COMP6441/COMP6841/LAWS3040 22T1 Lecture Notes

Lecture Collaborative Notes

Table of Contents

Table ofContents

Table ofContents

Table ofContents

Week 1 Lecture 1

Welcome to the Course - 14.02.2022

Course Structure

- Students are allowed to join across law and computer science classes
- Tutorials are mixed between law & engineering students to promote discussion/
    - Focus is on collective problem solving
    - Case study analysis - will require prep beforehand
- Monday lectures are optional for law students
- Tuesday 2-4pm law seminars are optional for COMP students, located in Law Building G02
- 4-6pm Tuesday lecture is the general security lecture (except Week 4 & 6), which is followed by movie night (completely optional but apparently fun). Followed by a discussion/ critique and comes with free food - need to register : https://secso.cc/food
    - Students not enrolled are allowed to come to lectures and seminars!
        - Wear a mask and register
- Monday evening (6-8pm) is when we do engineering content, introductory content, not the advanced stuff. Slightly technical, Comp students compulsory and law students optional
- You can transfer between 6841 and 6441 within the first week. 6441 is less technical then 6841 and is able to be done by people without too much of a technical background. To swap courses contact course email
- COMP Students: 40% weekly activities, 30% final exam, 30% project
    - Quality > quantity
- LAW Students: 40% Final exam, 20% CP, 30% Something Awesome, 10% Logbook
    - Bonus marks available
- Do not try to do everything
- Final exam: Based on the weekly activities, runs for 3 hours (has 4 hour bracket), sample released in week 6
    - Open-book exam
    - Is a hurdle, though is apparently easy so everyone should pass
- Week 1: Figure out “Something Awesome” you want to do in this course. Pick something and spend 30 hours on it in the course and at the end hand it in and make a video on it. A report attached to it. Basically, it’s up to you.
- 4 aspects/categories for project:
    - Make something
    - Learn something

Table ofContents

    - Teach someone something
    - œAudit (analyse) something
- Law students, think about something you want to teach the COMP students and comp students, think about something you want to teach the law students from each other's respective courses.
- Hall of fame: If you appear in the hall of fame you get 1 course mark (verrrrry rarely 2). Multiple appearances dont award extra marks.

Introduction to actual course content

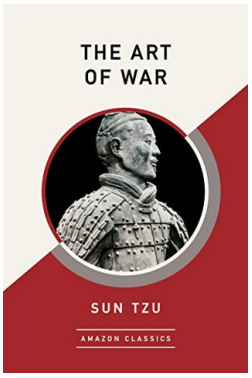
- What is security engineering?
    - Many different definitions
- What is an engineering approach to security?
- Security vs computing:
    - Security- end to end property/ more holistic. Aims to prevent any insecurity.
    - So long as there is one weakness, there is an insecurity. You are not secure unless the entire system is secure.
    - Essentially, closing 3 doors isn't useful unless the 4th is also closed
    - Computing - ensures that what is supposed to happen actually happens. They make sure computing processes run properly. Security is hypothesising what happens when something that was supposed to happen (postcondition), does not happen. What are the consequences and what are the ways to mitigate or defend against it.
    - People suck at responding to events that rarely happen - we need to be able to respond to the one in a million event in security. People cannot identify invisible risks and thereby cannot predict the foreseeable consequences.
    - We have never completely fixed a security problem, there are always ways to further improve a security solution
    - Both security and computing are prone to mistakes
    - Be proactive not reactive in security through analysis; plan in advance
        - Have some kind of analytical framework so you're approaching a problem analytically ("security eyes") - **notice what's the most important thing in the midst of a crisis.** Importantly, you should identify the source of the problem as opposed to merely detecting the symptoms.
        - The more complex something is, the harder it is to defend. There is more room for errors.

Attacker mindset:

Table ofContents

Don’t think like a defender - inherently limiting mindset; proud of their defence mechanisms and become overconfident; think like an attacker -they look for weakness, no inherent bias in thinking it is impossible.
Defenders can only see the good stuff. When defending, think like an attacker - look for the weaknesses (What comes next?)
Continually look for weaknesses and fix them.
However, if we only think like an attacker, we will be ‘barbarians’, with a reactive approach.

Key Takeaways:

- Ukraine is about to be invaded (Big F)
- Read the art of war
- 

- I didn’t realise this book would make me a good cyber security engineer
- Wear camo clothing at all times
- Set neighbours house on fire
- “How much is the final exam worth?” - guaranteed question in final

- Because of the threat of impending war between Russia/Ukraine and China, there is a threat of cyber-attacks too
- A clever attacker looks for clues around, to see if there is any information that can help them attack
- Law students provide useful insight through mechanisms such as corporate governance, regulation, incentive structures in companies, and critical infrastructure regulation. We need the technical and legal in collaboration, which then mirrors policy-making
- Security is more holistic than computing; an end-to-end property. Insecurity means finding a weakness. Computing is about dealing with things that are in-spec.

Table ofContents

Week 1 Lecture 2

- Trust is everything in security, even when coding we trust the api
    - No trust = extra work
- Trust in regulations, industry standards, engineers who built the bridge have good education, maintenance regime
    - Trust is placed in the engineering institution
- Trust in digital systems not guaranteed like trust in civil structures

    Methods tried to build trust in digital world : credit card

    Security is reactive: something breaks/is breached -> fix and repair

    We can never guarantee that our devices will not be hacked.

Mont-Blanc case study

https://en.m.wikipedia.org/wiki/Halifax_Explosion

- Confusion over two ships passing causing the ignition of munitions on one ship
- Called in by the governor to review the accident and make a decision on what should be done?
- Firstly, don't assign blame - instead focus on what we can learn for the future
- Crisis: rare opportunity to learn so that they never happen again
- Foreseeable accidents should have contingencies and plans in place to mitigate them

Crisis response - Three phases:

1. Planning and design
2. Response to crisis
3. What to learn for next time (audit) - take actions to prevent foreseeable accidents.

What it means to be an engineer:

1. Problem solving/doing
2. Testing in advance - never make assumptions
3. Backed by theory & framework
4. Adherence to regulations, codes and standards (We love standards <3)
5. Responsibility
    - Professionals: have a duty to the profession (not just to themselves and their employer).
6. Community (team work)
7. Measuring - familiar with (big) numbers

Estimation is critical to check how reasonable it is

Table ofContents

- Toast to fill a lecture theatre
- Break down to steps
- Issue with estimation is that we can't verify it - requirement for security engineers
    - Triangulation/Dual control

History of cyber

- Phone Phreaking - mixing data and control (not good)
- Microsoft money (home banking) -> now there is actual value to hacking computers
- Advanced Persistent Threat

What were the bingo words again? (silly words)

- Blockchain
- Threat Actor
- UnHaCkAbLe
- Cyber
- Top men
- APT

Proposed reading:

- Cuckoo's Egg (Clifford Stoll)
- * Bill Cheswick: An Evening with Berferd. In which a *Cracker is Lured, Endured and Studied*
- * The Art of war (Sun Tzu)

  * recommended read before week 2

Table ofContents

Week 1 Law Lecture

Definition of Regulation: sustained and focused attempt to alter the behaviour of others according to defined standards or purposes with the intention of producing a broadly identified outcome (Black 2022, p26)

- Intentional (but can be indirect)
- Not limited to state actors
    - For example: business standards
- Different types (including self-regulation)
    - Of industries, and individuals.
- Examples of regulation: Info gathering and representation; standard setting; behaviour modification (sticks, carrots, sermons, architectural barriers **defaults (for example, privacy defaults on phones**).
- Making a desired behaviour the most rational option likely outcome

Cyber security is inclusive of:

- System security
- Cyber resilience
- Cyber safety (including scams, abuse)
- Info security
    - Confidentiality, integrity, authentication (CIA)
    - But also: availability, non-repudiation (particularly in the context of legal transactions)

Examples of types of regulation for cyber security:

- Legislation (Acts and Regulations)
- Common Law
- Policy (government and organisational)
- Private rulemaking
    - ASX Rules
    - Industry self-regulation
    - Standards
        - Professional standards
        - Technical standards (ISO/IEC, IEEE, Standards Australia, NIST, ASD); ratings systems.
    - Education
    - Influencers

Who do we want to regulate/ Whose behaviour do we want to influence?

- Companies and organisations
- Critical infrastructure- power stations, courts, universities, defence industry (etc things that are necessary to our countries that require protection.
- Consumers.

Table ofContents

- Governments themselves are also regulated by themselves, international policies and conventions. Other countries may threaten sanctions against other countries.
- Attackers and defenders

Laws related to cyber security:

- Contracts
- Criminal law
- Corporate governance
- Equity- fiduciary obligations
    - Obligations of loyalty.
    - "insider threat"- hacks by inside employees
- Consumer law
- Corporate governance
    - ASIC
    - Director duties
- Constitutional law: telecommunication laws can be passed
- Laws around secrecy:
    - Contractual obligations of confidence etc.

Table ofContents

Week 2 Lecture 1

Logbook activities due Tuesday Noon the following week.

Overview

Chekov's gun: showing something *in*signifid later

- Guy driving + school nearby = 🤔🤔

Every cyber attack is a **misuse** of trust

- E.g. trusting employees, dating sites, trusting inputs, trusting user's actions

Everything you trust is a point of attack -> ripe for ecant -> will most likely be significant

- E.g. gun on the wall is most likely usexploitation
    - If you don't test it

Locked room problem

There's a hole in a room and messages come through it on a ticker tape

- Use holes to send messages back
- **Only communication in the world, no personality in the message at all**
- If only two random messages, the computer has no way of knowing
- **The computer is the guy in the room**
    - No connection to the real world
- A human would say **show me**, or ask someone, or confirm the authenticity of the "message"
    - How would you know it's actually the person you're sitting next to?
- All a computer is, is a person in a room getting an anonymous message
    - The computer can never know **anything**
- Biometric systems don't really allow verification of the data, as somewhere along the line, a signal is passed down a wire to the computer in the locked room, and the computer implicitly trusts the signal coming along the wire
    - Creating a dummy fingerprint scanner renders the added "security" of the biometrics useless
- Lots of different components in a system, everything can be compromised but a computer can't detect that
    - Computer verification: this computer doesn't know anything about the real world
    - Taken adv of by salespeople, emphasis on technological capabilities
    - There are some very helpful protocols which mitigate this problem but never fully solve it
- At the end of the day, it's only a true or false output from data given by an authenticated source *or* some malicious input

Table ofContents

Never forget that the system-wide property relating to the real world depends on a chain of things happening perfectly and securely, and the computer only deals with the abstract.

Cake

Cake is about trust.

- Richard and his brother fought over cake. Wanting more than their siblings.
- So they added a **protocol**.
- What about a protocol without the trusted third party?
    - One person divides the cake, the other picks the piece they want.
    - It's in the interest of the person who cuts to make equally desirable pieces.
    - And the picker picks the most desirable. Even with different values about cake. (icing > cream in the centre)
    - This is hard to expand to three people. Exercise for the reader.

Arbiter-less protocols are vital for the internet to function.

Reminder: don't burn yourself out! 😇🤩🤠👇

Richard wants your work by Wednesday, not perfect. Just do the best you can with the time you have!

Risk

People are very bad at assessing and understanding risk.

What *is the risk*?

- I have my laptop, and I was about to give a talk. It died.
    - Went to nearby laptop shops with 3 hours until the talk.
    - It came back, all fixed, and was charged $100.
- What about from another point of view?
    - Laptop shop workers - crazy production line fixing. There's a lot of throwing computer parts around. Watch the recording I can't do this explanation justice in text: https://www.youtube.com/watch?v=8sgCijpGc_w&t=2077s
- **PROBLEM: The risk was enormous. It was not 0 risk.**
- Is $100 worth a difference between 1/100 chance or 1/10000 chance of your laptop being destroyed?
    - Is your answer the same if you don't know the risks/probabilities?
- Not just the laptop, but the information on it is important

Table ofContents

- To think about: risk is personal. What is the impact of the risk on you? Different for everyone

Why aren't risks known?

- **RISK IS INVISIBLE. You're taking a gamble.** You never see the coin being thrown**. Humans only see the outcome.**
    - Reversing out of a driveway and hitting a kid: pain and suffering spreads wide, life is ruined, goes to jail
    - Two worlds. Is the person better in the world when they hit the kid than the other?
        - The only difference is **luck.**
        - **If you take a risk and you get a good outcome, the world only sees you being lucky.** No one sees the risk.
        - **The person is just as guilty in both worlds. It's just that in one, they're lucky and they get away with it**
        - **The crime is taking the risk.** Regardless of whether they hit the kid or not.

There's a list of risks that will probably occur during the course in the slides: https://www.openlearning.com/unswcyber/courses/security-engineering-22t1/week02/slides/?cl=1

- Impact can be **personal** or **society** wide.
- Classification of risks (not absolute)
    - Consider the impact of a risk vs likelihood of a bad outcome
    - Listed above are **HIGH IMPACT LOW PROBABILITY** events

High Likelihood	*we'll be talking about this more	oh no fix this
Low Likelihood	meh	Hollywood Risks: Disastrous if it were to happen, but will not be likely to
	Low Impact	**High Impact**

- Humans judge risk based on their **experiences**
- If a risk is more likely, people are more likely to know about and care, even for low impact. Often low likelihood risks are rare and not experienced, so they are 'Hollywood risks', used in films. People either expect it to never happen or definitely happen (freak out, overreact)

Table ofContents

    - E.g. People think they'll be struck by lightning if they're outside in a thunderstorm - it's probably fine. But then they're completely oblivious/uncaring about other Hollywood risks.
    - You (as a security engineer) need to be careful to not obsess over these risks.
- To think about whenever something bad happens:
    - What they could do in advance
    - While it's happening what do they do & how could they have dealt with it better
    - How should we change things in the future
- Best way of learning is through mistakes
    - **The best mistakes to learn from are other people's, not your own**
    - Always think about what they could've done: clues that they neglected, how could they known this was going to happen a bit sooner, mitigated this risk in some way, training and set up so that it wasn't so disastrous, plan responses
    - Learn from history for low probability risks

Error : False Positives and False Negatives

- The Problem of X
    - Mankind keeps inventing stuff. For example, X.
    - There's always an attached problem: The problem of X.
    - Take, for example, X-Rays. We can use them for medical things.
        - But they also cause cancer and their own medical problems.
        - They *used* to be used for fitting shoes. Not anymore, but it took a while to find the problem because cancer is slow.
    - Similarly with cigarettes, but it was even harder because lobbying was occurring.
    - Cars: Pollution, accidents. But we still have them - we've deemed the problems are worth it to have easier transport.
    - The mayor of a suburb wants to cut down trees when constructing a park to eliminate the risk of falling branches.
        - Richard thanks them for banning cars, since they're a bigger risk/danger than falling branches.
    - Problems only occur later
    - What's the problem with computers?
        - We do *everything* with computers. It's a big X.
        - But there are several problems with computers. In particular we care about cybersecurity. It took 20 years to find.
- We are awful at assessing errors, both False Positives and False Negatives.

Table ofContents

    - You won't be penalised for forgetting which of FP or FN is Type I or Type II, because Richard can't remember either.
        - Type I is FP
        - Type II is FN
    - e.g. Some people care about False Positives: people who shouldn't get benefits are getting benefits. How terrible!
    - Ripping the system off vs. deserving something and not getting it
    - But then people who care about False Negatives: people who should get benefits aren't getting benefits. How terrible!
    - Usually both problems are serious and we need to think about them both
        - The errors occur between the mismatch of the system that makes a decision and the real world
        - Are people innocent or guilty? They could be guilty and be found guilty, or they could be found innocent, etc.
        - All outcomes are possible but only with a perfect system.
        - Always trying to minimise error
- Reduce chance of T1 error, increase T2. Vice versa. Only way to reduce both is to spend money (a lot of money)..
- Try to understand the other camp. You have to understand the other person's point of view.
    - Unless the groups talk together, you'll never improve the system
- Every system will have T1/2 errors, but you/your client will only see one type
- Passport system example:
    - Sales perspective: let many people go through
    - Security perspective: catch the bad guys
- Does anyone log the mistakes?
    - The boy entered with his mum's passport; a **silent failure**. Only noticed when the mother tried to enter with her son's passport. The event wasn't logged.
    - Consider foot traffic. The more secure, the more errors you'll get. Slows the system down.
    - Turn the knob to reduce the error that you won't get matched with your own photo.
- Two possible outcomes, two possible ways it could fail
    - People neglect either of the two errors
- Don't have both errors? **Security theatre;** looks secure but failures are silent and it's just there to reassure people
- **Creeping determinism**: reinterpreting the event and everything seems more likely (Monday's experts)

Table ofContents

Risk assessment

- What are you protecting? **Assets**
    - E.g. laptop, data
- What are the threats? **Threat models**
    - Threat models: the scenarios it could be attacked
    - E.g. Who are the bad guys? The government, other states
    - What am I defending against?
- **What are the vulnerabilities/risks?**
    - What are the bad things that could happen
- **Assessment**
    - The final matrix/rubric assessment
    - What's the most important thing to focus on?
- **Dealing with risks: 6 choices**
    - **Mitigate/ Reduce Impact** (prepare for the impact, wear a helmet)
    - **Reduce Probability** (potentially avoid the risk completely)
    - **Pass risk on** to another
    - **Accept the risk,** meaning do nothing
    - **Immunise** (to talk about another time, i.e. if a bad thing happens, making another good thing happen, typically a finance thing)
    - **Pool the risk** (share with others)
- "Zero tolerance for risk"
    - The board is therefore idiots.
    - No chance of zero risk in cybersecurity.
    - Don't take this job - you'll be blamed for anything going wrong.
- Daniel Kahnerman
    - Won a Nobel prize for showing that the assumption (in economics) that people are rational is wrong. By looking at people's risk tolerance
- **Risk registers**: document where companies write all their risks down. "The most **useless document** I've ever seen in my life" - Richard. Good to think about your risks but doesn't actually manage risks

Table ofContents

Week 2 Lecture 2

Patterns

- Mixing data and control
    - Client and users have the ability to input data into control system
    - If mixed in the same channel, data can be controlled by the users - Phone phreaks mixing of control tones on old phones. Captain crunch whistles used to exploit systems for free calls.
    - How to prevent it ?
- M & M's
    - Temptation to build system to make like M&M
        - Protective shell, inside mushy - like our bodies, cells
            - Can be attacked by virus, breaking through
        - When the system has a layer of protective shell, which just doesn't trust anything, but once that shell is broken, then you are trusted and have access to everything.
    - Single point of failure
    - Insider threats
    - Once you're in, you're in
    - Similar to trusting a firewall in cyber security
- **Locard's principle**
    - Every contact leaves a trace
    - As technology gets better it's easier to find traces
    - True of police work and forensics, true of security

Anatomy of a Typical Attack

- Someone is tricked into doing something dumb, dumb thing lets bad guy get foothold in system
- Privilege escalation, bigger way of getting in, as usually the target is something higher up
- Persistence, chain system so they can get back in someway in another time
    - Sometimes dont like persistence, leave no trace of getting in
- Stealth, hide presence, deleting and changing stuff inside system, defences cant detect intrusion
- Getting through an unpatched part: Accellion. A device on the perimeter of a system
- Usually 0-Days are not used

Table ofContents

- Can also hack into systems through unknown, unpatched problems. Very unlikely though because people don't want to expose these methods unless whatever the attacker is hacking into is very important
- Patching quickly is important, as when a patch is released, the world knows that there was a hole somewhere in the system, which will still be there unless its patched

Physical

- game Over
    - Physical access is the foundation that cyber security is built on
    - If someone can steal your physical computer, it doesn't matter how strong your software security is
    - Server rooms are often locked
    - You Hack into Richard's Mac Laptop because he doesn't have his **FileVault**(??) on - once you have the device, you can just get in if there is no extra protection
    - The location of server rooms are often kept secret
    - Destroying harddrives is also an important business and requires large amounts of damage when disposing of hard drives since data can be extracted if it is not destroyed properly
- Locks
    - We assume physical security works, but this is not always true
    - People also leave data on combo locks by only moving the dials by 1
    - Keypads/screens often have fingermarks showing the password/gesture\
    - Generally, the cleanest keys on a keyboard or the cleanest keys are usually the keys used for unlocking locks
    - Always make sure that the physical security is adequate at the very least.
- Tampering

Table ofContents

Recon

- Hackers have recon phase - getting to know a much information
- 2 sorts of recon
    - Active
        - Interact with people or devices to actively extract information
    - Passive
        - You look at what's left lying around, clues that are there
        - Things that don't seem important can be leveraged into an attack
            - E.g. if you know someone's kids school, you can call the school pretending theres a bomb threat
        - Can aggregate seemingly useless info into something useful, into an attack
- OSINT
    - Open Source Intelligence (OSINT)
- Bellingcat
    - https://www.bellingcat.com/
    - Publish groundbreaking investigations and uncover wrongdoing all around the world

Shred

Special guest: Kevin Nguyen @cog_ink on Twitter

www.abc.net.au/radionational/programs/backgroundbriefing/the-base-tapes-part-one/13274832

Secrets

- To keep a secret, tell no one
- You cannot untell a secret
- People feel good when they are told a secret, as it is a kind of power. But secrets are only impressive if they are shared. Almost structurally designed to leak
- INFORMATION SECURITY - CIA (Confidentiality, Integrity, Authentication)

Table ofContents

- Confidentiality
  - **Steganography**
    - Keeping information confidentially by hiding it in something that is not a secret
    - Hiding in plain sight
    - E.g. shrinking images in text, hiding data within audio
    - Six design principles for ciphering
      - The system must be practically, if not mathematically, decipherable.
      - It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience *(The magic one)*
      - Key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents
      - It must be applicable to telegraphic correspondence
      - Apparatus and documents must be portable, and its usage and function must not require the concourse of several people
      - The system must be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.
    - **Security by Obscurity** doesn't work, as nothing will be kept fully secret for long. Ensuring security this way is a sign of weakness
    - For example, the enigma machine was not a hidden machine but still proved to be an effective cipher
      - Security through obscurity (or security by obscurity) is the reliance in security engineering on design or implementation secrecy as the main method of providing security to a system or component
    - *However*, while the enemy may know the system, the data is still kept secret, normally a shared secret called a key.
    - This key holds all the information which the cipher depends on
    - Finding one key does not unlock systems that use a different key
    - Codes is where logical units are swapped (words for words)
    - Ciphers is where lexical units are swapped (letters for letters)
      - Sometimes done by rotating letters (Caesar/Substitution Cipher)
      - Sometimes done by permutation, which is resistant to letter frequency analysis as it rearranges the order of the letters
      - Vigenere cipher - quite good and hard to crack
      - Playfair cipher - is also more resistant to letter frequency analysis

Table ofContents

        - Classical ciphers are all breakable once we got computers
    - Integrity
        -
    - Authentication
        -

Week 3 Lecture 1

Measuring

- Engineers measure things to quantify something
    - I.e. If it works you know why
    - Might want to build it again; enough details recorded in order to replicate the process
- **QQQ** - 3 levels (Qualitative (lowest), Quantitative (middle), Qualitative (highest))
    - **Qualitative:** Things that sound wishy washy(?), people just go with their gut/guessing (not measure)
    - **Quantitative:** Measuring things. Science period, people started measuring and recording - we had a lot of technological advances since then
    - **Qualitative (again):** Build on top of quantitative, so you aren't just following a computer essentially
- Not everything that is worth measuring can be measured e.g. how good a song is
- All professionals should have a quantitative base with a qualitative above that to build upon it - a way of improving things
- Measurement is just the baseline layer of security

Mathematical Measurements

- Get familiar with binary
- 3 different ways of thinking about numbers:
    - 'The fourness of four' - the **essence** of a number
        - Crow food experiment: Someone walks in and puts food in the nest. Crows wait until that person leaves. Then do the same for 2, 3... people. Shows crows can count up to 4
    - How you **pronounce** the number: when you say 'four' we imagine 4. In different languages we still think of 4 even with a different way of saying it. Doesn't matter how you pronounce or write it, it's the same concept

Table ofContents

    - How we **write** the numbers themselves
- Binary only affects how we **write** numbers
- Rules of exponentiations + logs (make sure you know!)
    - $B^A \times B^C = B^{A+C}$
    - $(A^B)^C = A^{B \times C}$
- Growth rates (i.e. linear, quadratic, cubic, exponential) → often people in the media talk about exponential growth but they usually just mean 'non linear' growth. Mentally check when people use this phrasing.
- Any cyber person should know the doubling numbers, should know up to the first 10 & can use a trick beyond that
- This is important because we are going to be measuring things that are really big… but humans are really bad at measuring/ calculating/estimating big numbers. So practice estimating 2 to the power of different numbers
    - E.g. 1 billion / 66 using powers of twos
    - 1 billion = 2^30, 66 = 2^6, therefore 1 billion / 66 = 2^24 = 2 ^10 * 2^ 10 * 2 ^4 = 1000 * 1000 * 16 = 16 million
- XOR function → learn it, very handy

Binary/ Why are we usin bits to measure numbers

In security we are often working with big numbers and it's hard for us to understand. We could talk in digits eg. he has a seven digit salary. This gives us an estimate that is a bit easier to comprehend. However, instead of using base 10, we use bits (powers of two) to get a slightly more accurate estimation of a number that is easier for us to comprehend.

Measuring Information

- Measuring will allow us to start making assertions

<u>Outer space example:</u>
Martian men lie always
Martian women tell truth always

Venusian men tell truth
Venusian women lie

-Raymond Smullyan

Table ofContents

- What yes/no question can we ask the four characters to find out which ones are women (just say they all look the same). [Answer: Are you a martian?]
- Now what yes/no question can we ask the four characters to find out what their gender and species is? [Answer: there is no possible question]
- Why? Trying to select between 4 combinations based on their answer, but with a yes/no question we can only distinguish between two combinations.

20 Questions Game
(note that similar to the martian example, with only 20 yes/no questions, we can never distinguish more than a million objects with this game → we can try to use binary search method to find the answer in 20 questions)

1. Is it an object - Yes
2. Is it an object I would have seen before - Probably (Yes)
3. Is it one of a kind - No
4. Is it in this room - No
5. Is it in Australia - Yes (potentially)
6. Is it bigger than a dog - Yes
7. Is it bigger than a car - Yes
8. Is it bigger than the lecture theatre (interior) - Yes
9. Is it a building - No
10. Is it manmade - Yes
11. Does it move - Yes
12. Does it move through the air - No
13. Does it move on the ground - No
14. Does it move in the water - Yes
15. Is it a cruise ship - No
16. **Is it a submarine - Yes**

Entropy

How do we measure information:

- How can we **compress** without losing information (notice we have a lot of **redundancy** in the english language) eg. try to tell your friend to meet you somewhere in the least amount of words
    - Meet me at KFC at Town hall
    - Maccas at Town hall
    - Maccas at 3021 [postcode]
    - Meet at our maccas [information based on shared memory]

Table ofContents

- Pre-shared information (the meaning is agreed in advance) works like a code that can be transmitted with the least amount of information
- Exercise: Try specifying a number in less than twenty letters using the english alphabet. Can we communicate any number in the universe with 20 letters? No (pigeon hole principle). You can only communicate up to the number 27^{20}.
- We are going to work out how many **bits** communicated are information. Bits will be measured as a power of 2. (The number of bits is equal to the power of 2)
    - Eg. $6 \times 10^{15} = 2^2 \times (2^{10})^5 = 2^{52}$ (approximately 52 bits of information)

Sentence guessing game
"Over the next ten days NSA technicians "

- 28/39 letters guessed correctly
- 11/39 wrong
- English language has redundancy as seen in the sentence guessing game
- 27 Letters (including spaces) and 39 so 2^190 bits of information
- However there is so much redundancy here as we only needed letters 11 times , using 52 bits of information
- The amount of information given to a student was enough for him to distinguish between 27^11 bits of possible information
- Each character gives us about 52/39 bits of information approximately = 1.33
    - 1.75 bits per character → https://aclanthology.org/J92-1002.pdf

Measuring Security

We have been talking about measuring information but how can we measure security?

- Knots and friction: when you make a knot with rope, it doesn't come undone because of friction, the more pressure applied, the more friction.
- **We can never make something perfectly secure, we can just give it friction**. We can only make it easy for the good people and hard for the bad people, but we can never make it perfectly secure. The bad guy will get there by brute force, it is only a question of how long it will take to get there
- We could measure security in terms of time but time isn't a great measurement (not a universal measure). So we will always now measure cryptographic security in terms of work. **What is the amount of work the bad guy has to do** before he can crack the code? Eg. he has to do 20 (2^20) bits of work (bits being binary digits). We can say that has 20 bits of security
- Example: 2^50 passwords to guess. 1000 steps to test each password.
    2^50 * 1000 = 2^50 * 2^10 = 2^60 operations required

Table ofContents

Computer: 2^35 operations per second.
2^60 / 2^35 = 2^25 seconds ≈ 32000000 seconds ≈ 2^8 days ≈ 1 year
In conclusion, 2^60 is not a lot of security (easy enough to crack, especially for a team of people or a computer with a GPU etc.)

- 2^128 is the bare minimum you need to be secure
- Measurements of computer processing speed
    - Floating point operations (i.e. decimal numbers) FLOPs → a measurement for super computer's processing speed
    - modern CPU core typically does ~ 32 FLOPS / cycle

Modern Ciphers : Confidentiality

- There was no standard in place to determine if a data link was secure
- DES (data encryption standard) was released from the NSA (no such agency) and there was a rise in research about codes and ciphers. (Early 70s late 80s) hackers began to use differential analysis to hack DES (the key was too small: 52 bits was easily cracked)
    - AES is the Advanced Encryption Standard that is now currently still used
    - Idea: we take the message and separate it into blocks, encrypt each block.
    - Then combine the blocks again each block is passed through S boxes (substitution cipher) then after all the letters are transposed. This is called a round and multiple rounds are completed
    - Each round does a little jumble which is repeated over and over until the message is thoroughly scrambled.
    - Claude Shannon - “a good code should have confusion and diffusion” (confusion = relationship between key and ciphertext is obscure, diffusion - the relationship between the ciphertext and plaintext is obscure.)
- Cards: Repeat a shuffle to make it more jumbled. Do the same with codes.

Table ofContents

Week 3 Lecture 2

Course map

- **Security Engineering**
  - Security should really be an engineering as we use principles and should be more systematic
- **Secrets**
  - Distinguishing a trusted person from a malicious attacker. Challenge of distinguishing because if we are too strict then no one can access it but if it is too lax then anyone can. The notion of a **shared secret** is what allows us to distinguish between people
  - How to demonstrate they know this knowledge without giving it away
  - Secret is a weak point. What can we do if an attacker finds it
- **Humans**
  - Understanding humans are important as one of the weakest parts of a system is the human
  - We want **end-to-end security**, the entire process being secure. Thus the person should also be secure. “Ends” often involve people
- **Insiders**
  - Humans inside the organisation that you trust, but they go bad
  - Most systems fail due to insiders. Can be part of human nature to be blind to insiders. We often overlook insiders despite them being a weak link. Looking at the nature of insiders and behaviours etc.
  - Google created a google team to watch insider attacks
- **Privacy**
  - A lot of attacks are privacy compromises
  - Publicity of attacks makes cyber more important
  - Talking about privacy to understand what it is and what we can do to promote the field
- **Data**
  - What data is, why is it an important asset
- **Just Culture, Normal Accidents**
  - Organisational culture and how to deal and think with accidents (including designing around them). Can learn from safety engineering. Difference is defending against bad luck vs defending against the worst adversary
- **Communication and Change**
  - Learning how to effectively communicate and start change
- **Nation States**

Table ofContents

    - Looking at nation states

Logbook

- Have photos in it
- Mark the best activity with "!". Will be marked more closely
- Photo of yourself on the logbook cover

Passwords

- Everything operates on shared secrets
- Secrets have keys. Sometimes the password is the key. Is often changed or combined with other things to change the key, however the human part is the **password**
- Electronic password manager or write password on paper
    - Password on paper: you can lose it, not portable, can be stolen (physical breach)
    - Electronic password managers are a jackpot for hackers because they are stored in the cloud (a single point of failure). Once it is hacked, all your passwords are compromised.
- Security questions for password recovery can be compromised from social media information (e.g. What is your favourite colour?) and some of these questions (e.g. birthday), once compromised they will be compromised forever.
- Truth is important. But when filling in forms on the internet, LIE! Use these for recovery questions. Have a book to keep track of these lies.
- How do we recover? Password recovery is a weak point.
    - 2FA SMS
    - Recovery email is very important. It should be secret (have an email just for password reset), no one else should know about it. They are your weakest point.
    - Signing on with facebook, twitter, google etc, is not safe. If one of those is compromised, then everything is lost.
- NIST 800-62 2019 password guidelines:
    - 8 character min when a human sets it
    - 6 character min when set by system/service
    - Support at least 64 characters max length
    - All ASCII characters (including space) should be supported
    - Trunctuation of the secret (password) shall not be performed when processed
    - *Check the chosen password with known password dictionaries !*
    - Allow at least 10 password attempts before lockout

Table ofContents

    - No complexity requirements
    - No password expiration period
    - No password hints
    - No knowledge-based authentication (e.g. who was your best friend in high school?)
    - No SMS for 2FA (use one time password from an app like Google Authenticator)

Humans

- End to end - ends involve humans
- Games, war games, RAND, Tragedy of the Commons, Prisoner's Dilemma
    - Prisoner's Dilemma - in each prisoner's benefit to dob the other prisoner in. Results in suboptimal outcome as each prisoner acts in their own interest rather than cooperatively
    - Tragedy of the commons - individuals with access to a shared resource act in their own interest and, in doing so, ultimately deplete the resource
        - Everyone's interest is to exploit shared resources, because they can get some benefit even if it is bad for everyone else. If everyone exploits the shared resource, then it is bad for everyone and no one benefits.
- Nuclear Powers
    - Mutually assured destruction: If you attack, I also attack, then the whole world is destroyed. It is in our best interest to not attack.
- Important to think about how humans behave when thinking about security, as hackers often use the weakest link (often humans) to get access to companies
- Social engineering
    - Recon - gather as much information on their target as possible
    - Phishing - communication intended to trick someone into doing something
    - Spear phishing - communication targeted towards a specific individual or organisation
    - Long con/short con
        - Long-con is a scam that unfolds over a series of weeks
        - Short-con is a scam that occurs in a short moment
    - Hot state - getting a person in a state of high emotion can impact their rational process when making decisions, which is good for an attacker (e.g. magic, misdirection in bang or stage lady, kidnap family member and demand ransom)
        - Don't transfer money before you contact your buddy, or take a pause before decision

Table ofContents

    - Timing (when distracted or misdirected something else) (mitnick attack)
    - “Hubris” - excessive pride
    - Abuse of trust
- How would you get into a building without a swipe card?
    - Tailgating - people often won’t confront you
    - Carry boxes - people will help you
    - High-vis vest
- Airport screening
    - ‘Random’ bomb screening, was able to intentially be picked/not-picked by acting in a certain way
- Cognitive flaws/vulnerabilities
    - Flaw and bug is an imperfection in the system, and becomes a vulnerability when that flaw is used for some security breach and exploit is how you do it
    - Cold water test
        - Place two hands in one bowl of hot water & one bowl of cold water, then after a while when you move it to tepid water will still feel like it is burning/cold
    - Optical illusions
    - You can see your own nose (in your field of view), but your brain filters it out
        - Also have a blindspot, but your brain tricks you into not realising
    - We are all flawed
- Things to think about:
    - Dan Ariely - psychologist / behavioural economist - read his books
    - Misdirection - learn about how magicians do misdirection
    - Weakest link
    - Dating Scams
    - Anti phishing training
    - Mitnick
    - Heroes and Villains
        - People always look for heroes and villains in crises
            - Very simplistic idea, which doesn’t help us with analysing the problem and what we can do to mitigate it in the future
    - Watch Penn & Teller: Fool Us

Table ofContents

Week 4 Lecture 1

Review

- A feature of engineers is estimating things and putting numbers on thing
    - Guesstimation estimation
- The idea is to come up with a reasonableness check
- If we focus too much on details we forget how many zero's there are
- Just checking things are overestimated enough to ensure safety
- Concrete
    - Free podcasts about security on lecture slides (Apple | YouTube)

Modern Symmetric Ciphers

- DES
    - Keys are only 56 bits long which makes it insecure as it can be brute forced
    - Thus extra jumbling with triple des does not work
- Triple DES
    - Encrypts with a key first
    - Then decrypts with a second key
    - Then encrypts with a third key
    - Use 3 different keys makes 56 bits + 56 bits + 56 bits
    - However had flaws
- Feistel Networks
    - Message goes into L. R is generated
    - L goes into an cryption
    - R goes into a function - XOR
    - XOR fast to compute
    - If one of the inputs is random, the output is also random
    - XOR is invertible
    - We generate K - This is a key
        - Generate lots of round keys
    - Then switch sides and XOR's and encrypts
    - $L_{i+1} = R_i \mid R_{i+1} = L_i \text{ XOR } F(R_i, K_i)$

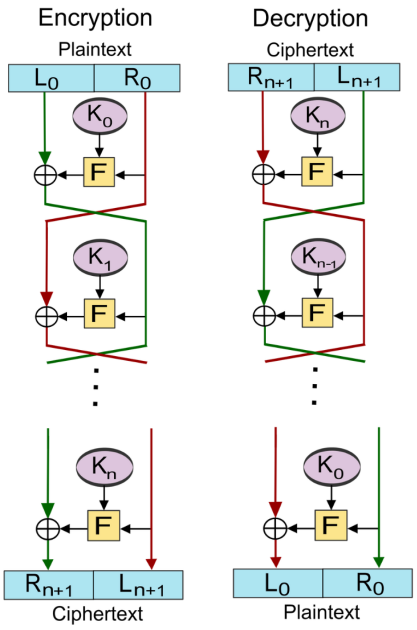
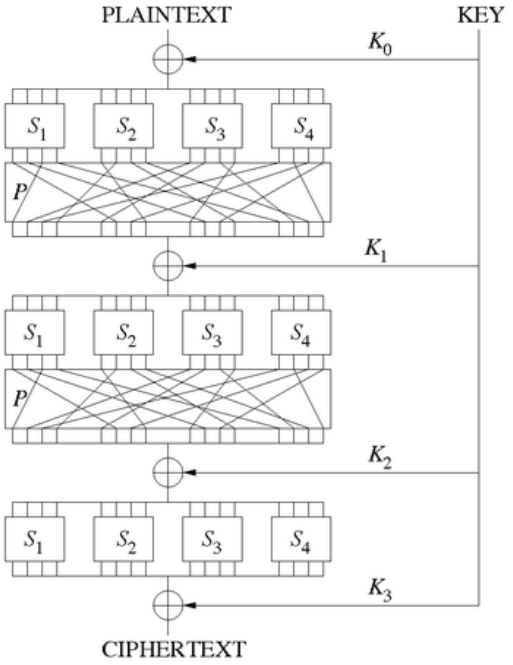


Table ofContents

- AES
    - Does less rounds than DES and people can break them for small number of rounds
        - Still looks safe, for higher number of rounds
    - Uses SP (substitution-permutation) network
    - Initial key is broken down into many subkeys
    - The subkeys are then XORed with the plaintext
    - Breaks the text into segments, and then a substitution occurs
    - The outputs are then jumbled round again, with the output being XORed with the next subkey
    - This repeats for multiple rounds
    - Everything in the algorithm is invertible
    - The algo itself can't be attack only if the implementation is not correct



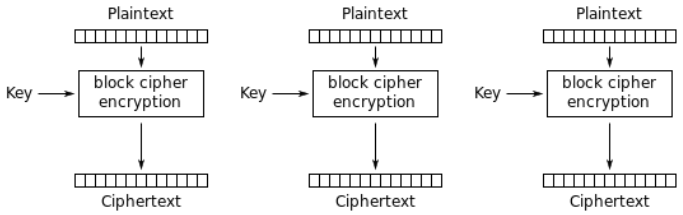
Don't roll your own

- Most likely that anything you roll out will have bugs. A bug in a crypto means more likely it can be broken and so will be insecure.
- 'Rolling your own crypto' means you designing a new algorithm that you then proceed to use without either:
    - Without auditing it, or worse
    - Without publishing it at all. That is keeping the algorithm private.
- Side-channel - a secondary channel where you are leaking information
    - E.g. FBI shines a laser on windows to detect the vibrations and figure out how many voices are speaking in a room
    - Fingerprints on a keypad/at the scene of a crime
    - The amount of power consumed by a computer/device can provide information on what operations its doing
- Tempest - Side channel attacks
    - Dutch tried online voting

Table ofContents

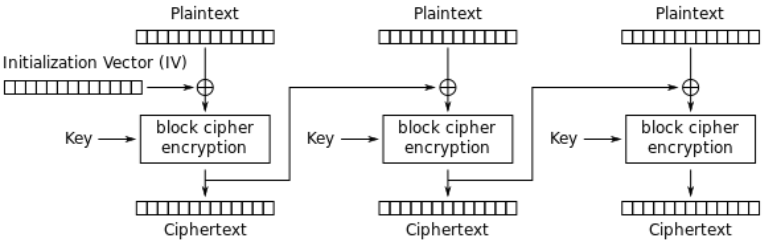
    - Outsourced cyber security to consulting firm who assured 128 bit encryption
    - Security engineers tested system by sitting outside polling station a radio receiver dish, did frequency analysis and reconstructed EMF from cathode ray tubes to see who people was voting for
    - Had side channels of the EMF leaking
    - Could reproduce images on the screen by scanning the EMF

- Joining together blocks of cipher is called the mode. Block cipher modes of operation
    - ECB (Electronic codebook): Treat each block of the plaintext separately. Identical chunks will have the same output.
        - Problem is that you give the attacker some information about the relationship between the plaintext and ciphertext
        - For example, if hail hitler is the first line then we can observe the pattern



Electronic Codebook (ECB) mode encryption

        -
    - CBC (Cipher Block Chaining): The plaintext of a block is combined with the ciphertext of the previous block via an exclusive or (xor) operation, and the result is encrypted
        - Problems include that you have to do the first block before doing the second, meaning you can't do things in parallel
        - Plaintext is XOR with an initialization chunk then put in an encryption

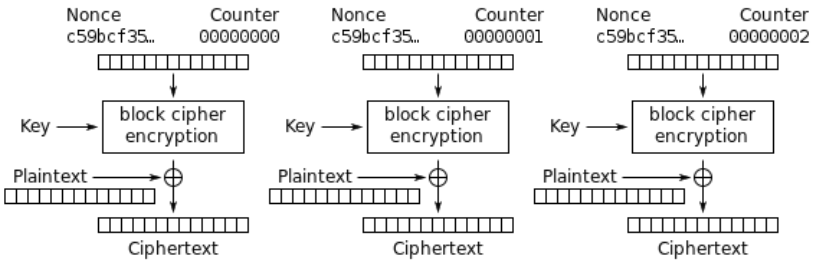


Cipher Block Chaining (CBC) mode encryption

        -

Table ofContents

- CTR (Counter): Involves XOR-ing a sequence of pad vectors with the plaintext and ciphertext blocks. The pad vectors are generated with a counter.
    - Diffie and Hellman
    - Take a counter - a nonce
    - Encode the counter
    - XOR with plain text to get ciphertext
        - Plaintext patterns are destroyed by an XOR as XOR only requires one of the pair to be random
    - A random number generator
    - “The counter ensures the input to the block is different (only by one digit!) each time. This means that after the block is done the output will be on average 50% different from the previous bit (see the avalanche effect). If the same counter amount or nonce was used the output of the block XORed with the data would be the same - so essentially the same as ECB encryption. The counterpart of CTR means that each block will be encrypted with an effectively random new encryption string”

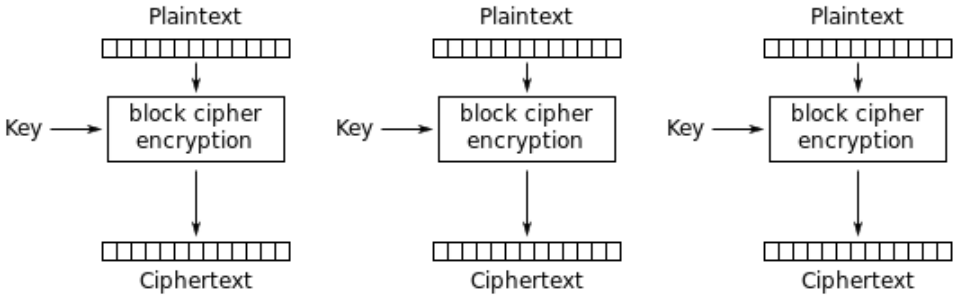


Counter (CTR) mode encryption

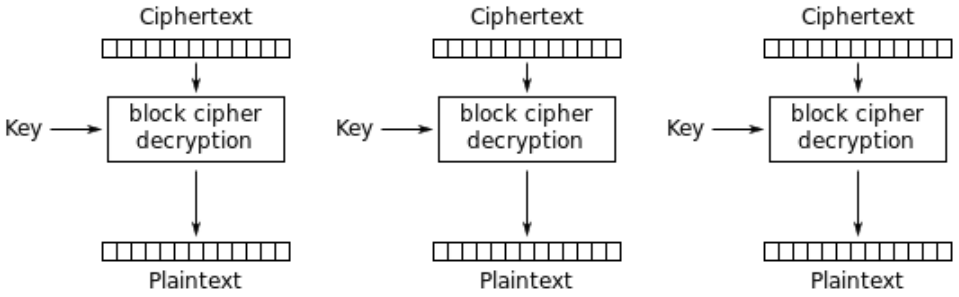
- Padding
    - Not always exact size (message and encryption)
    - Padding oracle attack happened due to bad paddings

Table ofContents

ECB



Electronic Codebook (ECB) mode encryption



Electronic Codebook (ECB) mode decryption

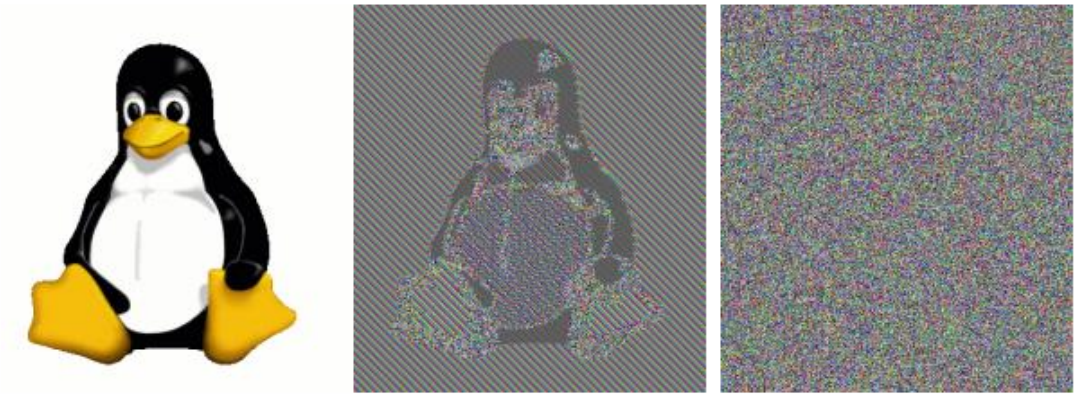
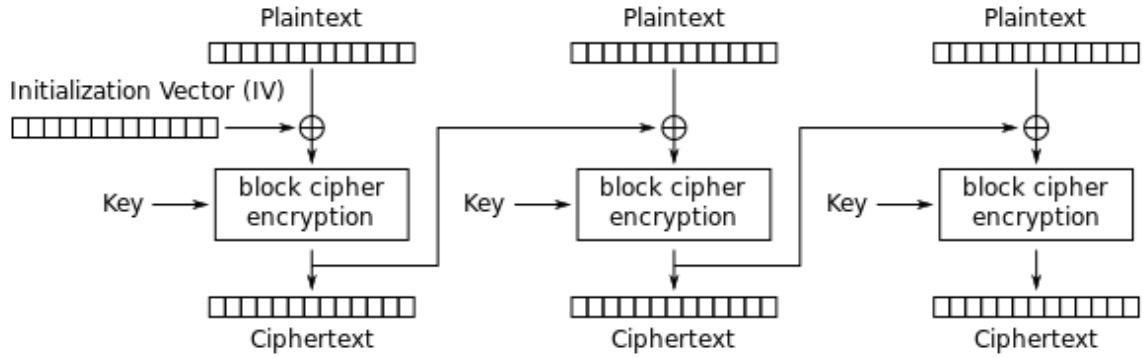
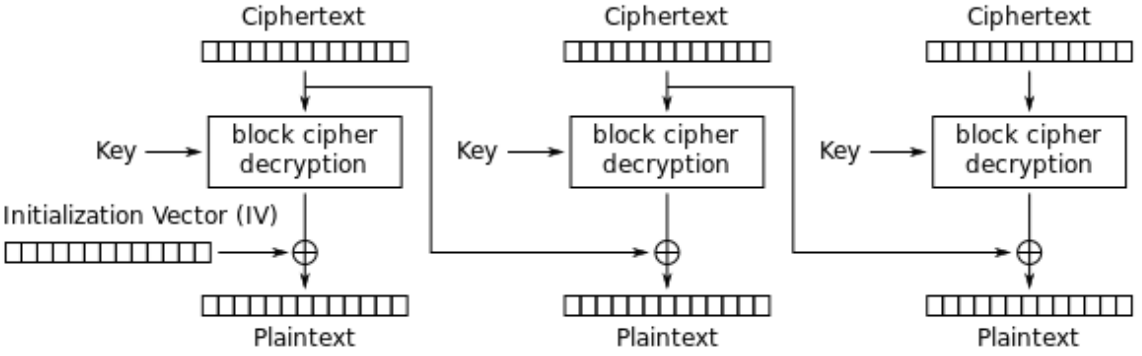


Table ofContents

CBC

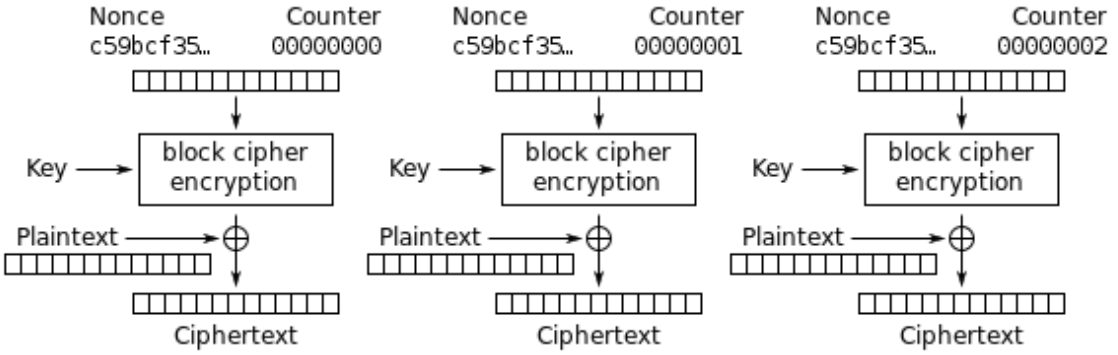


Cipher Block Chaining (CBC) mode encryption

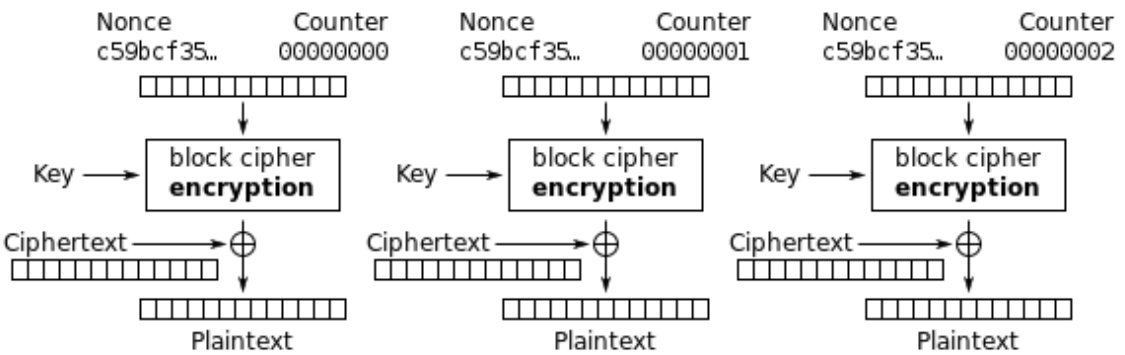


Cipher Block Chaining (CBC) mode decryption

CTR (diffie and hellman)



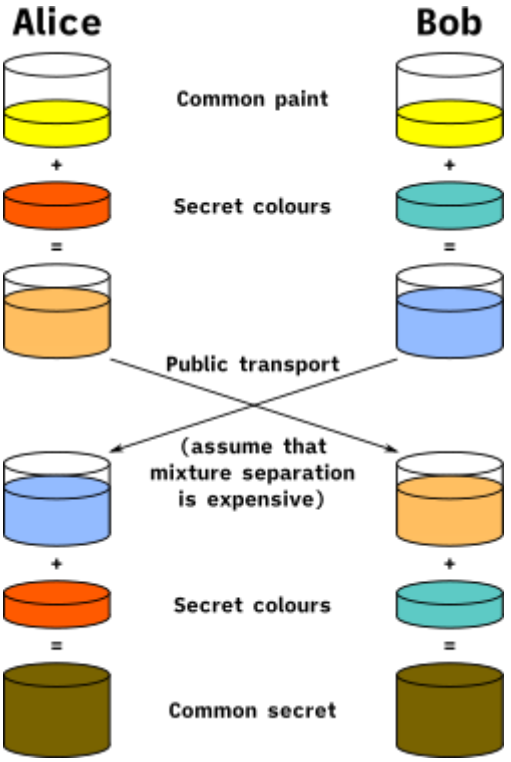
Counter (CTR) mode encryption



Counter (CTR) mode decryption

Key Problem

- We don't know security works until it fails
- The key problem
    - One time pad's problem was the one time pad
- How do we transmit the secret of the key? How do we make it secure
- What if we want to write messages to two people
    - Do we use the same key for both?
    - If we wanted confidentiality we would need many different keys
    - nC2 keys -> n^2 keys needed
    - Public key cryptography
        - Asymmetric cryptography
        - Different key to encrypt and to decrypt



Asymmetric Cryptography

- Ralph Merkle's Idea
    - Gives confidence that you are talking to one person but not someone else
    - But how does Rosanna communicate which sentence she is using without that being intercepted?
        - She can pass some arbitrary information (i.e. the number in plain text for us all to see) that tells Richard which sentence she has resolved, then they can communicate using the secret
- Work factor
    - Amount of work a defender does vs attacker
- Diffie Hellman
    - A way to talk and generate a key and people can spy but still won't know the key
    - Like Merkle, we do not know who we are talking to, just that we are talking to 1 person
    - Alice and bob example
        - Alice and Bob both know a number
        - Then they put it to a power - G and mod it by 100 (i.e. x mod)
            - Mod is good because mathematical properties travel through
            - If we do not know the power, then it is hard to solve. Discrete logarithm problem

Table ofContents

        - Alice and Bob combine the results of their keys together so decipher the secret
        - People eavesdropping only know the result mod by 100
- Just because a message is secure in the past does not mean it is secure in the future
    - With a session key, if it is broken, it only breaks 1 secret
    - However if we repeat the key, and they record all secrets, then they can break all secrets

Diffie Hellman Fails

- Flaw in how it was implemented
- 50% of web servers that used Diffie-Hellman used the same “G”
    - Could have been uncrackable if random G used

Failures

- Single point of failures are bad
    - Things where if 1 thing fails the entire thing fails
    - Happened in Silver Bridge disaster as people had high confidence in the super steel with the smartest men building it
    - Also commented how would the engineers maintain it if they found that it was broken

RSA - Rivest Shamir Adleman

- Public encrypt key are used to encrypt messages
- Once encrypted with a public key, it can only be decrypted by another key or a private key

Table ofContents

Week 4 Lecture 2

Revision

Porting

- Hackers can ring up and ask the provider to move your phone number to another sim card. Surprisingly easy to do with little authentication. Bad guys can port your number to their sim card, and this is how they can bypass the 2FA, since they have your number!

Brute forcing

- Trying every single possible option/ combination for a password
- With passwords, brute forcing is usually easier because humans generally use meaningful passwords
- If the code can be guessed one digit at a time, then it will be faster. Linear time to solve. Example shown: the opening scene from The Matrix where the numbers are cracked one by one (unrealistic)

SMS in the middle

- Want to hack bank account, but don't have your phone to get code
- Victim use a fake website, tempted by fake offer that's too good to be true and decides to buy cheap item, and enter the code into the website
- Simultaneously the hacker uses those bank details to purchase something super expensive and as a result the bank sends confirmation code via SMS
- The code is actually to confirm purchase of the super expensive thing, but victim enters it into the website thinking it's for the "good deal" thing they want
- Hacker use the code to extract money
- This kind of process can also work between three parties who are texting, where a middle person intercepts and uses the information provided by each to falsely prove their identity

Human weakness

- Humans think they and the things they build are perfectly rational and are idealised. Richard used to think of his body as a meat taxi that drives his brain around and wouldn't have minded being a brain in a jar.
- However in the end we are all vulnerable to animalistic weaknesses, and everything we build is built by animals. Our cognition is embodied. This is a type of cognitive bias.
    - Greed
    - Anger
    - Pride
    - Panic
    - Hunger

Table ofContents

    - Excitement
    - Jealously
    - Over-confident
    - Self-centeredness
    - Bias
    - Gullible
    - Trusting
    - Ignorance
    - Lazy
    - Stubbornness
    - Creatures of habit
    - Defer to authority
- How can social engineering exploit these imperfections to manipulate them into doing what we want
- Corruption, self interest and greed
    - The policemen all went to help a girl who was engaged with a policeman to prevent a fight in a pub (gang has hired the venue)
        - The abuse of entrusted power for private gain.
        - What if someone else needed help elsewhere for a much more serious issue
    - Conflicts of interest: Doing one duty often hurts your responsibility for another duty. People are always conflicted.
        - The policeman had duty to his girlfriend and to his profession.
        - Use complicated password for more security or duty to yourself to have an easy password
        - You can't bet against a horse called self interest, in times of conflict of interest humans will normally act in their self interest. We need external parties to help with situations of conflict of interest
    - Self regulation / red tape / referees
        - “Trust us, it’s going to be okay”.
        - Referees can’t be biassed, they have to be impartial
        - Organisations always conflicted (duty to public and to employees)
    - Another example of corruption: Leasing of the Darwin Port to Landbridge
        - Person who argued strongly for the leasing was in government but then went and got a job at Landbridge.

Insiders

- Walls
    - Walls on top of hills. Gives the defenders an advantage
    - Consider the Maginot Line, supposed to protect France from Germany. Trumpian in its grandeur, but did not work.
    - Square walls have weaknesses at corners. -> Walls are now rounded.

Table ofContents

    - Ladders -> People on the wall shooting people on ladders. Towers on the wall so people on towers can shoot the invaders on the wall.
    - But once people get through the walls, the insides are left undefended
- Concentric castle
    - The design of castles has been developed over hundreds of years to have greater defence mechanisms, but the attackers always manage to find a way through!
    - Once you break through one wall, there is another wall inside it, killing in zone in between because people shooting from both sides
    - This is defence in depth
    - Ships have compartments, so the whole ship doesn't sink. Only one compartment would be affected = limits effect of impact
    - Richard's favourite castle, Krak des Chevaliers is considered almost impregnable. How could attacks get inside in 10 minutes? **An insider!**
        - Insider gave faked note from pope to tell defenders to surrender
- Firefighters
    - If someone in a family is killed. Police first suspect a family member. Media reports the hunt for the killer instead.
    - Firefighters could be the people lighting the fire? -> Insider
    - People are shocked by insiders because of betrayal of trust.
    - People are sceptical of the people on the outside and trust people on the inside. That is bad.
    - We should have zero trust in anyone. Including outside people and inside people.
    - Spies, double agents
    - To ABC when consulting on how to encourage and protect whistleblowers to approach with information. "Can you trust your staff?". ABC replied "Of course we can". Planting someone on the inside would be the easiest way for ASIO etc to get information.
- Whistle blowers:
    - A person, usually an employee, who exposes information or activity within an organisation. Everyone hates whistleblowers, they often get attacked
    - Whistle blower's handbook: spends first bit warning about the consequences of being a whistleblower
    - Whistleblowers and their anonymity ties into side channel attacks as well. Even though the form is "anonymous" it's often possible to work out who blew the whistle by what information they give to the authorities
    - Snowden (ex fil NSA info when CIA employee and subcontractor)
    - Wikileaks
    - Chelsea Manning (Adrian Lamo) Collateral Murder Army Lady Gaga)
    - Andrew Wilke - ONA Iraq War based on a lie (WMD)
    - Grace Tame and Brittany Higgins (reporting on issues in the institution)

Table ofContents

    - “Whistleblowers and their anonymity ties into side channel attacks as well. Even though the form is “anonymous” it’s often possible to work out who blew the whistle by what information they give to the authorities”
- Horror movies
    - “The call is coming from inside the house” is so unsettling because we see the home as safe and everyone in it as trusted (M&M theory)
    - Zombies, werewolves, vampires. They look like a human, they were something that we trusted. = Shock!
- Why do we have insiders?
    - Corruption
    - Greed for money
    - Different value system to the organisation
    - Interests of the public
    - Blackmail eg. if family is threatened
- We normally try not to think about insiders because they make us feel sick!
- Who will watch the watchers? Everyone could become corrupt.
- We have to build a design systems that are reliable in the face of these challenges (i.e. double agents, insiders, corruption from the inside in the real world)
    - If no one is watching you, then it is not a well designed system.
    - Wherever there’s no oversight or inadequate oversight, it’s going to fail. There needs to be red tape because self regulation does not work.
- Notion of Zero Trust: let’s not just have a perimeter, let’s make security hurdles inside the organisation as well. Even if people get in they can’t access much.

Solution to prisoner’s dilemma

- The dilemma
    - 2 split ball - if both people choose split ball then money is split 50-50
    - 2 steal ball - no one gets anything
    - 1 split 1 steal ball - the person who chose split gets nothing, person who steal gets everything
    - Majority of time 1 split 1 steal outcome happens.
    - Normally the fear of being the sucker far overwhelms the desire to share
- Golden Rule Game example:
    - People don’t want to be the person who loses, so they would choose to steal. No trust.
    - PersonA tells PersonB, “I am going to steal. And I will give you half afterwards”
    - PersonB argues that both splitting is the same outcome. But PersonA is adamant about sticking with their choice of stealing.
    - People hate PersonA after a long argument.
    - When they revealed their choice, both people chose to split.
    - Afterwards it was revealed that PersonB was NOT going to share and had been lying about promising to share
    - Sometimes there are wonderful things about being human. Not all our weirdnesses are flaws.

Table ofContents

Week 5 Lecture 1

Review

RSA and Session Keys

- Work out a key that doesn't work very long
    - Each time it is used, use a new key each time
    - Maintains **forward secrecy**
        - Using the same key creates a single point of failure
        - If something is recording everything, and in future the key is broken, then all messages will not be broken by 1 key break
        - Using public key cryptography RSA to establish initial session
        - They confidentially work out a session key and use something fast like AES (RSA/Diffie Helman always slow - only use for hard part)

Correct Horse Battery Staple

- Using 4 words is easy for humans to remember but hard for computers to brute force
- However people might not pick them randomly - uncertain
    - Can use a machine to generate passwords randomly
- 4 words = 2^44. Assume 1000 guesses/second. 2^44 / 2^10 = 2^34 seconds
    - = 2^28 minutes = 2^22 hours = 2^17 days = 2^9 years = 550 years

Integrity

- How can we check when things were tampered with e.g. wills, photos, agreements
- Things that are hard to fake: driver's licence, passport, money
- Physical things are often harder to forge than digital things

Puzzles

- What to do in an exam if Moodle crashes?
    - Email exam instead
        - What if email does not work either due to internet failures?
            - Message us on a phone number & send us a hash of the exam
            - A hash gives you integrity, that something hasn't been tampered with
    - Honour system
- Telegraph
    - In the wild west, with a bank in the town
    - Seb goes to the bank and asks to take out some money from his account
    - They use a telegram to ask the main office whether Seb can take out the money
        - They then reply yes
    - What can a bad guy do?
        - Snip the cable, to intercept it - man in the middle

Table ofContents

        - Replay attack - network attack where valid data transmission is repeated or delayed
    - What can the defender do?
        - Have a secret code
        - Improve physical security
        - Folding in a nonce (i.e. something that changes all the time like timestamp) to the message to stop a replay attack
        - Cryptographic ways to attack messages
        - Almost impossible problem to solve
- Password files
    - Need to login to each computer you use. Type your password in & computer checks that what you input matches the DB
    - But the inside of a computer isn't secure, so you don't want passwords to be in plain text
    - Instead store the username & a hash of a password
        - Everytime you login it hashes the password, and then compares it with the file
    - Now, the attacker has to brute force it to find the actual password / use a dictionary (of common passwords) attack

Hashing

- Hash function
    - Takes one input and produces one output
        - They should be related e.g. through a deterministic function
        - Generally a one-way function
    - Fingerprints are essentially a hash of a person
    - An example summary could be the paper deed of a property/land
    - Properties of hash functions
        - Deterministic (always the same result given the same input x)
        - Easy to compute
        - Hash function and hash are public knowledge
        - Avalanche property - small changes in the input, have large changes in the output
            - Every bit in the hash is equally likely to flip or stay the same after one bit in input changes (XOR)
        - Generally have a fixed size (no matter the input size)
            - Functions not too big (or else just send the original)
            - Pigeon hole principle -> hash collisions
            - Collisions should be uniformly distributed
    - Verify with certain properties of an object
    - Non-crypto means, CD Tracks, fingerprints, proof of work etc
    - Shazam -> records the (invariant, salient) fingerprint of the song to find the song
        - Two related people shouldn't have related hashes
    - A hash is not the same as a digital signature

Table ofContents

- Hash collisions
    - Two related (similar) people shouldn't have a similar hash, changes in the input lead to changes in the output
    - Welp
    - What if multiple entities have the same (similar) hash?
        - The bad guy can make collisions to happen
- Cryptographic Hashes
    - Normal hashes are not resistant against attackers
    - Hackers will attempt to exploit hashes by creating same key hashes or reversing a hash
    - Send hash and message in different channels to verify the integrity of the message
    - Hashing function and the output are made **public knowledge**
    - Hash the passwords and then store them. Should never write down the exact password anywhere, no one or no system is fully secure and trustworthy.
    - In this course hash == cryptographic hash
    - A good cryptographic hash comprises of three properties
        - **Preimage resistant** (Given f(x), can't easily find x)
            - Irreversible
        - **Second preimage resistant** (Given x, can't easily find y where f(x) = f(y))
        - **Collision resistant** (Difficult to find a pair of x and y where f(x) = f(y))

Preimage attack

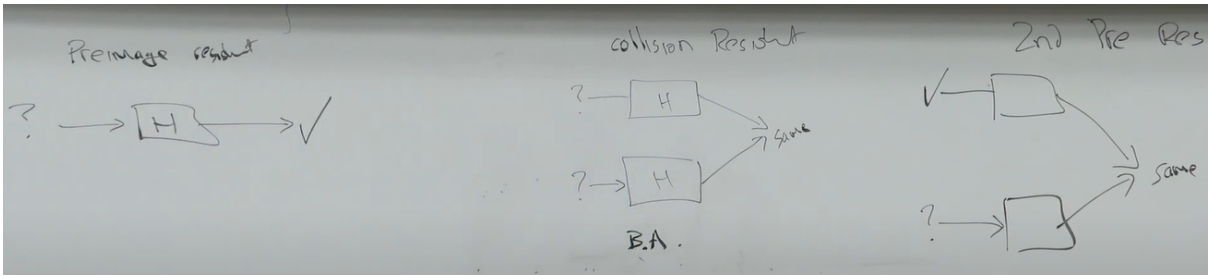
- Message = pre-image, hash = image
- Given the hash can you work out what the message is?
    - Brute force it
    - Try and find the inverse of a hash
- Want hashes to be pre-image resistant - hard to find input given the output

Birthday attacks

- To find the probability (p) of at least two people sharing a birthday in a group of n people.
    - p = 1 - P(365, n)/(365^n)
    - It can be approximated by finding p = n^2/(2 * 365).
    - The number of people required for the probability to be a certain number p is n = sqrt(2 * 365 * p).
- Brute force and try all possibilities until a collision occurs.
- Collision resistant
    - Hard to find a collision
    - Vulnerable to a birthday attack
- Preimage resistant - change only the new file until a collision
- Second preimage resistance
    - Find a second file such that the hash will collide with the first file

Table ofContents

    - Not vulnerable to a birthday attack
- Only has half as many bits of security as you expect with the birthday attack (sqrt(all space))
    - Therefore, hash output should often be 256 bits



Hash Algorithms

- MD5
    - Cryptographically weak, could be cracked quickly (preimage attack)
- SHA/SHA1/SHA2 (SHA128/SHA256)/SHA3 (Secure Hash Algorithm)
    - Bitcoin uses SHA256

Hashbrown

Table ofContents

Week 5 Lecture 2

Insiders (Revision)

People in power

- People in power want to stay in power for many reasons- may believe they are the best choice, money
- Trustees are making calls for other people but aren't usually overseen -> recent case in qld??To change laws you need to have will, power, money, and this frequently doesn't occur

Look for Secure designs and systems with checks and balances to ensure a single person doesn't go rogue (susceptible to conflict of interest)

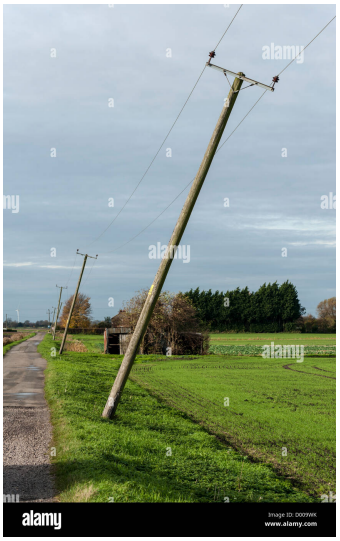
Security is all about levels of hierarchy, privilege, insiderness

Panopticon/Chilling effect

- Animals in zoos have been found to act differently when they are watched

Remember you are a chimpanzee

Privacy



- Privacy and Security are highly related issues
- Check if your telegraph pole is straight or leaning (a little lesson in maths/physics)- the force of wires pulling unevenly on the top of the pole causes a massive force on the bottom like a lever and the pole starts to lean
    - Similarly- a tiny force applied unevenly over time will eventually cause a "leaning" in a system
    - Consider- banks-> banks want to take your money, you want extra money-> stays at tension, balanced

Privacy is a Telegraph Pole

- Government: Wants to know about us
    - Crime aspects: To protect us
    - Tax aspect: Interest of the public
    - No reason to collect data or delete it
- Companies:
    - Wants data to make money
    - No reason to collect less data or delete it
- You
    - You might like high privacy

Table ofContents

    - AU, UK, US, citizens often trust their government such that they do not mind about privacy
    - This is what we are concerned about as we do not have much tension over privacy as an uninterested community

Issues

- Tricky
    - Lots of good reason to collect data for government
    - We can prevent crime and bad things from happening
- Zoo?
    - Animals in zoo are being watched all the time
- Human rights?
    - The feeling of privacy is nice
    - Chilling effect: When worried about what people will think, they are less likely to do things. More creative when unobserved
    - When Cardinals vote for a new pope it is completely private. Votes are burned after counted secretly
    - People watching you change behaviour. Let us be less controlled. Observation is a form of control over us
    - “I have nothing to hide” but what if you just want to be a private person with your own thoughts?
    - Phantom of Liberty- film clip (What if we didn’t mind relieving ourselves in front of people but were conscious of eating in front of people)

Tranquillity

- Thinking you could use algebra and maths to prove things are secure
- One weakness is invalid proof
- Another weakness is that it is not end to end
    - Only proving some mathematical model works but not what actually is going on
- Example
    - Belle Appagua??
    - Classifying secret information
    - Proving systems with this model could not leak information to people
    - Proof showed it was impossible
    - Someone found a breach
    - If at one security level, then were promoted, it was able to undo the system
    - Mathematicians claimed that this was not possible under assumptions. These assumptions are called **tranquillity** - putting things in assumptions
    - In **security, things go wrong because tranquilities are violated**

Table ofContents

Yes

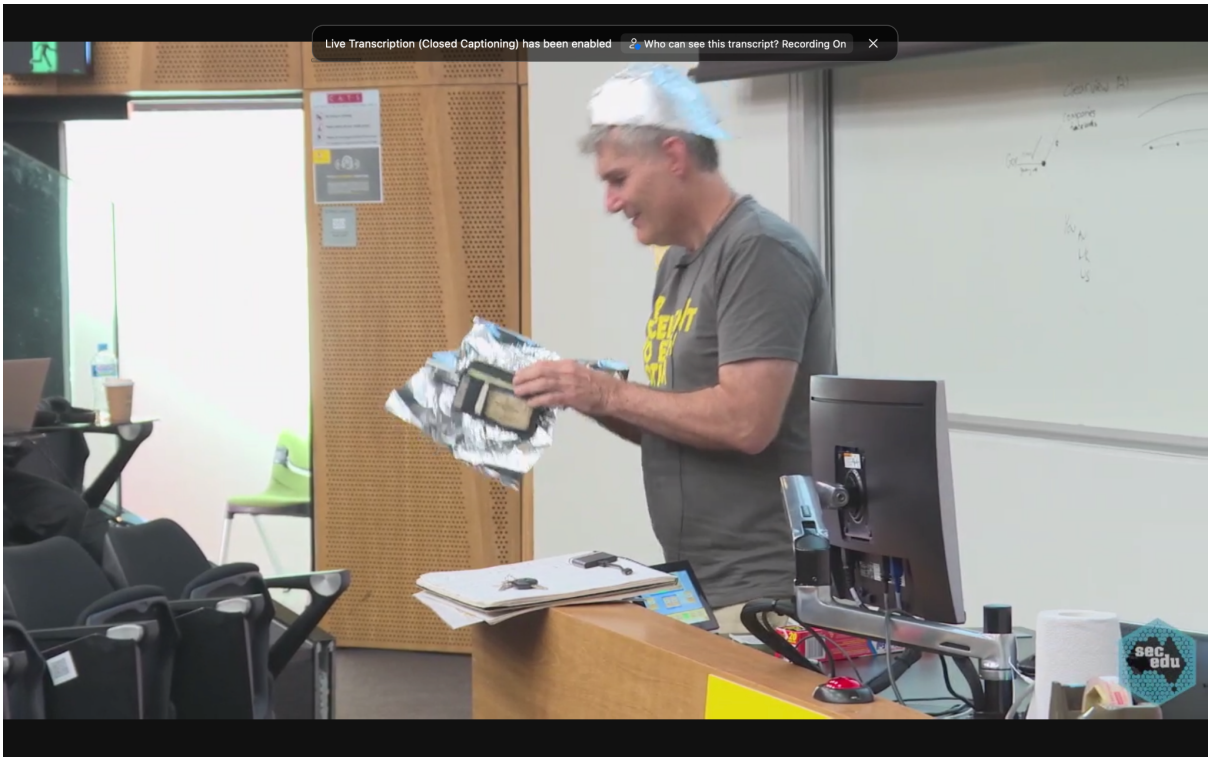
- More information police have, the easier the job
- However there is a balance between reducing crime and life

Interests

- Don't assume interests with government is always aligned
- They may change. A government's interest can change. They have your data forever
    - Denmark during the Nazi expansion
    - Tutsi and Hutu in Rwanda
    - Things collected innocently could be used for nefarious purposes later

Panopticon (Chilling) Effect

- One guard in a tower
- Prisoners THINK they are being watched



Tin foil lecture (It works!)

- What signals can you receive through tin foil? Is it the ultimate form of security 💪😳

Twin Towers and Changing

- After being told to evacuate (after first plane hit) people took about 8 mins to get out
- All lifts and stairwells (save for one, which was structurally damaged) were destroyed
- Only Rick Rescorla actually eVACuated, head of security at Morgan Stanley

Table ofContents

    - Richard's role model
    - Recommended earlier to Morgan Stanley/port authority about the structural weaknesses of the Twin Towers
    - Made everyone practice evacuation drills every week
    - Overruled official advice and told everyone to evacuate- saved 1400 people
    - Really good at designing, planning and executing a compromise solution and very exceptional at frame shifts

- People suck at doing frame shifts -> doing something pretty normal (going on a date, eating your lunch) and shifting to an emergency mindset

Table ofContents

Week 7 Lecture 1

Authentication

- Hard problem that will be hard to solve

What are the ways we can identify someone from inside a box? (As a computer)
How can a computer ever know that a user is who they say they are if they've never met the person, the only solution is to use data (since they only receive and send data)

1. **What you know** - shared secret
2. **What you are** - Biometrics/How you walk - creation of data. This is a kind of SECRET that people can intercept, manipulate, copy.
    - Another problem: if this data is stolen, and/or leaks out, you can't refresh or change it! It's compromised forever.
3. **What you have** - RSA token or phone. This comes down to data too.

- We call these ^ authentication method factors
- At the end of the day every method is data. To the outside world they seem completely different and safe, but they're not completely different factors, to a hacker. Snip the wire, insert my signal, and it's the same method of authentication.
    - Physical control so that people can't snip wires… it's never end to end.
    - You could impersonate someone. Eg, False fingerprints.

- Bishop Berkeley was a philosopher who advanced the theory of immaterialism
    - A philosophical theory that material things have no reality except as mental perceptions.
    - Argument by stone: your only argument against someone's idea is that you think their idea sounds ridiculous [Samuel Jackson]

How do we authenticate in the real world

- Things you rely on:
    - How someone looks/sounds
    - Shared experiences
- Phishing is when someone tricks you to click on a link, by pretending to be someone else
    - How do you know who is a trusted source?
    - This is an example of Authentication failure.
- Identity theft: If someone has enough information on you they can steal your identity & can authenticate themselves as you
- For convenience we ask people to authenticate as little as they can. Because authenticating annoys people.
    - SSO/cookies reduces security for convenience

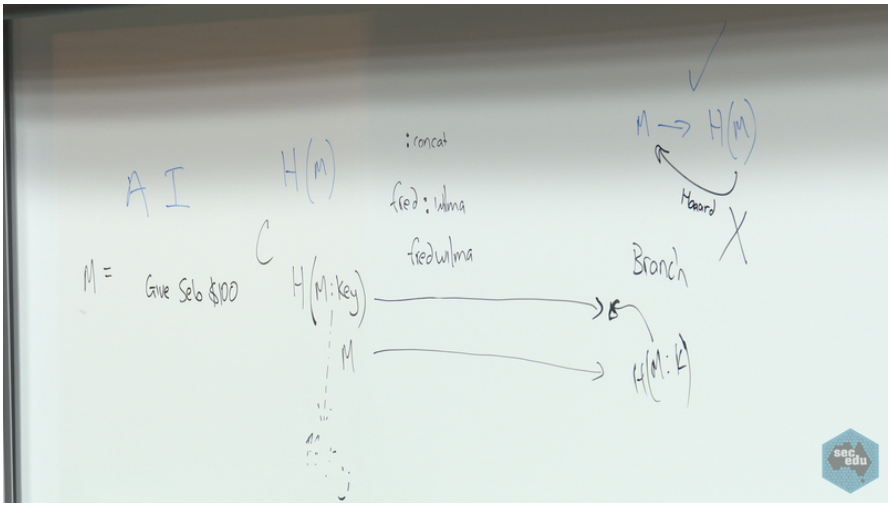
Table ofContents

- We have to make sure the person logging in is still the same person if we don't want to authenticate constantly
- But doing that weakens security.
- Attack authentication AND method of persistence

MACs (Message Authentication Codes) and HMACs / Keyed Hash

Integrity problem: we don't want the hash to be tampered with and we have **authentication** problem, we want to make sure the person is really who they say they are

Possible solution: Before encryption and RSA was widely used, a Message Authentication Code was a method that could be used to ensure authenticity and integrity of a message when sending a message.



- Requires message sender and recipient to be the only two people that know the key
  - If we fold a key into a hash then only the person who has the key can verify the hash
  - Attacker can see both messages being sent from C, but cannot compute key (preimage resistant hash)
  - This method gives authentication and integrity (not tampered with), however not confidentiality since the message is public
  - Integrity check: Send the message then the authentication code so when the receiver hashes the message, if the hash does not match the authentication code, the receiver will know that the message has been tampered with (tamper evident)

The issue with H(Message|key) - Collision attack

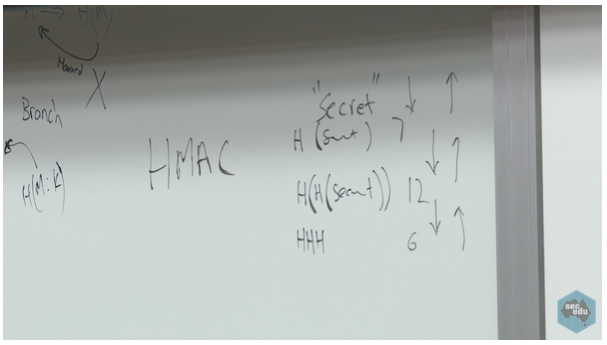
- If M = "hello" and key (secret) = "123", then H(M|key) = 34782384 (e.g.)
- If M = "hello1" and key (secret) = "23", then H(M|key) = 34782384 (as well)

The issue with H(Key|Message) - Length Extension Attack

Table ofContents

- Take start of message, hash it, combine with the next block of message, hash, combine again and so on. Hash so far includes the key

- Consider H(secret|test) = 1234567
- And, H(secret|testhello) = 7834364
- Given H(secret|test) = 1234567, we can determine the final state of the hashing function, then instead of finalising the output, we then continue the hash for 'hello' H(H'(secret|test) | hello) = 7834364
- Because the key was used at the beginning of the string, it has already been factored in into the internal state of the hashing function



S/KEY (by Leslie Lamport)

- A precomputed finite list of keys, starting with X, then H(X), then H(H(X)), H(H(H(X)))), .
- Use the rightmost key first (server needs to remember this key), then the key just before it (server can verify hash of key is the last key), and so on, each time server just needs to remember the last key and check that the hash of the each key offered matches the most recently used key**.**
    - Essentially becomes like a one-time login system, so it doesn't matter if other people overhear it
    - Server just needs to store the initial secret & a counter for which login you are up to
    - It is a bounded sequence
        - Using something like Google Authenticator/RSA SecurID can make the sequence infinite
            - Can be time-generated or hash-generated one-time passwords
            - RSA SecurID was hacked in 2011
            - Vulnerable to replay attacks and MITM

Table ofContents

Week 7 Lecture 2

- Movie for tonight is the Truman Show
- Recommended the book 'Klara and the Sun' by Kazuo Ishiguro

Data and Governance

- Richard suggests we listen to his podcast episodes on data
- There have been changes with time as to the meaning of data
    - Previously, it was talking about simple objects and the study of data itself would not have been a point of discussion
    - Now, data is important as computing collects data that you can use
        - Seen as an end in itself
        - However, non-security people only believe that data is good and aren't aware of the new problems and weaknesses that are emerging
- Even though honesty is seen as a mark of integrity/trust, being truthful on forms can be a risk
    - Should lie because you might not trust the collector of information to be good/competent → there is a risk you don't want to take
        - Might also just have their own failures
    - i.e. **letting someone holding your baby**
        - Just because you don't think they are evil doesn't mean you trust them.
        - **They might also have something else on their mind i.e. already carrying their own child→ conflict of interest**
    - **People won't be able to look after your data as well as yourself. But in the end, no one is competent enough to look after data.**
    - Once you've given the data to someone you now have to trust them and hope they won't be conflicted
        - Can hack into machines to get into your databases depending on their resources/determination
        - Only place that might be able to keep data secure is the NSA
- Census
    - If you are recording data about yourself that you know people are going to look at it, people might lie/exaggerate
    - National census tells you to be honest
    - **Suggestion that someone could reconnect your name with your data after 99 years has its own challenges**
        - Insiders could access it, it could be breached or leaked, might still be used despite this promise if it's an issue of national security
        - **Collated data is attractive to everyone e.g government**
- **Privacy act** - states but does not control
    - **Privacy Act (Cth) regulates larger companies, most of the federal gov't [have exempted themselves from their own laws]**

Table ofContents

        - Politicians and political organisations, i.e. parties, may be exempt from the Act
        - Controls PII
    - **State legislation does also exist**
- **PII:**
    - Used as an abbreviation for **personally identifiable information**
    - Tight definition which is controversial depending on the meaning of 'information about an individual'
    - E.g. Information about a child's DNA, is it yours or not? They're related to you, but it's not directly about you.
        - Data about network communications by themselves aren't about you but might be happening because you are making a call
    - Have been debates about what's personal information
        - Data that is one step removed from you is not personal information.
    - **Difference between personal vs private information**
        - Personal i.e. Richard is a man is not necessarily private
    - **De-identification is also controversial**
        - Process you do to data (not an end state)
        - **Can also re-identify data even if we strip some information. i.e. Vanessa and Victorian Health Records**
            - **So if someone's information is missing we could guess what it is based on surrounding information.**
            - Used birthdays to identify particular individuals depending on the day, location
                - Quite public information that's been shared
        - What you know about individuals in a dataset is relative but the Privacy Act operates in something being in or out (either personal data or not)
- Naive idea that a piece of data gives away the link to you
    - **Data grows in value as you have more of it→ double data doubles the value**
    - **There's a network effect. Once social networks i.e. Facebook know more information about users, the whole is greater than the sum of the parts**
- Data lakes (the collection of a lot of data) are tempting

Something Awesome

- People are asking for extensions for a variety of reasons.
- There currently exists a no-fault two day extension that students can use once this term that requires no explanation
    - Can submit Something Awesome on Sunday without needing a reason
- If you've been affected by something, you can ask for an extension providing you have a reason→ might be up to a week (don't know whether this is finalised)
    - Need to identify the criteria
    - Need to tell the course account, tutor
- If you need more time than Week 9, you need to apply for special consideration

Table ofContents

- Video is worth 10 marks and is 2-3 mins due on the same date as the deliverable→ this information will be updated on the course outline soon
    - Need some documentation attached to it
- Criteria for marking is dependent on it being a challenge
    - If one thing about your project impresses the marker, it is worth a credit; if two things impress the marker, it's worth a distinction; if three things impress the market, it's a HD
- Need to reflect on it→ have you achieved your objective
    - Could include challenges, examples of what was impressive about it, what you would change next time
- No word limit but the tutor has 30 mins to mark it
    - If it's not an essay, do a 3-4 page report with an appendix that's sensibly linked.
    - If it's an essay, the report could be shorter
- Non-assessed presentation in Week 10

Video

- Dr Strangelove or How I Learned to Love the Bomb at 6:07-11:49
- What do people do when they get the go code

Data breaches

- Breach is a good name as breach has connotations that makes people more interested in it
- 2003 California law - 2005 action
    - California brought in a mandatory disclose law: if hackers attacked you and stole personal data, it was mandatory to disclose it in a public way that couldn't be hidden
        - Need to tell the stock exchange, which affects the share price
        - This makes the board unhappy and encourages people to pay more attention to securing their servers
        - Now they are spending resources on preventing breach instead of covering it up.
    - Before that, people would not disclose it as it reflects badly on them and might encourage other attacks
        - Naturally want to keep it a secret to the extent they hired people who had breached them
    - Public didn't realise how big it was until the 2005 attack
        - Companies in California started to protect themselves, eventually leading to a high demand for computer people
        - It's comparable to musical chairs/spoons, where we don't have enough items for everyone, as we had less cyber experts than the need for cyber experts
            - 2005 breach was an example of the music stopping
    - Other American states also brought in these laws

Table ofContents

        - **Australian eventually brought mandatory data breach disclosure laws in 2018** (more expensive than expected as we started lack)
            - Making something public and visible is beneficial
- to tell or not to tell
    - Many still don't want to do this
- Trains and masks
    - Premier said people should wear masks on trains→ did not say 'must', which meant people didn't wear it
    - When Gladys said it was mandatory, everyone started wearing it
    - When it reverted back, people stopped wearing it
    - Making things mandatory is good. But no one wants to be the first person to make something mandatory.
- **PII defined narrowly**
- **Will data breaches keep happening ?** (troy hunt's site lists the most recent data breaches)
    - **Data is becoming more valuable→ have a larger demand for it**
    - **In terms of supply, the more data there is, the harder it is to protect**
        - More enticing
    - **More people holding data, more change for people to slip up**
    - ***Everything can be stolen/broken into it***
        - We will never have a system where everything is secure
- big data plankton gold
    - There are flecks of gold in the ocean, which plankton sometimes eat. People could centrifuge it to get a lot of gold
    - Similarly, companies aggregating all the data is valuable

Data lakes

- Good name as a lake collects all the water on the ground in one stop
- **Analogy: on a bush regeneration program (aiming to make the bush more natural), they noted that a track in the bush needed a lot of work as it was very eroded**
    - This is because water lands on the ground and moves around depending on their energy. If the water is travelling faster enough, you would break the track.
    - Waters erode the track. The steeper it gets, the faster the water will go and the more eroded it will become.
    - **Solution 1: could put a drain/gutter next to the path**
        - Fun to build with a lot of earthworks→ Big, visible, expensive
        - Problematic as it goes against what you are setting out to do (restoring the bushland to be more natural) and doesn't provide a solution regarding the high-speed water at the bottom
            - What will happen to the water -> it just moves the problem from one spot to another?
    - **Solution 2: don't let water get on the path**
        - Have buffers on the steps so it falls to the side

Table ofContents

        - When it rains, just get rid of the water
- **A particular company has asked for copies for passwords(passports?) to confirm citizenship. This is an issue due to the potential of being breached**
    - Solution 1: making a digital database of the information
    - Solution 2: burning the data
- More like Data Tailings Dams than Data Lakes
    - Water is collected, aggregated, put in a spot with lots of kinetic energy. People lose interest in it and abandon it. Eventually the dams burst and residents' homes got flooded, native flora and fauna was destroyed.
    - Need to maintain it forever even when it's not fun enough more
    - Better to not collect it, but if you do, get rid of it as it's toxic
- lakes are wonderful vs mushy ground
- random vs systematic - entropy vs order
- responsibility
- Data governance
    - More roles for data governance than privacy in a firm as the former is considered an asset
    - Example: Richard collects galvanised M10 bolts with washers and nuts
        - If he didn't collect it then he would think back with regret that he should've got it. He didn't collect it so he had to go and buy it.
        - We all mentally hoard things (not necessarily physical)
        - People think the things they're collecting are not useless. It makes sense to them. But they're all lunatics.
    - Data governance is similar to hoarding as these pieces of information might be useful one day
- Marie Kondo: get rid of things that don't spark joy
- Data wants to be free
    - There's a notion that if data is kept secret, there's no value to it→ people believe we should make use of it
    - When people say data wants to be free, they aren't talking about their own but rather your data (governments discussing their citizens, companies talking about their clients)
    - Some of the 'data wants to be free' mentality is very valuable as it's not linked to personal information i.e. collecting scientific information about planets would assist the entire scientific organisation
        - Data is still valuable, which enables us to do a lot of positive things
        - However, there are still risks present
- NAPLAN: three step path (collection, published and have decisions make)
    - 1. If you can measure the data, you should get the data
        - Why wouldn't we test students about their literacy? Allows us to see if there's a problem in a particular school/area/age
    - 2. If we got the data, we might as well publish it
    - 3. If a big dataset is public and available, we should make steps based on it
        - Influences budget given to schools

Table ofContents

- In the UK, public data about schools was commonplace and data was free
    - Had been manipulated by removing low-performing students (example of a pervasive decision)
- camera footage
- 1 - tempting to steal
- 2 - tempting to use - scope creep

Tailings Dams

Data Breaches

- Identity Theft - in Australia costs over $2 pa, 13% of surveyed Australians were victim of identity crime in the previous 12 months (2017) - Australian Institute of Criminology
- More? Data has its own value. Value of personal data now exceeds the value of all the world's oil reserves.

Big Data

- Data lakes
- Aggregation
- Value not additive (non linear! Amazing)
- De Identification
- Never deleted!

Openness

- "Data wants to be free"
- Open Government
- FOI - federal
- GIPA - Government Information (Public Access) - state

Regulation

- Privacy Law -
- Mandatory Data Breech Disclosure - **Notifiable Data Breaches**
- Telecommunications and Other Legislation Amendment (Assistance and Access) Act
    - ASD press release: https://www.asd.gov.au/publications/statement-tola-act-2018

Secrets by the state - censorship

- Principle of openness
- The Fourth Estate
- FOI
- Wikileaks
- Stasi

Table ofContents

State Surveillance

Social Credit

OPSEC - under surveillence

Command and Control

Nuclear

Dr S - 6:00

The cold war

Hiroshima, Nagasaki

> *And he alone, in all the world, must say Yes or No to that awesome, ultimate question, 'Shall we drop the bomb on a living target? - Truman*

Actually Truman (succeeding FDR) just stood by - airforce had control.

- reasserted control after second bomb

Dec 60 Agnew visited NATO Germany. "nearly wet my pants." P258 C&C

PALS - 00000000 - (proscribed vs premissive)

The Terrorist Threat to World Nuclear Programs (Bruce Blair former minuteman launch officer, argued it would take 4 people working together to launch)

- Read about the known Broken Arrow Military Nuclear Incidents
- Thule 1968
- Recent Russian explosion (2019) - Norway detection side channel every contact leaves a trace ...
    - Toilets

Since 1950, there have been 32 nuclear weapon accidents, known as "Broken Arrows." A Broken Arrow is defined as an unexpected event involving nuclear

Table ofContents

weapons that result in the accidental launching, firing, detonating, theft, or loss of the weapon. To date, six nuclear weapons have been lost and never recovered.

- 2007 - six cruise missiles sent on plane live - left unguarded - initially decided to keep it secret
- (terminology: bent spear, broken arrow, NUCFLASH)
- The Dead Hand (Russian, fail deadly)
- Further Reading:
    - Command and Control by Eric Schlosser
    - 
    - A short history of nuclear folly by Rudolph Herzog
    - 
- weapons safety
- Command and Control
- central vs decentral
- pyramids, transformers
- force vs ideas, romans organisation trumps savagery, divide and rule Philip II, Machiavelli, JC, Napoleon, agile waterfall, human body
- strengths and weaknesses
    - Kings
    - Democracy
    - Tyrants (Plato and Aristotle) - a person who rules without law
    - Draco draconian, rule of law, cabbage death 600BC - "In a traditional ancient Greek show of approval, his supporters threw so many hats and pieces of clothing onto his head that he suffocated"
    - Dictators - *rei gerundae causa*, "for the matter to be done" - a magistrate in the Roman Republic appointed by the Senate to rule the republic in times of emergency
- single points of failure
    - the plot against America
    - decapitation attack

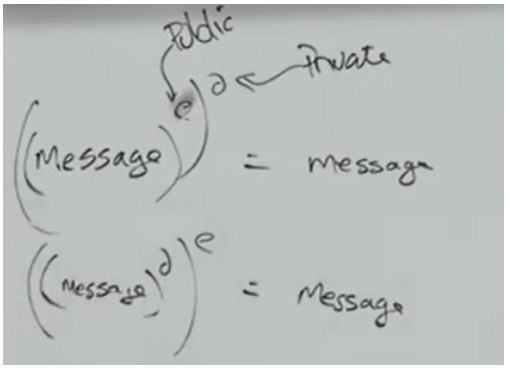
Table ofContents

unobtainium: checks and balances,

- limits (dictators 6 months)
- the estates
- leaders like leading (strangelove, Douglas Adams)
- Covid-19
- Dual Control, two man rule
- Book keeping
- Icecream

Table ofContents

Week 8 Lecture 1

- Token hardware is designed to be tamper-resistant to deter reverse engineering
- Back dooring the software
    - For example: An engineer putting a back door into a ATM so they can get money whenever they want without deducting money from their account
- 

    - Encrypt message with recipient's public key which they can decode with private decryption key
- You can use RSA to authenticate too. It is very versatile.
    - A sends B a challenge text. B encrypts it with their private key. A decrypts this with B's public key, thus demonstrating that B has access to B's private key. So this is probably B.
    - Don't actually do this. Don't use your private key on text people send you. For example: if you were to use your private key on random text people send you, they can use that to trick you into decoding past messages you have been sent.
    - Example above is signing. Similar to signing a paper saying you owe $50. Then they change it to $50000 and now you owe that much.
- Difference between authentication and authorisation
    - Showing passport is authentication
    - Having a passport to do something is authorisation
    - Authentication is more hassle and expensive to implement.
    - Government (e.g. transport) is spending more data on authentication because they want to gather data. E.g. authenticate then they can track your location moving from place to place.
    - Using cash in supermarkets is authorisation
    - Using a credit card on the other hand is authentication as you are identified by your card (and therefore can be tracked)
- OAUTH
    - Used by google, facebook etc for authorisation. Idea is to let you authenticate to login and then they give you and/or other servers authorisation tokens to allow you to do things without having to log in again.
    - Single sign on across multiple platforms.
    - Convenient but there are risks.
- Digital signatures

Table ofContents

    - What is a signature in real life?
        - A physical signature gives you both authentication and integrity, digital signature aim to do that too
    - A digital signature using RSA would involve hashing a message with crypto hash like SHA3 and then encrypting that hash using your private signing key. It would be verified by others using your public signing key.
    - It is better to use different public key pairs for signing and encrypting
    - The old NIST signature protocol was DSA - don't use it now. It was replaced by DSS, which was influenced by the NSA.
    - Snowden also revealed that the NSA gave the RSA company $10M to use a flawed random number generator in signature implementation. RSA took the money and did it.
- Authentication Attacks
    - **Downgrade/Fallback attack** is an attack in which one party negotiates to a less secure protocol therefore making that communication channel vulnerable (more likely to be intercepted)
    - **Recovery** - Hard to recover your identity once someone else has obtained it
    - At some point a digital identity must be linked to a real life person - requires work
    - Authorisation tokens can be stolen
    - The seed value for random number generators can be brute forced (pseudo-random)
    - **Man in the browser**: Similar to man in middle but using a Trojan Horse to intercept calls in applications
    - Someone can be locked out from using their MFA by brute force (denial of service)
    - MFA can also be bypassed
- Web Protocols
    - Originally, users communicated on the internet on their local network where messages were passed unencrypted, in the clear, via HTTP
    - The need for encrypted channels rose as complexities of systems increased e.g. online banking.
    - Instead of a plain, unencrypted socket, Secure Sockets Layer (SSL) was used instead.
        - HTTP with SSL was now called HTTPS
        - While it wasn't extremely secure, there was no priority to upgrade as it was "good enough" for many users
        - SSL was vulnerable to downgrade attacks as attackers simply fell back to earlier and earlier versions of the protocol with no complaints from the system.
    - This was eventually upgraded to Transport Layer Security (TLS)
        - There were some intermediate versions of TLS with terrible security which were used in smaller, less popular browsers.
        - The latest version of TLS is resistant to downgrade attacks as it refuses to accept any weak encryption algorithms.

Table ofContents

- Establishing a connection between client and server
    - A connection is setup between a client and a server using a five step handshake
    - Such a connection should have confidentiality, integrity and authentication
        - Confidentiality is important to ensure that the actual data is invisible
        - Integrity is important to prevent man-in-the-middle attacks
        - Authentication is important to ensure the client is talking to the right server and vice versa, especially when information such as credit card details are being sent.
- Heartbleed Attack
    - There was a need to detect whether a user was still viewing a page so the server would know to terminate the SSL socket if they had gone away.
    - An extension was proposed to SSL to include some Javascript on the client-side to ping the server to let the server know the user was still active on the site. This was known as Heartbeat
    - It involved sending a packet of data to the server containing some data and a number representing the size of the data.
        - The data had to be unique to the user to differentiate between all current users.
    - The server then sent the same message back to the client as an acknowledgement.
    - However this was poorly implemented as the server didn't check that the size of the data which was sent equalled the size that the packet said it contained.
    - The server decided how much data to send by looking at the size included in the packet. If the size was larger than the actual data, it would fill the rest of the response with data from its buffer, potentially exposing other users' data including their private keys.
- Certificates
    - How can we verify that a provided ip-address is the address of the site we wish to access (e.g. Amazon).
    - We use certificates
    - How do we know what Amazon's public key/certificate is however?
    - 2 Ways of Authentication:
        - Web Of Trust
            - Crowdsourced truth
            - Check with many trusted people to see if a site can be authenticated
        - PKI - Public Key Infrastructure
            - Trusted third party to provide and verify certificates
            - Browsers come with certificates preloaded of which authorities to trust
            - Domain name then tied to certificates instead of companies

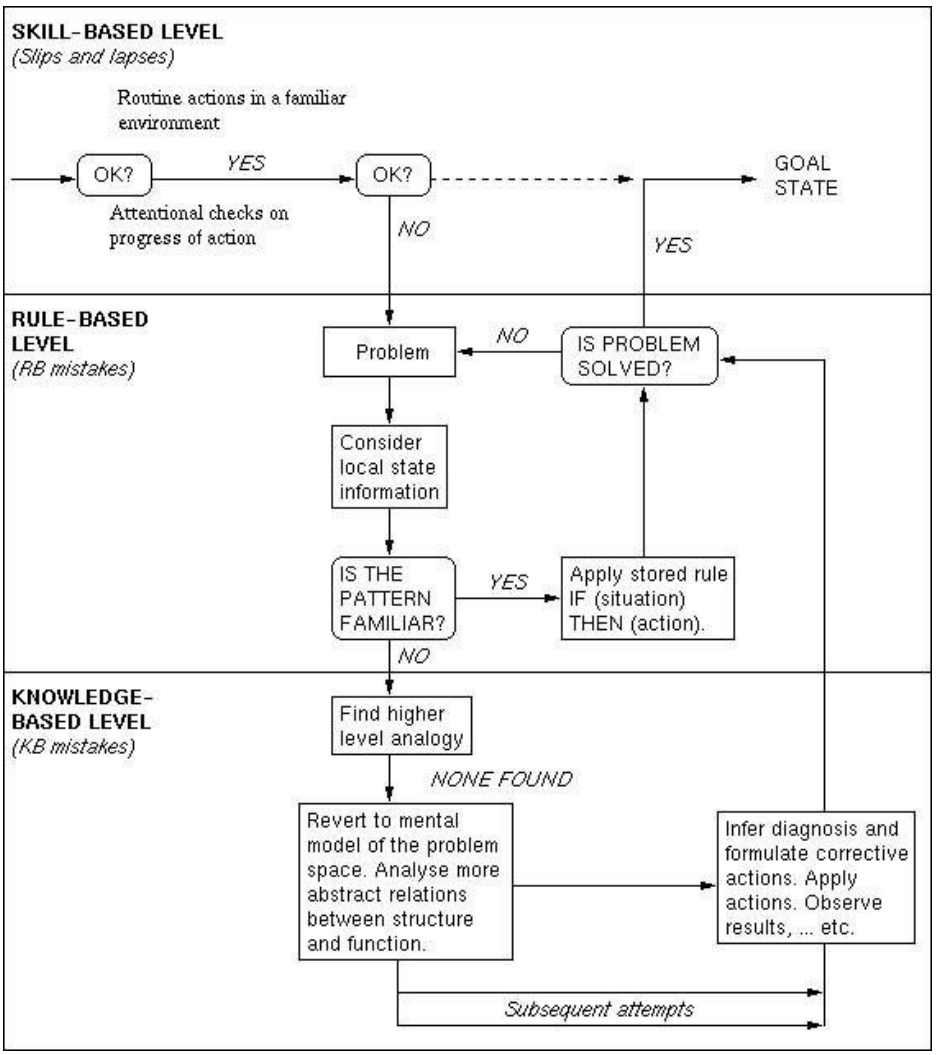
Table ofContents

Week 8 Lecture 2

Three levels you can operate at:

1. Skill base level: carry out routine things
2. Rule base level: if something happens, you have a rule to deal with it. Rules you come up by yourself
    a. Rule-based only works well for high probability risks, not low probability
    b. Example: You live on the side of a volcano and it rumbles a couple of times each year. It has been safe for as long as you know. So when someone comes and tells you to leave, you would laugh at them.
    c. If you have used the rule in the past and were successful, then you think it's a very strong rule.
3. Knowledge base level: use your general knowledge of the world and apply it.
    a. Humans like skill base processing. Knowledge base is hard and people would rather use rules even if it doesn't apply well.

Table ofContents



Signs:

- Types of signs, all which will simultaneously present when there is a problem:
    - Signs: confirm you should do the normal thing
    - Countersigns: warn you that something is different and maybe you shouldn't do the normal thing
    - Nonsigns: don't indicate exactly what you should do
- When people get multiple signs in a problem, they prioritise the one that confirms the scenario they think is happening, not necessarily the most important one

Cognitive Biases:

- Availability heuristic
    - People focus on things that come readily to mind.
    - First things you think about are more correct than the rest.
    - You don't consider what you don't know or can't see as much.

Table ofContents

- Hindsight bias / creeping determinism, the illusion of control (Langer, 1975)

1986 Challenger - Space Shuttle disaster:

- Used o-rings which were less effective in cold weather:
    - Designer set a minimum temperature for safe launch
    - On the day of launch the temperature was below the minimum
- There was immense pressure to launch on that day, so higher ups ignored the potential problems
- After launch, the o-rings collapsed and the shuttle exploded
- Normalisation of deviance:
    - On previous launches, there were serious indications that things weren't working correctly and things were going wrong (i.e. marks of leakage, things breaking, foam breaking off).
    - Because there were no horrific accidents, people grew to just accept these problems as normal.
    - People didn't focus on fixing these problems, saying they were "normal"
- Five whys: Someone tells you the root cause. And you ask why? So instead of describing, we reflect on the mistake. Diane investigated this for Challenger.

  Accident causes (Normal Accidents by Charles Perow, Just Culture by Sidney Dekker):

- Human error is often blamed but is rarely the actual cause
- Usually the error is a cumulation of various factors, because systems are complex.
    1. Human error
    2. Mechanical failure (e.g. coffee pot breaking)
    3. Environmental problems (e.g. bus strike)
    4. System failure (e.g. spare key not there)
    5. Procedures used failing
- Accidents in complex systems are very normal, not freakishly rare that deserve blame. Designers roles are to deal with the problems, mitigate them, or simplify the system
- Just Culture:
    - When there is a problem, don't blame someone but try to find the root cause (keep asking questions about not who made the mistake but why it was made).
    - Don't punish the individual mistake.
    - This culture allows for bad news to be told to everyone and then the problems would be solved.
    - E.g. Health Department of NSW, Qantas
    - A bad culture means bad news is not shared because the messenger will get in trouble. This is a terrible place for safety

Table ofContents

Week 9 Lecture 1

Security by Design

- GRC: Governance risk and compliance roles
    - Be careful about these roles but they are more about complying with legislation and standards and doing audits at a policy level
- Tension between compliance and creativity (e.g. GRC)
- Security should be **by design**
    - To make a system secure, there are 2 general approach
        - Reactive: Respond as problems arrive
        - Security is something worked out in advance
            - E.g. Non-polluting cars by design or safe by design
    - Should always try to put security in the beginning as a built-in feature
    - "Soft power" refers to how it is better to have security by design
        - Easier to get a seat at the design table before it is built than after
    - "Most effective" refers to how hard it is to add security if the design is fighting you
- Checklist for when you see a problem
    - Enumerating assets
        - Don't know how to make something secure if we don't know what we are trying to protect
        - The challenge is noticing the things we miss
            - Can't make something secure unless you know what you are trying to protect so make a list of assets
            - Most entities don't realise what their assets are until they are attacked or lost in some way
            - Quite easy to protect the wrong thing, rushing to decision leads to protecting wrong asset
            - No matter how much you try, you will most likely never get all of them
            - It is important to notice these in the design phase
        - Challenge in doing a security by design exercise: noticing the things you missed (notice them before they are attacked or lost)
        - How to minimise you missing assets or how to help notice the missed assets
            - Work as a team with diverse members who think differently (diverse as you have different perspectives)
            - Constantly add/update
            - Ask lots of questions you don't know about the design
            - Make sure you solve the right problem
            - Use checklists (help you stop forgetting things and allows others to see what your looking at [they can add their own advice])

Table ofContents

                - Put structure on assets (helps you see what categories you have missed or what you are light on)
                - Never relax - You will never have everything
            - How to make sure you are asking the right questions when you are working beyond the checklist?
                - Understand the environment
                - Ask people about the categories and you can gain more information of what to consider
    - Threat model
        -
    - List the risks you face
        -
    - What's next?

Guest Lecturer - Siva Sivasubramanian: Optus

- Important to share knowledge and receive help and help others, passing it on (not a question of competition, if we are going to be hit, you will be hit)
- Security community works as a whole and helps each other out - members of the community are apart of something bigger
- Why do you like security?
    - Started Mechanical Engineer -> Finance
    - Takes too long to become higher in the finance hierarchy (jobs)
    - Joined IT as it was becoming popular
    - If you don't know something, learn it
    - Enjoyed learning
    - By trying things, they increased their confidence
    - Search for learning, introduced to hacking which introduced into security even though knew nothing
    - Learn things which are unknown to you without fear
    - Not getting bogged down, understanding and moving forward looking for new things with hunger
    - Once comfortable you lose the ability to be more analytical (be comfortable with fluidity rather then just labelling something)
- Now that you're a leader, what is your advice to when they become leaders? What is your central approach?
    - Help team embrace change, happy to go learn -> cultivate this healthy mindset
    - Keep yourself away from pressure of the job
        - Can't hit your target if your mind is distracted
        - Keep the team away from stress, give them only what they can handle
        - Some members may be more resilient than you and you can help them lead

Table ofContents

    - A leader should face and under-write all risks of an activity and deal with them accordingly
        - Always ask members Why did they do this? If they can list points we let them go but if points are invalid then the leader should say how they should think differently
        - If the answer is that you don't know then - "pink slip"
    - Primary focus: Team centric approach -> focus on developing your team through crisis rather than just solving the crisis (rather than focusing on how to use the team)
- What principles have guided you in leading Optus's approach to government requests for customer data? How do you maintain an ethical framework that stays valid?
    - Question has a fundamental assumption: that an ethical framework and the principles that we implement for gov. standard are against each other and then how are we going to manage that? This assumption is no necessary, what matter is that we are all at the same front - we all want the same thing done.
    - We all want the best government, there is no conflict between a legal organisation and government, we are on the same side
    - Fundamental question: How is the data protected?
    - 3 Mechanisms to answer it:
        - Set of infrastructure that prevents any protection
        - Outstanding monitoring capabilities so that as the thing happened you can catch it
        - Enough logs to know where data has moved so that you can catch them
- Thoughts on offshoring data?
    - There is data you store in order to control yourself, access is monitored,
    - and other information we can put on a cloud
    - Cloud: Some countries safe to store information and some countries we should not move data thus corporations have their own rules
    - Outside a country, you want other government structure you can rely on and bilateral agreements give you that (as long as they are backed)
- Is there an increasing move to localization rather then globalisation for data? Internalisation of information stored? (i.e due to tensions rising up in the world - For example in Australia we are trying to generate vaccines ourselves so we do not have to rely on other companies and outsource)
    - Believe it has already happened
    - View data from 2 views:
        - Access of data from different locations
        - Data living in different locations
    - Earlier pre-cloud days, data used to live only in your location
    - Post-cloud, goes into locations which are compatible for you (like some countries may not be as well equipped to handle international software)
    - Risk management is involved
- Any advice on how to balance between shielding a team and developing them

Table ofContents

    - There is no specific formula, it is something you intrinsically do which is a part of your leadership development
    - When you try to document processes, you become a slave to the process
    - Rather than if you document the principles, you become more free
    - Treat everyone as an individual not a resource
- What proportion of your time is spent thinking about your team and functional problems?
    - I don't think much about team because once momentum starts building up, we all build about the operational emerging problem
    - Initial investment of time on team but post-that it is dramatically the time falls down otherwise it start affecting the process
- An investment upfront pays off in the long run. Is there a concrete example of this?
    - 18 years ago: Small team is deep rooted into processes, facing a problem, communication issues, spent time figuring out and developing the team members with exercises -> helped develop their thinking
    - Constant pulling back to change their thinking

Magic Trick

- How can we solve real world problems with cryptographic primitives?
- Distributed coin toss
    - E.g Toss a coin to determine the outcome, both people are speaking on the phone
    - How can you ensure that the person doing the coin toss is not lying?
    - No trusted 3rd parties
    - Both people toss coins? Well both people could lie
    - How can we develop a protocol so it is fair and secure
- Election
    - Characteristics we want it to have
        - A vote cannot be connected to a voter - secret ballot
        - Once a vote is written it cannot be changed - tamper proof or evident
        - Know if someone has voted or not (find if didn't vote or make sure they did not vote a second time)
        - Cannot vote more than once
        - Need to know if there is a trustworthy way to count the vote
        - Know people voted freely - not coerced in some way
        - Should be easy to cast a vote despite an individuals circumstances
        - Quick to count and have fast results
        - Other people cannot see your vote
        - Everyone votes during the same time window
        - Vote can't be changed
        - Valid people can votes based on their ID - authorisation
        - **Winners actually win and the public believes the winners were entitled to win** (allows regime change without blood shed)

Table ofContents

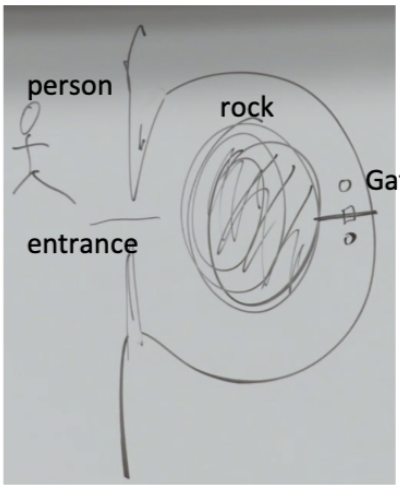
        - Verifiability
    - Real world problems are hard because we have so many conflicting requirements
    - Regime change is important
        - When in power for too long they become corrupt and self interested
        - Old fashion way was bloodshed so democracy good
        - Democracy only works if people **believe in the outcome** of the election
            - E.g. Trump: If I don't get in it is a fraudulent election
            - Trump was prepared to damage the electoral system to win
            - Can also be called verifiability - People can check themself

Zero Knowledge Protocol

- Suppose you know the formula for coca-cola and someone wants to buy for $1 million
    - If not careful and the exchange become "oh you give me that then I'll give you this", then the other party can just run off with both the formula and cash OR a tug o war can occur
    - The holder can create the coca-cola to prove they know the formula (they are locked in a room to ensure there are less external influences)
        - Could always poison the buyer
        - The maker could be monitored for the recipe in which they no longer need to spend $1 million
    - How can we know that they know the formula without them telling us the formula?
        - I lock you in a room, you make coke, you come out, I taste it to make sure it is coke
        - Need to make sure no coke in room beforehand
        - Downside: party watching can observe the method with cameras or by surveying the ingredients
        - Can be seen as a one-sided approach
        - Their knowledge can leak out in the act of doing things
    - What we need is a protocol, that tells me what I need to know but tells me nothing else - get Zero Knowledge from this protocol other than knowing that this person has the formula to coca cola
    - How can you prove something does not leak anything? Hard to prove but for that we have Zero Knowledge protocols

- Cave/Gate example - zero-knowledge interactive proof

Table ofContents



    - You know how to open that gate, can you prove to the person outside that you know how to open the gate without revealing how to actually open that gate
    - Can do this by playing a game
    - Zero knowledge protocols are always a game
    - You go into the cave by the gate -> yell I am in position now -> person outside is blindfolded
    - Then person outside says I want you to emerge from the left/right
    - Either you just walk backwards or you have you to pass through the gate
    - 50,50 chance of me using the gate
    - Do it again - 1/4 chance u were just lucky
    - Again, and again…
    - If there is a ½ chance of actually doing it, if we do it 10 times, then the probability is 1/1000 that you have been tricked
    - And this grows exponentially by a factor of 2
        - This is an interactive proof that is zero-knowledge
    - How do we know that this interactive proof is zero knowledge?
        - Could do person entering the cave one way and leaving the other but that would prove it but it would not be a zero knowledge proof (1)
        - Because the problem is you do not know how to prove that no one has learnt anything from that (1)
        - But the interactive proof that is zero-knowledge we know

- If we film this whole thing happening, from the outside of the cave. If you are watching the video, are you convinced that the person knows how to open the gate? Or even if the video shows that the inside is valid like no extra tools etc
    - Could have been scripted or altered
    - Video won't work to prove to a 3rd party because collusion may be involved
    - No way someone watching it can learn anything because nothing more is happening that we could have worked out by just faking the whole thing
    - Scripted vs not-scripted is identical
- The idea of a zero knowledge protocol is:

Table ofContents

    - 2 players - prover (person dealing with the gate) and a verifier (person standing outside cave)
    - Play the game where verifier calls out random numbers, series of yes's and no's, blacks and reds etc
    - And the prover has to do what they can do
    - If they get it right every time we start to think "maybe they can do this"

Computation Example: Graph

- A classic zero-knowledge protocol proof involves Hamiltonian cycles (where you visit every node in a graph once and end up back at the starting point).
    - The prover aims to show the verifier that there exists such a cycle in the graph without showing them the actual cycle.
    - First, the prover makes an isomorphic copy of a graph which they know contains a Hamiltonian cycle. This graph containing a cycle is also known to the verifier
    - Then, the prover “commits” the list of all the edges of the isomorphic graph and a table showing which node in the original graph corresponds to which node in the isomorphic graph.
        - Something can be committed by:
            - Encrypting it
            - Hashing it (the integrity of which can be confirmed by hashing the original message again)
            - Sending it to a trusted third-party
    - Then, the verifier will make a choice between two options as to how the prover will show that there exists a Hamiltonian cycle
        - Option A: The prover will open the commitments for the edges in the isomorphic graph which make up the Hamiltonian cycle, demonstrating that such a cycle exists in it.
        - Option B: The prover will open the commitments for the table, demonstrating that the two graphs are actually isomorphic and hence a Hamiltonian cycle exists.
        - Opening a commitment means undoing the commitment to reveal the original contents
    - https://daniel.schemmel.net/post/2016/zero-knowledge-proofs-using-hamiltonian-cycles/
- Exam
    - How to show the exam is easy without giving knowledge of the exam itself
    - Make 40 questions, students pick 20, other 20 go in exam (all questions similar difficulty)
    -

Solution to coin toss problem:

- Commitment
- Involve a person somehow locking in her choice before I toss the coin or toss the coin, lock it in and make the choice:

Table ofContents

- Commitment occurs though writing on pare through trusted 3rd party
- Hash it and send me the hash

Week 9 Lecture 2

Ice Cream example:

- Have two entries to reduce the risk of corruption to improve check and balances of the data. (example of Buckland requiring a ticket to get an incream so that one person would give it away and the second person would acknowledge it)

Command and Control

- Command and control is coordinating subsystems and can be achieved with trusted third parties, well trained people obeying professional codes, military follows chain of command
- Control is like a pyramid, it gives the person at the top the power of 1000 people
- Cons
    - **Single point of failure**
        - Ensure the person at the top is not a crazy person/corrupt
        - There are some checks and balances to ensure the person at the top does not have absolute power, i.e. separations of powers

Guest Lecturer Professor Merlin Crossley, molecular biologist

- Gain-of-Function research
    - Covid came from bats
    - Protein mutation survive on bats, check if it can survive on human cells
    - Now we have a dish of a virus which is dangerous
- Radioactivity
    - Can't see anything
    - Can only see with a geiger counter or x-ray films
- First thing looks at accidents
    - People make things deliberately that can be dangerous, and are really bad for humans
    - They think they can save the world by making the bad thing
- Why do researchers think about the chances of making a mistake in the future?
    - Researchers select for confidence
    - They want the overconfident people (not mad)
- Gene drives have potentials to wipe out species
    - However security is just chucked aside and not really considered

Table ofContents

- Testing vaccines
    - Reaction is not too bad
    - Test if it works
- No ethics clearance if you work on test tubes in australia

Communication

- Communication is about them not yourself
- Communication is when you enter an interaction with an objective and you must have an objective. The objective is always of the form, at the end of this interaction, this is how the people will change - Objective change
- Listen and understand people

Week 10 Lecture 1

Podcast

Table ofContents

Week 10 Lecture 2

Loose Ends

- Horton's Principle
    - Keeps being tempted to leave the egg he was protecting
    - In cryptography, verify the integrity of the actual thing not the integrity of a proxy for it
        - Authenticate what is being meant not what is being said
        - Mean what you sign and sign what you mean

- Supply chain attack
    - Instead of defending yourself, you have to defend what you depend on
    - A bad guy will attack what you depend upon not you
    - E.g. attacking security guards guarding an ATM

- Derivative attacks
    - You can make some money making shares, but the real money is at derivatives
        - Risk higher, returns possibly higher
    - Instead of attacking a firm with ransomware, short selling shares in that firm in order to make money (as stock price will go down if it is published a firm is hacked)
    - Random thought of Richard: Economists are generally more self interested
        - Economics based on the idea that people act rationally
        - Assumes people are generally selfish, and that assuming people are selfish makes them become selfish themselves
        - People who teach ethics are no more likely to act more ethically than people who don't teach ethics

- Replication crisis
    - Positive results are privileged over negative results in psychology papers
    - Famous results when attempted to become replicated were unable to be replicated
        - E.g. Seeing is people help when stabbed
    - Interesting thing to think about in cognitive psychology research

- Sovereignty
    - Related to the issue of supply chains
    - Do you want to control your own supply chain
    - At what level should we be in a world supply chain and where are the boundaries of what should be produced here and offshored
    - However when the war hit and pandemic hit, suddenly borders just appeared everywhere between supply chains
        - India produced a lot of vaccines then stopped shipping it out

Table ofContents

        - Pfizer was being produced and EU was taking all the vaccines
    - You can **trust a friend if their interests align with yours → what are you relying on?**
    - A supply chain can be malicious
    - Why don't we get each country to do what they are best at, then we all share? Sovereignty is the reason why we don't do that, because it's a risk.

- Data and Governance + Scope Creep
    - Most organisations have a team and policy on this
    - Governance
        - It is about ensuring in a particular context that the arrangements are such that you are sure things are the way you want them to be
        - If you got a committee, they should follow the rules. There should be terms for the committee
    - It is about the good running of things
    - For a country, it is about compliance of rules and policies and govern that the ministers act in the interest of the nation or that individuals aren't ignored
    - Right ways of using data and the checks and balances of data
    - Appeals and people checking from time to time and maintaining the current laws and policies and that they are achieved
    - It is why citizens have faith to do anything. Stuff like how you trust we get in a car and it'll work
    - **Make people think about governance and it is actually governed**

- Digital Identity Podcast
    - It is going to be big
    - It is how we monetise a lot of products
    - Everyone wants digital identity

- Humans in the loop
    - Your decision process depends on humans
    - Should you always have a human in the loop/sanity check?
        - Three mile island, having humans was critical. Needed just one person to notice something crazy was happening.
        - Wargames, humans in the loop prevented disaster
    - Bureaucrats don't like humans in the loop. As time passes, more arguments are made to remove humans from loops.
    - If humans can't go underneath the output of a system, then humans in the loop won't matter. E.g. Printing out debt letters and humans checking them. Since the humans can't see the calculation behind it, they think it's all fine.
    - Systems are good at what they're doing (properly coded, tested, built etc), then maybe we don't need humans in the loop. In security, we have attackers that attack things outside of a system's ability, meaning you will need humans in the loop.

Table ofContents

    - Humans are not as good as computers in normal operation. But when operations are not normal, humans are required to be in the loop.

- Checklists
    - You don't forget what is on the checklist
- Security requires the system to be properly functioning from end to end, and located at the ends are people.
    - Technical knowledge is necessary, but not sufficient. We need a cyber mindset - a mindset geared towards people.
- Teams are important - there is a culture of helping each other in the professional world.
    - e.g. in the Matrix clip each of them assumes that the other is working selflessly in their interests and they have absolute trust in each other.
- Security is all about people - a cyber mindset is a human mindset
    - Despite all the problems with humans that have been highlighted in this course, humans are really remarkable things - just look at what we have done so far.
    - Even in seemingly hopeless scenarios humans are able to use creativity to solve problems.
    - We just need to be aware of our flaws and weaknesses.

Table ofContents

Table ofContents