Computer Security

Reagan Shirk

August 27, 2020

Recap

- Security is about confidentiality, integrity, availability
  - Confidentiality = secret
    - an employee should not know the salary of his manager (bs imo)
  - Integrity = unaltered
    - an employee should not be able to modify their own salary
  - Availability = easy to get
    - the employee should get their paychecks regularly and on time
- These are the three fundamental parts of security

Achieving Security

- What, how, and how well?
- Infosec is the meeting point of comupsec and comsec
  - Comupsec is where computers and security meet, comsec is where communications and security meet
  - Basically infosec (information security) is just where computer security and communication security meet

Security Mechanisms (the what)

- There are three types: prevention, detection, and tolerance
  - Prevention:
    - When you want to secure your system, what is the first thing you want to do? Limit unauthorized access, make sure only the people you want to have access are the ones with access. That is prevention. Is prevention enough? Nahh
  - Detection:
    - When prevention doesn't work, what do we want? Detection, gotta be able to tell when someone slides their way in. What do we do when we find the fucker you don't want all up in your business?
  - Tolerance:
    - Gotta be able to recover, that is tolerance. Can't just get a new computer every time some asshole decides to fuck around a little so you gotta kick him out or be able to tolerate him. At least I think that's the point he's getting at?
- Good **authentication** is the foundation for good prevention and good detection
- Which is more important out of prevention, detection, and tolerance?
  - No one fucking knows but James made a good argument for tolerance

Security Services (the how)

- Back to confidentiality, authentication, and integrity

- Also non-repudiation, access control, and monitor/response
  - non-repudiation: how to determine who is responsible for what...?
    - making sure which you know people send or receive information
  - access control: determining and enforcing who can do/access what
  - monitor/response: monitoring attacks, generating indications, and tolerating/recovering from attacks

Security Assurance (the how well)

- This is how well your security mechanisms guarantee your security policy
- high assurance = very secure, but also means high cost. Might not be able to afford it
- You gotta have some sort of tradeoff, you don't need aaaalllll of the security, you just need enough for you to be secure

Security by Obscurity

- If we keep secrets our shit is more secure
  - Okay, that was terrible. Don't tell people how your shit works if you want to keep it safe. Like Sridhar once said, "if you want job security, write code no one else can read"
- This doesn't really work though because more applications open their standards and people are getting better with computers
- In theory you could make some weird shit and not tell anyone how you did it and it'll be secure, but in reality someone will figure it out
- Apparently there's an existential crisis happening now

Threat-Vulnerability

- Threats are possible attacks
- Vulnerabilities are weaknesses that may make them more likely to be exploited by an attack
- We need to assess threats and vulnerabilities

Cryptography: The Foundation of Computer Security

- What is cryptography? A secret writing
- Cryptography transforms data into some sort of random looking string
  - The catch: it's gotta be reversible bruh. You gotta be able to get the original string back
- When cryptography is combined with compression, which one do you do first?
  - Before we ask this, we gotta ask how we compress. I missed the answer. It's cold and I'm tired

Cryptography vs Steganography

- Wtf is steganography? Hopefully someone knows
- Steganography: concealing the existence of communication, like invisible ink or hiding words inside of other words