7. Top Men, RSA and Misdirection

COMP6441 • KC Notes

7.1 Top Men

- Security should never rely on "Top Men"
    - Brody: The Ark is a source of unspeakable power and it has to be researched!
      Maj. Eaton: And it will be, I assure you, Doctor Brody, Doctor Jones. We have top men working on it right now.
      Jones: Who?!
      Maj. Eaton: Top... men.
    - Everything needs **openness, scrutiny and oversight** in security
    - When people say 'trust us', you should never trust them.
- As a Chief Security Officer, reporting to CEO is better than reporting to Chief Information Officer, as they are the ones making the computer/IT system
    - Because CIO **sets up the system**, they **will always say it's fine** (or sack you)
    - CEO is a better path to get to the board of directors – to get a decision/action
    - **Mandatory data breach notification**: compulsory notification that stock exchange will know about, and acts as a shortcut to the board of directors

7.2 Attacks and Security

- **Side channel attack**: attacks that are based on metadata of a system that is leaked from its use
    - An attacker can film a chip packet in a room with music playing in it, and transform it back into music
    - Attacker can listen to the CPU –1's and 0's may produce different sounds
    - Smartphone patterns easily visible when tilting the screen
    - Side channel attacks are **won't be tested or proved** because it is hard to know about it.
- Attacks that **affect something later**
    - Terrorism before an event can change an election result
    - **Insider trading** before a **merger** allows an individual to purchase stocks in advance
    - Trading by saying a price will go down because of some threat
- Jewel heist: how can you improve its security?
    - Assets: people, jewellery
    - Threats, sorts of attacks: smash and grab, coercion
    - Mitigation: remove their ability to see – smoke, organic spray

7.3 RSA

- **RSA** relies on mathematical functions that are **hard to undo** and applied to crypto

1. Select a function, e.g. x^3
2. Select a set of characters we want to encrypt, e.g. [0…49]
3. Modulo the total number of characters in the set

- We require it to not have **clashes/collisions** (otherwise, it cannot be reversed with certainty)
  - E.g. A → 3, B → 3, but going backwards, 3 → A OR B
  - We can prevent clashes by **modding it with prime numbers**
- We can easily reverse RSA with a private key by **modding it with the product of two prime numbers (π)**, as long as both have nothing to do their primes less 1 ($\pi - 1$)

Encryption Function: x^k mod p

1. Let prime p be $7 \times 11 = 77$
2. Let the encryption key k be 7

You can share k = 7 and p = 77

x^7 mod 77

Decryption Function: y^n mod p

1. Calculate m = $(7-1)(11-1) = 60$ from the prime numbers, **keep secret**!
2. Let n be the decrypt key where $n \times k \bmod m = 1$ – here n = 43

Private: y^{43} mod 77

Example:
k = 3
$p_1 = 5$
$p_2 = 11$
Encrypt with $x^3 \bmod 55$ – say $x = 6$
$6^3 \bmod 55 = \mathbf{51}$

Alice tells us secretly $m = 4 \times 10 = 40$
k = 3
n is 27 ($27 \times 3 \bmod 40 = 1$)
Decrypt with $y^{27} \bmod 55$ – y is 51
$51^{27} \bmod 55 = \mathbf{6}$

- Relies on the fact it is **easy to multiply two large primes**, but **hard to find a prime's factors**

7.4 Misdirection and Magic

- Magicians commonly use misdirection to perform magic, and **is similar to social engineering**
  - Make sure viewers **never concentrate on the important thing**
  - Exploit human weakness, greed