarian.

Deontological - duty, obligation or rules based ethics. The action is more important than the consequences.

- Kant
- Kant believes we have been given a privileged palace in the world because we can reason

3 rules

- Always act on the maxim or principle which can be universally binding. Without exception, for all humans
- Golden Rule - Would I be harmed if someone took the same action against me/
- - Everyone should treat others as an end in themselves as people who deserve respect and dignity rather than merely a means to an end.
-

John Rawls, american philosopher
“Since we are not objective but rather tend to subconsciously act in our self interest, we need to apply the veil of ignorance: If I was blind to my position, I didn't know my gender, race, social class, nationality - what rule would I then be willing to adopt as universal in this situation?

The difference Principle - By applying the veil of ignorance, we act to improve the condition of the leader favored people in a society.

Critiques

- Too idealistic - for example assuming that others are trustworthy
- Too inflexible - the duty to be truthful
- Rawls insisting on equitable solutions

Virtue ethics - emphases good habits, good character.

- Applied to human beings, virtue is an optimal mean that avoids excesses either way.
- Not enough to do the right thing, it has to be with the right intention
- It does not require self sacrifice
- Actions are aligned with their values
- You can continue to improve through your life
- Good judgment emanate from good character and not from being a good person is not about following the rules
- Intent intent intent

Critues

- Reality is more complex then being able to use a model
- Individual level is not an appropriate level for achieving morality
- Person character is not fixed and unchanging as people behave differently in different situations
- Aristotle's virtues ethics is Western and male centric ie Courage.
- Circular reasoning - one acts according to their and actions build character
- It is selfish for an individual to focus on their own virtues and well being instead of the overall good.

Principlism - Derived from deontological ethics

- One has to honor his duties, unless there are more pressing duties that are in conflict with it

  Originally written for guidelines for human subjects in bio labs

  4 ethic principles
  - Respect for persons - research subjects who voluntarily submitted, respect them as people who are in control and make decisions for themselves
  - Beneficence - Do not harm, Maximize probable benefits and minimize the probably harms
  - Justice - Each person has equal consideration in how to be treated
  - Respect for law and public interest - engage in legal due diligence, be accountable for your actions

Human Rights

Cybersecurtiy technology are intended to protect individuals from cyber crime, however in doing so cybersecurity technologies may conflict with the human rights of individuals

Cyber crime:
Cybertrespass - unauthorized access
Cybervandalism - corrupting/disrupting data and /or processes
Cyberpiracy - illegal reproduction and distribution of content
Computer fraud - deception for financial gain

Methods use to fight cyberpiracy include secret access to computer systems and interception of data which is exactly what cyber trespassing refers to.

According to hildebrandt the affect rights are:

- Privacy
- Data protection
- Non-discrimination
- Due process
- Free speech

Violating a human right defeats the purpose of a right, however it is very likely that human rights will be in conflict with each other and in conflict with cyber security goals

In practice it may be possible to distinguish between the core elements of a right which must be preserved. Peripheral elements can be sacrificed if it doesn't interfere with a core right.

Ethics of Risk
(There is a case study I watched in the lecture that sets the scene for the below writing)

Expected Utility maximization - the right action is the one that maximizes the aggregate expected utility

- Policy A - It is expected that 0.6 patients will die
- Policy B - Expected financial loss (disutility) of $140,140,000

Maximin Rule - The utility of a mixture of potential outcomes is equal to the lowest utility associated with any of these outcomes

- Policy A - in the worst outcome, one patient will die
- Policy B - in the worst outcome, financial loss is 400,000,000

Deontological theory - If it is morally prohibited to perform a certain action then this prohibition extends to all mixtures in which this action has non-zero probability.

- Policy a - Prohibited as a patient dying has a non zero probability
- Policy B - Not prohibited, We do this.

Rights based Theory - If someone has a moral right that a certain action not be performed then this right extends to all mixtures in which this action ahs non zero probability

- Policy A - Prohibited, as a patient dying has a non zero probability
- Policy B - Not prohibited.

Probability limit for risk-deontological theories: “Each prohibition of an action is associated with a probability limit. The prohibition extends to a mixture that contains the action id and only id the action has, in the mixture a probability that is above the probability limit,

Contractualism - Minimax Compliant Principle - When we would not be violating any moral constraint we are morally required rto act in the way that minimizes the strongest individual complaint.

> Since the complaint against loss of life is greater then the complaint against paying the ransom, we should choose policy B.

Ex ante Contractualism - compares complaints in terms of expected harm.

> We compare a very small probability of loss of life of loss of 140$

Ethics Recap

Virtue ethics

- Quest to understand and live a life of moral character
- We acquire virtue through practise
- Practice being honest, brave, generous, etc develops and honorable and moral character
- By honing virtuous habits, you are more likely to make the right choice when faced with ethical challenges
- Not enough to do the right thing, it has to be with the right intention
- In Virtue ethics you analyze a person's character in the choices they make, do you want to be a person who is seen as “x”?

Deontology

- Rules to distinguish right from wrong
- Ethic actions follow universal moral laws, such as don't lie, don't steal, dont cheat
- It only requires that you follow the rules and do your duty
- Fits well with natural ethical intuitions about what is or isn't ethical
- Deontology doesn't require you to weigh costs and benefits of a situation, which avoids subjectivity and uncertainty as you only have to follow the set rules
-

Utilitarianism

- Ethical theory based on determining what is right or wrong from outcomes
- Form of consequentialism
- The most ethical choice is the one that produces the greatest good for the greatest number
- The only moral framework that can be used to justify military force or war
- Most common way to approach moral reasoning in business due to the weighing of cost and benefits
- Due to the unpredictability of the future, its hard to know if the consequences of our actions would be good or bad
- Has trouble accounting for what is just or individual rights
- Most reason based approach to determining whats right or wrong

Week 3 - Computer and cybersecurity ethics & code of conduct

- Origin of computer ethics
- Ethical issues in IT and cybersecurity
- Code of conduct

Aristotle revisit:

To be a good human being of good character, extremes are not good, be the middle ground

Animals

- In simplest animals, the information is not stored but rather triggers immediate reaction (Reflexes)

- In more complex animals information is retained and affects future behaviors. Animals learn which allows them to adapt to the changing environment

- In the more sophisticated animals, this translate into memories, recognition and processing of complex patterns and situations and decision=making.

- Humans as the most sophisticated animals are capable of theoretical and practical reasoning which allows them to evaluate different possibilities and make choices.

- Aristotle's model of animal behavior is suggestive of automata theory and ai.

Wieners Ethics

Prof Weiner argues that computing and fundamentally different from other technologies
He anticipated that the time will come when we would be surrounded by computers that will constantly collect and provide data.

Weiner's model of animal behavior is strikingly similar to that of aristotle. He also argues that an animal's purpose is determined by its physiological structure.

Wieners Great principles of justice

In order to capture conditions for human beings to flourish and full their purpose weiner defines three great principles of justice and an additional principal to limit the negative influence of government nad society

The principle of freedom

- 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

- 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

- A good will between man and man that knows no limits short of those of humanity itself

The principle of minimum infringement of freedom

- What compulsion the very existence of the community and the state may demand must be exercised in such a way as to produce no unnecessary infringement of freedom.

Origins of Computer Ethics

Wiener argues that the invention of computing machines in 1940s introduced new ethical challenges

Weiner argues that in order to understand human society, one needs to understand its internal messages and communication, computing machines with the ability to fundamentally change internal messages and communication can also profoundly transform society.

‘Perhaps I may clarify the historical background of the present situation if I say that the first industrial revolution. The revolution of the dark satanic mills was the devaluation of the human arm by the competition of machinery. There is no rate of pay at which a pick and shovel laborer can live, which is low enough to compete with the work of a steam shovel as an excavator. The modern industrial revolution (ie The computer revolution) is similarly bound to devalue the human brain, at least in its simpler and more routine decisions. The answer, of course, is to have security based on human values other than buying and selling. To arrive at this society we need a good deal of planning and a good deal of struggle…’(Weiner, 1948)

Methodology for Applying Computer Ethics in Practice

Bynum proposed a methodology for applying computer ethics based on Wiener principles [Bynum 2000]. The methodology includes the following guidelines:

▪ Human Purpose. Ethical judgments and practices must be grounded in the overall purpose of human life: society and the rules which govern its members must make it possible for people to flourish -- to reach their full potential in variety and possibility of action.

▪ Principles of Justice. The Principle of Freedom, the Principle of Equality and the Principle of Benevolence should govern every person's judgments and practices; and society must neither permit nor impose unnecessary limitations upon individual freedom.

▪ Unambiguity. The meanings of ethical concepts and rules, in a given situation, should be clear and unambiguous. If they are not, one must undertake to clarify their meanings to the extent possible.

▪ Precedent and Tradition. New ethical judgments and cases should be assimilated into the existing body of cases, rules, laws, policies and practices.

Based on those guidelines, Bynum [Bynum, 2000] proposed the following steps for solving issues in computer ethics based on Wiener's principles.

❑ Step One: Identify an ethical question or case regarding the integration of ICT into society.

❑ Step Two: Clarify any ambiguous concepts or rules that may apply to the case in question.

❑ Step Three: Apply existing principles, laws, rules, policies and practices which govern human behavior in the given society. Use precedent and traditional interpretation in such a way as to assimilate the new case or policy into the existing set of social policies and practices. If a given case or question does not fit easily into the existing set of rules and policies, then one must either (1) make adjustments in the old policies and rules to accommodate the new case, or else (2) introduce a totally new policy to cover the new kind of case.

Code of conduct

"What constitutes ethical behaviour for those who work with or have access to information systems?" [Stallings, 2017]

1. Computer technology amplifies both the volume of data/activities and opportunities for misuse:
◦ record-keeping on an unprecedented scale, particularly regarding information about individuals
◦ the ability to collect and organise fine-grained personal information
◦ the ability to conduct data mining and machine learning, as well as data matching
◦ empowers individuals to do harm

2. New technologies and concepts are emerging that did not exist before and for which no ethical rules already exist, such as databases containing personal information, Web browsers, chat rooms, cookies, AI, cloud computing, etc.

3. Individuals with computer knowledge and skills bear extra ethical responsibilities and obligations.

Gotterbarn [Gotterbarn, 1999] proposed a hierarchy of professional obligation adapted and summarized in the table below

Level 1 Humanity
- Integrity -
- Freedom -
- Justice -
- Fairness …

Level 2 Professionalism
- Higher order of care Societal wellbeing …

Level 3 Each Profession
- Profession-specific standards and professionalism Standards in profession's code of ethics

A Code of Conduct

Many professional societies have their own Code of Conduct. According to Gotterbarn [Gotterbarn, 1999], a software engineering code of conduct serves the following functions.

1. Inspiration “It might be designed to be inspirational - either for ‘positive stimulus for ethical conduct by the practitioner’ or to inspire confidence of the customer or user in the computing artifact and confidence in its creator. Unfortunately, inspirational language tends to be vague, limiting the code’s ability to help guide professional behavior.”

2. Guidance “Historically, there has been a transition away from regulatory codes, designed to penalize divergent behavior and internal dissent, toward more normative codes, which give general guidance. Although a professional can use a normative Code to examine alternative actions, such codes are only a partial representation of a profession’s ethical standards. Because the use of normative codes requires moral judgment on the part of the professional, they should not be considered a complete procedure for deciding what is right or wrong

3. Education “Codes also serve to educate both prospective and existing software engineers about their shared commitment to undertake a certain level of quality in their work and their responsibility for the well-being of the customer and user of the developed product. Codes also serve to educate managers of software engineers, and to educate those who make rules and laws related to the profession, about expected behavior. Managers’ and legislators’ expectations will affect what is asked of software engineers and what laws are passed relating to software engineering, respectively. Directly and indirectly, codes also educate management about their responsibility for the effects and impacts of the products developed. Codes also indirectly educate the public at large about what professionals consider to be a minimally acceptable ethical practice in that field, even as practiced by nonprofessionals.”

4. Support “Codes provide a level of support for the professional who decides to take positive action. An appeal to the imperatives of a code can be used as counterpressure against others’ urging to act in ways inconsistent with the Code.”

5. Deterrence/discipline “Codes can be a means of deterrence and discipline. They can serve as a formal basis for action against a professional; for example, some organizations use codes to revoke membership or suspend licenses to practice. Because codes usually define in detail the minimal behavior for all practitioners, the failure to meet this expectation can be used as a reasonable foundation for litigation.”

6. Public image “Codes have been used to enhance a profession’s public image. They prohibit public criticism of fellow professionals, even if they violate some ethical standard.

Week 4 - Law

The impact of law on technology.

Law and technology consequences:

- Importance of the 4th industrial revolution
- beyond disruption for clients/customers and lawyers
- Harnessing Generative AI in new innovative ways
- Legal challenges of intellectual property, data privacy, employment confidentiality, competition, governance
- The importance of information governance

  Corporate governance == the board of directories.

  TAQKE NOTES ON THE THREE PILLARS ARTICLE - Michael adams

Legal directors duties

- Act honestly
- Act to avoid conflicts of interest
- Act not to use confidential information
- Act not make a profit above entity
- Act with care and diligence

Privacy IT and Regulation

“the system of rules which a particular country or community recognises as regulating the actions of its members and which it may enforce by the imposition of penalties” (OED) •

Tendencies
– Support the status quo
– Slow to change

Science - a systematic investigation of nature to create knowledge of our universe: hypothesis, test, evaluate, restate hypothesis

Rate of change is speeding up

What is privacy?

Personal information is what?

- Is just the information that can identify an individual

Australian privacy principles

1. Open and transparent management of personal information
    - Corporations must look after the data they store from you and have a clear use for storing it.
2. Anonymity and sudo anonymity
    - Individuals must have an option to not identify themselves.
3. Collection of personal information
    - You must not collect persona; information of individuals unless consented
4. Dealing with unsolicited and personal information
    - Lawful and fair means of collection, i.3e point 3
5. notification
    - At the time of collection of information you must inform of what you are doing
6. Disclosure of information
    - You cannot disclose the information for other purpose other then consented
7. Marketing and how information can be used in marketing
8. Cross boarder disclosure
9. Disclosure
10. The integrity of personal information
    - Entities must keep your information safe and it must be accurate
11. Similar to 10
12. Access to personal information
    - Entity can only allow access to you or anything under the consent
13. You can correct the information

Week 5 - Privacy

Common law states:

“The right of people to lead their lives in a manner that is reasonably secluded from public scrutiny, whether such security comes from a neighbors prying eyes, an investigators eavesdropping ears, or a news photographers intrusive camera”

Australian privacy law and practice (ALRC Report 108):

Information privacy, which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as ‘data protection’;

Bodily privacy, which concerns the protection of people’s physical selves against invasive procedures such as genetic tests, drug testing and cavity searches; Privacy of communications, which covers the security and privacy of mail, telephones, e-mail and other forms of communication; and

Territorial privacy, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.

IN THIS UNIT WE WILL ADOPT THIS DEFINITION

“Privacy may be defined as the claim of individuals , groups or institutions to determine when, how and to what extent information about them is communicated to others.”

In other words, privacy is right of individuals to control personal information about themselves.

Types of Attributes in a datasets(used for attacks):

Unique ID - Driver's license, medicare number, Passport number, etc
Quasi ID - City you live, Age, Sex
Non-sensitive Attributes - marriage status, etc
Sensitive Attributes - Financial info, criminal info, medical info, etc

We can classify the main attack types into 2 broad categories:

1. Linkage Attack Models:
    1) Record linkage, where an intruder is able to link an individual to a record in the published data table.
    2) Attribute linkage, where an intruder is able to link an individual to a sensitive value in the published data table.
    3) Table linkage, where an intruder is able to link an individual to the published data table itself.

2. Probabilistic attack. Ideally, the published data should reveal to an intruder as little additional knowledge about individuals as possible, beyond what he/she already knew before seeing the data (background knowledge, or supplementary knowledge). Probabilistic attack occurs when the difference between the prior and the posterior knowledge regarding an individual is “significant”.

Record linkage

The intruder is able to link an individual to a record in the published data table.

Recall that in published data tables Unique Identifiers (UIs) are typically removed, so record linkage typically relies on QIDs.

Suppose that an individual A, which the intruder is after, has a value qid of the QID, and that the value qid is known to the intruder.

In general, qid identifies a group of records in the table. If the size of the group is 1, we have record linkage.

If the size of the group is more than 1, an intruder may still be able to uniquely identify A with the help of additional knowledge.

***A priori* knowledge** - Prior to accessing database
a posteriori knowledge - *After accessing database*

K-anonymity

In a series of papers ([Sweeney, 2002], [Samarati et al., 1998]) Samarati and Sweeny proposed k-anonymity in order to prevent record linkage.

For each value qid of QID that exist in the data table, there are at least k record having value qid in QID.

If a table satisfies this requirement, we say it is k-anonymous.

In a k-anonymous table, a probability of successfully linking a record to another table on QID is at most 1 k .

Week 6 - Staying safe online, part 2

Who has a responsibility to protect against cybercrime?

- We all do

How can we do that?

- Staying vigilant
- Protection of our own data and other resources
- Reporting crimes and suspicious activities

Summary:

- **Encryption** converts plaintext into ciphertext using a secret key, This process is reversible - ciphertext can be decrypted to revolver of the plaintext
- **Hashing** converts plain text into a hash code without using a key. This process is not reversible and it is computationally infeasible to recover the plaintext from the hashcode.
- **Salting** is a process of adding a random sequence of characters to a password before hashing,
- If passwords are encrypted then the same ciphertext means that a passwords are also the same
- If uniques salt is used for each password, then hashed values will be different even if passwords are the same.

Generating strong passwords

- Random sequence of lower and upper case letters, numbers and special characters.
- Don’t use the same password for different purposes

Password management

Password managers are software applications that can

- Store different passwords
- Generate strong passwords

A good password manager will

- Require you to use a password to access it
- Lock out after a period of inactivity
- Store your passwords in encrypted form (either on your computer or on the cloud)

Pros

- You can use strong passwords without needing to remember them
- Password managers are convenient to use

Cons

- Password managers represent the so called’ ‘single point of failure’
- If for any reason you dont have access to your password manger, you dont have access to any of your passwords

Week 7 Malware

Didnt write notes for this but there was a good amount of definitions in the week 7 lectures, flick through them to grab the definisiotns, it was an information filled lecture.