COMP6441 Lecture 2

Youhan Cheery

March 20, 2017

1 Reconnaissance

- Passive recon is not really doing anything. e.g. listening to someone talk
- Actively trying to listen, using something to influence/capture the data. e.g. placing a bug on a person. More effective, but also more detectable.

Do a passive recon of something? Dumpster dive and stuff

2 The problem of security

1. Complexity: as soon as any system becomes so complex that we don't fully understand it, it opens a door for hackers. This is not limited to only computer systems, but anything really. Simplicity is what we need for security and assurance.
2. Assymetry of attack and defence
3. Weakest link: only need to break 1 link to break the system
4. Hubris
5. Abuse of trust
6. Human weakness: this is typically the weakest link in the chain.
7. Having areas with less complexity is better. Outside and inside. Outside is bad and inside is good. Have a layer in between that protects the inside from security = the "M and Ms" concept.The problem with this theorem is that it's very difficult to find a layer to protect the safe space. Where is the boundary? Can you always trust the inside? It's a single point of failure and creates an unhealthy expectation of security.
8. Relying on secrets is very dangerous. A crypto system should be secure even if every thing about the system is known. It's better to rely on a small secret, if it's absolutely necessary.

You will never be able to assess how good your own system is objectively - need an external opinion.

Richard - ”the main point of security is asking the right questions... Sometimes quite hard to articulate what you want to achieve... You will be tempted to solve a problem that isn’t the problem”

Need a process. A process is testable, scalable and can be reapplied to other systems.

3 Type 1 and 2 errors

- There’s the truth, and there’s what the experiment says. You can reduce one the errors, but the price of reducing it you must increase the power of the test. If we focus on only one of those errors, we may become blind to other errors.
- It’s important to know what kind of error it is: is it type 1: reject the correct case, or type 2: accept the right case.

4 Cryptography

- CONFIDENTIALLY: How do we keep it secret from any listeners?
    1. Keep the whole thing a secret, including the existence of the message = ”steganography”. Not so good because the secret is too big. Also we want to have it so that the secret can be changed.
- INTEGRITY: How do we know it hasn’t been intercepted?
- AUTHENTICATION: How do we know it came from the intended source?
- Shannon - entropy.
- Two ways people typically follow to create new code?
- Bits of work? How many bits is 26 factorial?