10. WannaCry, Time and Knowledge

COMP6441 • KC Notes

10.1 WannaCry

- WannaCry was a recent malware affecting the world in a big way.
- **Incident response:**
  - **What have we learnt from this?**
  - **If you were IT, what would you have done?**
- Our suggestions:
  - **Disconnect, back up** your data, check if systems need to be live
  - **Assess your own system** – are the systems vulnerable?
    - At this time, **no one knows how to protect** and no one knows **what they are up against**
    - There are just theories, so you may just overreact to be safe
  - Tell staff members to not open attachments
    - Contact senior members
    - Internal response – if one system is compromised, the whole enterprise may be compromised
  - Have a **contingency system**, e.g. a paper based system next to the original system for ambulance services
    - It is a prudent act to have a backup or parallel system, in case one fails

10.1.1 RESPONSES IN GENERAL

- There was a planned choice to release the attack on **Friday**, when people are least alert
  - Attackers usually pick a time when people are **stressed, moving, closing**
  - It is when **defenders are least prepared and least ready**
- There is no need to panic – think and plan.
  - Weigh choices up, consider the cost of taking systems down
  - The Centre for Disease Control and Prevention (CDC) has many **contingency plans for disease outbreaks** – learn from cases outside cybersecurity
  - Ethics: make a decision that you won't be disappointed in later. Plan ahead and in advance

10.2 Effect of Time on Knowledge

- TOCTOU and Forward Secrecy (see 8.4, 9.4)
    - It is hard to prove something **has happened <u>before a particular time</u>**
    - It is hard to make a **tamper evident seal** on knowledge
    - It is also difficult to prove that **you have not leaked any information**
- **Proof of knowledge**: What protocols let us prove someone knows something, without sharing that knowledge?
    1. Post an encrypted file, and **later send the key**
        - Could possibly be decrypted by many keys to certain answers
        - Hash could reduce this possibility, though could be specially crafted
    2. Tell it to a **trusted third party or mutual friend**
        - Place it in a vault
    3. **Isolate** the information or the person who has the knowledge
    4. **Indestructible box with two keys**
        - Both parties must *simultaneously* open the box
    5. Demonstrate the power to know something on other similar objects
- **<u>Zero Knowledge Protocol</u>**: How I can convince you **that I possess some knowledge**, **without conveying that specific information**. In other words, to convey that I do indeed possess the knowledge, without sharing that knowledge.
    - **Prove that you can break into any house in the city**
        - Pick a city
        - The prover will build a replica house in the city
        - The verifier picks **where this real house is**, or **how to break into this replica house**
    - **Prove that an exam is easy**
        - The prover will write 30 questions into a hat, and
        - The verifier picks **20 questions from the hat**, and the remaining 10 will be in the exam
- Both examples have **two choices**, which **<u>combined</u> will leak the knowledge**, but when **<u>separated and repeated</u> will reduce the chance the prover is trying to trick us**.
    - This reduces the chance by ½ every time.