Todo:

- Reformat notes to be nice
- Think about what this week covered and shove it in so that we have it in the finals
- Move 6841 content to a different area to make it nice for them to see that extra bit
    - Just the seminars iirc
- Don’t delete the cat

When do we wanna do this btw

WEEK 8 LECTURES

Leave this sippy cat in to give determination in the final exam

Movie

- The Fog of War (this week)
- The China Syndrome (week 9) going to be in the exam - question based on a scenario in this film

When something goes wrong - What is the root cause?

- All cyber issues are due to human error (not necessarily 1 person, could be many)

Root Cause Analysis

1. Blame everything on the last person to touch it
    - Old airline industry blamed the last engineer to sign off
2. Culture - the culture of a company or organisation is to blame
    - Difficult to change

    - Doesn’t really tell you what to change
    - An easy thing to throw money at so that it looks like progress is made: Saves reputation rather than fixes root cause
3. The whole system; it was a “normal accident” -- the system was too complex/badly designed and something going wrong was inevitable. That things went wrong in this particular way was just bad luck.

Human Weaknesses

Honesty

- Commander in Cheat - book about how Trump cheats at golf with his tiny hands
- Humans lie
- Universities get students to sign honor codes·
    - They did a study to check effectiveness
    - Results: people were more honest when they signed the honour code before rather than after filling out information
- Richard didn’t jaywalk for the first 10 years of his kids lives because jaywalking while telling them not to jaywalk would be dishonest
- Richard didn’t lie about Santa ‘worked around by omission’ but ended up telling them the truth and it spoiled his kids’ fun :(
- People lie to themselves about their own honesty
- When asked who contributed to these lecture notes, people will honestly say they helped, but *will people lie about contribution? ooft*

Misdirection and limited focus

- 'Chekhov's Gun' is a concept that describes how every element of a story should contribute to the whole. It comes from Anton Chekhov's famous book writing advice: 'If in the first act you have hung a pistol on the wall, then in the following one it should be fired.
- people are bad at picking the right features for focus
- We often look for a few factors, in a very large space (needle in a haystack)
    - Attackers try to get us to focus somewhere else
- logically important vs psychologically salient
    - People SHOULD focus on what is logically important
    - People USUALLY focus on what is evident

similarity matching

- is when people look for similar situations that happened to them in the past that they are familiar with and applying it to the current situation.

Frequency gambling

- If many patterns match, you pick the one which you have the most experience with
    - A natural reaction - if gravity works 99 times it becomes plain it will work the 100th time

    - Note: this is the current proof of general relativity
- What worked in the past will hopefully work in the future
- Not always the best solution. Especially for new problems, which happens often in Security

availability heuristic - Kahneman 3

- The availability heuristic is a mental shortcut that relies on immediate examples that come to a given person's mind when evaluating a specific topic, concept, method or decision

Satisficing and bounded rationality

- Satisficing is only doing good enough, rather than doing perfect
- Bounded rationality refers to how we have a limited amount of information, meaning our ability to make decisions is bounded by that information

Tendency to verify generalisations rather than falsify

People prefer positive statements

- we ignore what we don't like, people convince themselves that they are right when the evidence don't exactly line up.

Cognitive strain

Group-think syndrome

- How people think when they're in groups rather than as individuals
- We prefer to keep the peace in a group rather than fight against collective ideas
- The result is groups become homogeneous
- For example: leader makes a joke in a group and everyone laughs even if it isn't funny
- Good for analysing systems

Confirmation bias

- We prefer the evidence that confirms what we believe
- Is an example of cognitive bias and describes that people gather and recall information selectively/interpret in a selective manner
- Richard is very smart and very good at orienteering

Accidents vs Attacks

- Intent is the main difference.
- In an accident, 'holes' don't really line up
- In an attack, the attacker will make those holes line up

Error

- Human error is inevitable - how do we fight it?
- 3-mile island - an example

    - Shaving the buffalo I think
    - A situation where an infinite number of things go wrong causing some undesirable situation
    - To fix the situation requires fixing about 100 different things
    - For example, late to work because of traffic because of a bus strike because you left late because you had to make coffee because a meteor struck your coffee pot because people are doing in-atmosphere asteroid mining because people like shiny things etc
    - In the real world 3-Mile Island situation, multiple parties blamed multiple other parties, mostly the operators
    - In reality, it was *everyone* and *no-one*'s fault - sometimes everything just goes wrong
    - See: Deepwater Horizon. Bad example but similar
- The point of the 3-Mile Island example is that fixing the problem isn't about finding a single point of failure, maybe it's just fixing everything you can, a tiny bit
- We have to design things so that when they go wrong, which they will, the impact is limited - assume you're going to be breached and set it up so that it's not a disaster
- **Simplification:** people will simplify situations to have only one cause, when the truth is probably a lot of causes
-

Error proofing systems:

- Luck doesn't cut it when it comes to building systems.
- Always assume that the person using the system is going to do whatever they can to attack it.
- Always assume that the environment of a system will be the worst case scenario

Common Mode Failure:

- related to redundant systems where one cause can lead to the failure of otherwise redundant elements leading to system failure.
- Elements which should fail independently are under some circumstances dependent.
- E.g: Indicator Failure (Too Many Alarms), Change Over System, Repeated Errors, Common Paths

Just Culture

- Don't just punish the person who made an error, or the last person who touched it
- It's about learning and stopping these situations in the future

Just Code

- Complexity bad
    - No one component should be too complex or too empty
- Coupling bad
    - You can change one component without having to rewrite everything
- Cohesion good
    - Components that are close to one another make use of each other
    - Components that are far away from one another do not make heavy use of one another
- These together create defence in depth
    - A good system can fail at one point or another, but if it doesn't fail at EVERY level, the system itself isn't faulted (yet)

Systems that follows these rules are easier to maintain, and more resilient to attacks

Cassandra Syndrome:

- knowing the truth but no-one believes you
- Occurs when valid warnings or concerns are dismissed.

Chekhov's Gun: anything on-screen in a movie is there for a purpose

- A gun is on a wall because it will be used
- A person coughs because they have Everything Disease
- Useless facts aren't included
- Belief event only has one significant cause
- Plan for fewer contingencies than occur
- Ability to control outcomes - illusion of control
- Hindsight bias
    - Knew it all along phenomenon
    - perceive events that have already occurred as being more predictable than they actually were before the events took place
    - illusion of control
    - plan for fewer contingencies than occur
    - Knowledge of outcome of previous event increases perceived likelihood of that outcome
    - Complexity, coherence, coupling, visibility

Distinguishing between latent errors and active errors

- A latent error is an error that is present but not detected; consequences will occur later
- An active error is an error that is present but detected

- Latent errors undermine defense in depth

Homework:
Learn about
- **Chernobyl**
- **Bhopal**
- **Challenger**

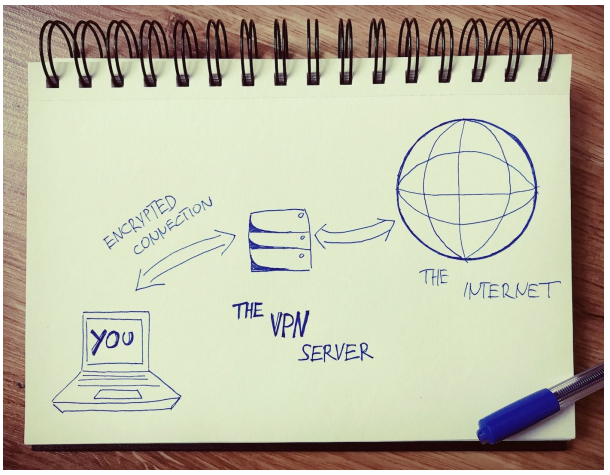
Focus on why things went wrong, where the focus was and wasn't
There will be a generic question about an accident we learned about in the exam

The password to richards lecture is 'password'
kk
Typing on one screen with multiple people is hard *no it isnt* yeah it is I feel like I'm gonna interrupt someone in text :(*get (it's git gud scrub, scrub) gud scrub* that's too hard

Recommended Reading
- Just Culture - Sidney Dekker
- Human Error - James Reason
- Commander in Cheat - no author given
- History Lessons - (book about high school extracts from different parts of the world),

Evening Lecture: Seminars
Seminar 1 - Privacy
- We sacrifice privacy for convenience and fun
- When private data is compromised it is dangerous because attackers can use it against us
- Signal Blocking on Phones
    - Police have been known to access metadata on phones without warrant, so signal blocking your phone may be essential to journalists (who might not want the police seeing their phone data)
    - Wrapping a phone in foil blocks bluetooth signal, but who knows if it blocks anything else
    - Faraday cage bags work on the same principle - dispersing incident electromagnetic radiation, making the phone inaccessible
- Online Privacy Practices
    - Incognito mode
        - Deletes cookies
        - Not very effective
    - Use privacy focused browsers
        - Eg DuckDuckGo, an alternative to Google - doesn't track personal data and requests like Google does
        - This info brought to you by Google
    - Take care of your accounts

        - Log out when you can
        - Don't link accounts or services unnecessarily
        - Lie
    - VPN
        - Virtual Private Network
        - Acts as intermediary between external servers and you
        - Encrypts all traffic between you and the VPN servers
        - Meaning external entities see your VPN, not you
        - Examples include nordvpn, and some other bad ones speaker doesn't advise using



    - Onion routing
        - Encrypt your data and obfuscate its origin by forwarding through multiple nodes
        - Outgoing packet is N-times encrypted, packet visits N nodes on its journey, each node it visits in the network decrypts a layer, like peeling skins off of an onion
        - Desired location then gets the unencrypted packet
        - Weaknesses
            - Logging into accounts like fb identifies you, gets rid of anonymity
            - Timing attacks
                - Cross reference when nodes receive and send packets to identify which sent packets correspond to packets which are received
- "*Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say*" - Edward Snowden
- Why should I be concerned?
    - "I have nothing to hide" just means "I have nothing I can think of that I want to hide"
    - The problem is an imbalance of power between citizens and the government
    - The issue of privacy is not one of a large flood of your data, it's the slow trickle of your information over time
    - "It's not about individual data it's about a pattern of data"

Seminar 2 - Digital Forensics

- See: COMP6445, there's still a few places left
- What is Digital Forensics?
    - Branch of forensics science
    - Recovery/Investigation of material found on digital devices

- Stages of an Investigation
    1. Acquisition/Imaging
        - Capture an “image” (duplicate) of the drive
        - Chain of custody
        - Need to preserve original data, so use write-proofed connector to data storage module to prevent data corruption
    2. Analysis
        - Keyword Searches
        - Look for data
        - Recover Deleted Files
        - Specialist Tools Used
        - Browser history, documents, pictures
    3. Reporting
        - Evidence used to construct events/actions
        - Compile data learned
        - Layman report written
- Types of forensics
    - Computer
        - Memory (Ram)
        - Data
    - Mobile
        - Contacts
        - Messages
    - Network
        - Routing table
        - Switches
        - Packet Capture
    - Database
    - Video/Audio
    - Steganography
- Tooling
    - Encase - used to duplicate files or analyse it
    - Autopsy/The Sleuth Kit - analyse different file systems
    - File and Strings - UNIX commands that give file type and ASCII strings
    - Xxd - Hexdump
    - Foremost - finding headers, footers and internal data structures of malformed files
    - Binwalk - finding embedded files
- Drives and partitioning
    - Allocates memory in clusters
    - The FAT record stores status of each cluster (bad region, allocated, unallocated)
    - When a file is deleted, it is not fully wiped out. The name of the file is changed to 0xE5[file_name].

    - Forensic analysis tools will check for this prefix in the file allocation table, and if it is there, they can extract the contents because nothing else has been removed.
- Actual Homework
    - https://imgur.com/a/X2mNAlZ
    - Flag format is picoctf{}
    - Hint:look between the eyes
- They talk very fast, maybe wait til they publish their slides *excellent idea i concur* ✔️
- When data is deleted, the electrons aren't destroyed, the pointer to that location is just forgotten
    - Meaning we can still access it if we have a very good microscope
    - For more on that try COMP3231, very interesting course
- Homework is look very hard at a dog picture and find a flag
    - Hint w

Capitalist Dog → (͡° ͜ʖ ͡°)

Chain of Custody: protecting forensic evidence from being changed while it's being moved from the crime scene to the place of analysis

Secure Systems: 3-Mile Island

- An island
- 3-miles long
- 0 miles wide making it a 2-dimensional shape
- Nuclear reactor - simple nuclear reaction to heat water to spin a turbine
- Homework: watch 'Chernobyl'
    - If you need to pirate it just use nordVPN
- The red part is the nuclear reactor chamber
    - It's super hot and submerged in water (or molten salt, whatever floats your salt boat)
    - It's meant to be abstracted away from the rest of the system
- The yellow and blue systems interface with the red one, are heated by the hot liquid in the red, and are used in turbines to turn them
- After the failure of the 3-mile island (unit 2), a lot of focus turned to it
    - Runners of the plant blamed the builders
    - Builders blamed the runners (management) I think

- Transfer of heat from primary to secondary to prevent core overheating
    - From red to yellow/blue, but someone deleted the diagram *wasnt me i swear* do you know you're a purple badger
- https://www.antipodesmap.com/
- Attacking people with nuclear weapons is against the course policies
    - Remember: do not be a dick
- A cupful of water leaked out of the cooling non radioactive water system into the pneumatic system
    - The pneumatic system drove the instruments which were used for monitoring
        - Water got into the pumps for the feedwater system and made the instrumentation give crazy readings
        - Feedwater pumps were auto shutdown to prevent damage
        - Turbine was shutdown
        - Core couldnt be cooled because turbine was shutdown
        - Secondary backup pumps were started to cool the core
        - The backup pumps weren't working because the valves to the pipes into the cooling system had been left closed after routine maintenance 2 days before
        - 2 indicators on the control panel showed the status of the valves
            - No one looked because they didn't expect it
            - 1 of the lights was obscured by a repair tag on the switch above
    - SCRAM protocol: do your best then run like heck
        - Drop the graphite rods and SCRAM
    - Relief valve should open to allow gas to exit to prevent explosions
        - It failed to close after it opened
        - The indicator for the valve failed and the operators were misled into believing the valve worked
    - So they flooded the reactor which is bad because it stresses the system
    - Then an automatic high pressure injection system came online
        - The operators turned it off because they were being told everything was ok by the indicators
        - The reactor core was becoming uncovered which is VERY INCREDIBLY BAD
        - **The water in the system started turning to oxygen and hydrogen which is very bad because that's the recipe for a bomb**
    - China Syndrome: when a nuclear reactor is so hot it melts through the crust and "goes to China"
        - Realistically, this happening would irradiate the magma in the earth under the melting site, causing nuclear volcanoes lol *magma is already radioactive naturally, wouldnt make a difference* I have to see sources on that m8 https://www.google.com/search?q=how+radioactive+is+magma&oq=how+radioactive+is+magma&aqs=chrome..69i57.3750j0j1&sourceid=chrome&ie=UTF-8
        - *Theres alot of magma and not much nuclear material*

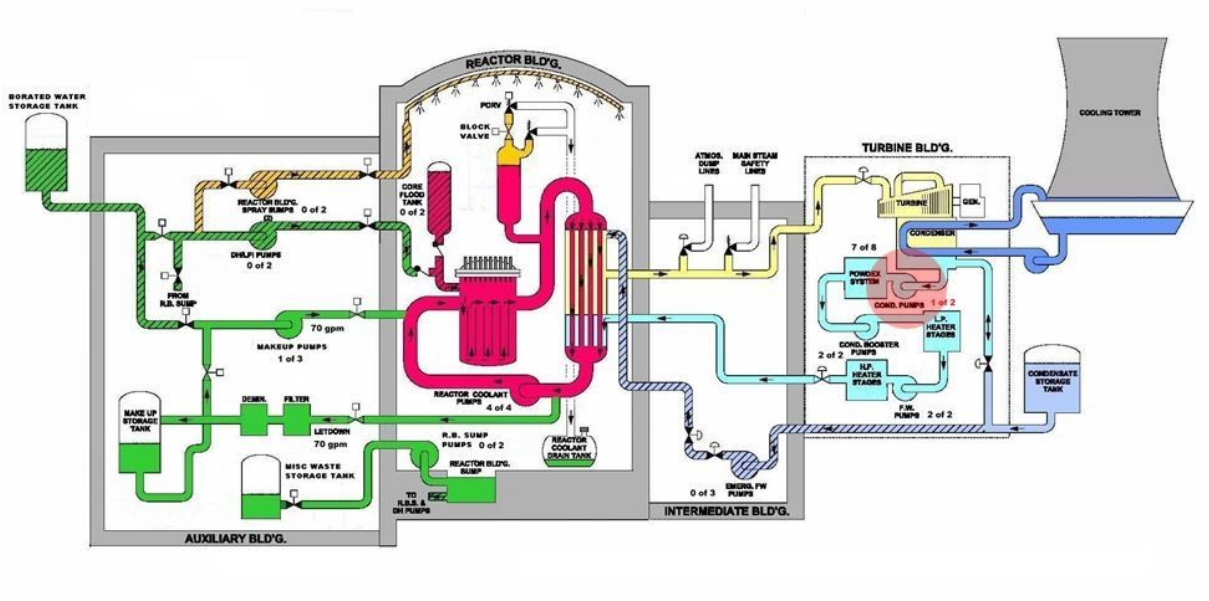
        - “Yes, and so are you, and maybe your kitchen counters as well. Traces of radioactive elements are found in many places. Carbon is a key element of all living things, and a small percentage of all carbon is the radioactive isotope carbon 14. Living things also contain potassium. Some of the potassium in your body is also radioactive. Your kitchen counters might be radioactive because granite contains traces of radioactive uranium and thorium. Lava is about as radioactive as granite rocks.” - Quora answer, https://www.quora.com/Are-magma-and-lava-radioactive
        - TI;DR magma is radioactive, but not as radioactive as bananas
- This bit is very dry, unlike the nuclear power plant, which is wet with radioactive water
- Nuclear reactors, like technological systems, are complex, and if we look at how they’re ‘failproofed’, it can shed light on how to design a secure system
    - Specifically methodology, eg how failures are discovered and buffered against
    - The system is tightly coupled but the problems were not directly related which made it hard for operators to identify the issues
    - Richard starts talking a bit quickly here, but the point is this:
        - In a complicated system you have high coupling
        - Therefore changing something in one place can do random dumb stuff in an entirely unrelated part of the system
        -

SYSTEMS THAT ARE TIGHTLY COUPLED AND OPAQUE AND COMPLEX ARE ALMOST GUARANTEED TO HAVE PROBLEMS

THINGS YOU CAN DO

- Identify the most important things to protect and focus all your energy on those
- Assume you’re going to be breached and work to make sure that that won’t be a crisis
    - Discard all the valuable data, make the system unattractive to attack

As more water flows in, it’s possible for reaction to break water down into hydrogen and oxygen.
hydrogen gas is highly combustible especially when mixed with oxygen => this is why water beats explosions, because it’s made of explosion
Reactor was producing oxygen/hydrogen.
At some point oxygen gas combusted.
Tank began to fill up with hydrogen (one spark can cause a large explosion)


BORATED WATER STORAGE TANK
REACTOR BLD'G.
PORV
BLOCK VALVE
CORE FLOOD TANK 0 of 2
REACTOR BLD'G. SPRAY PUMPS 0 of 2
DHR/LPI PUMPS 0 of 2
FROM R.B. SUMP
70 gpm
MAKEUP PUMPS 1 of 3
MAKE UP STORAGE TANK
DEMIN.
FILTER
LETDOWN 70 gpm
MISC WASTE STORAGE TANK
REACTOR COOLANT PUMPS 4 of 4
R.B. SUMP PUMPS 0 of 2
REACTOR BLD'G. SUMP
REACTOR COOLANT DRAIN TANK
TO R.B.S. & DH PUMPS
AUXILIARY BLD'G.
ATMOS. DUMP LINES
MAIN STEAM SAFETY LINES
0 of 3 EMERG. FW PUMPS
INTERMEDIATE BLD'G.
TURBINE BLD'G.
TURBINE
GEN.
CONDENSER
7 of 8
POWDEX SYSTEM
COND. PUMPS 1 of 2
L.P. HEATER STAGES
COND. BOOSTER PUMPS 2 of 2
H.P. HEATER STAGES
F.W. PUMPS 2 of 2
CONDENSATE STORAGE TANK
COOLING TOWER