COMP6441: Lecture 4

Youhan Cheery

March 2017

1 Human Weakness

- Humans are going to be the weakest part of a system. To be a good security engineer, you need to understand humans.
- Human weaknesses:
  - Fear, e.g. South Korean Ferry Disaster
  - Greed, e.g. working in a bank/position of power (police officer)
  - Laziness
  - Ego can stop reflection
  - Vice
  - Trust, sometimes people are too trusting. Social engineering will largely involve an abuse of trust
- "Security theatre" is the appearance of a secure system, which, is actually insecure.
- Training is an integral component in computer security. People should have some level of knowledge and calm when the worst-case scenario happens, so that they can behave appropriately. An example of this is Rick Rescorla, who trained the employees of JP Morgan to escape, thus saving the lives of thousands of people during the September 11 attack.
- Homework: find examples of human weaknesses. Watch magicians and study their tricks.

2 Physical Security

- Precursor to computer security. No point having the worlds safest software protocol only for a person to have access to the hard drive it's stored on.
- If a person has physical access, it's fair to assume it's over.

- In many ways, this is the hardest to secure. It's the first or last thing a person sees, and it has an element of "security theatre".
- Physical security can be used as a form of misdirection.
- Tamper proof vs tamper evident? Do you need to make something untouchable, or something that a user knows has been tampered with.
- Access to ports

3 Hashing

- Hashing is a strategy that allows us to look after the integrity and authenticity of a system
- "Nonce" used to prevent replay attacks. It's a number that changes all the time
- Hash means convert something of indeterminant size/type etc to a number in a much smaller range
- Cryptographic hash is a hash with cyrptographic properties. Take message, run the hash function on it and get a small block (signature). Send the block along with the message that has been encrypted.
- Does not rely on security through obscurity.
- They behave really good at connecting different blocks in a crypto system.
- "Pre-image attack" given hash and you find the message. This won't work on a cryptographic hash. Thus they behave similarly to diodes.
- "Dictionary attack" is a brute-force method of breaking a hash. Run a bunch of words through the hash to get the same hash output.
- "Birthday attack" based on birthday paradox. States that of a certain number of a people in a room, at least 2 people will share a birthday. The rate that the number of pairs grow as the group grows is quadratic. This is an example of a "collision attack". This is when two different objects hash to the same value. Chance of finding a collision increases quadratically. More efficient than pre-image attack.
- "Second pre-image attack" is if one person has a message, and tells this message to another person. This person computes the hash of the message and computes another message that corresponds to the same hash.
- There are a lot of hash functions, but not as many cryptographic hash functions.

- Hash the message with a shared secret - message authentication code. Achieves the A and I in CIA.
- Most cryptographic functions iteratively hash the message in different sections.
- "Length extension attack" is where middlemen will add to the end of the message and this will contain part of the message. This will break a message that has the password at the front, which is hashed.
- HMAC