1. Introduction to Security Engineering

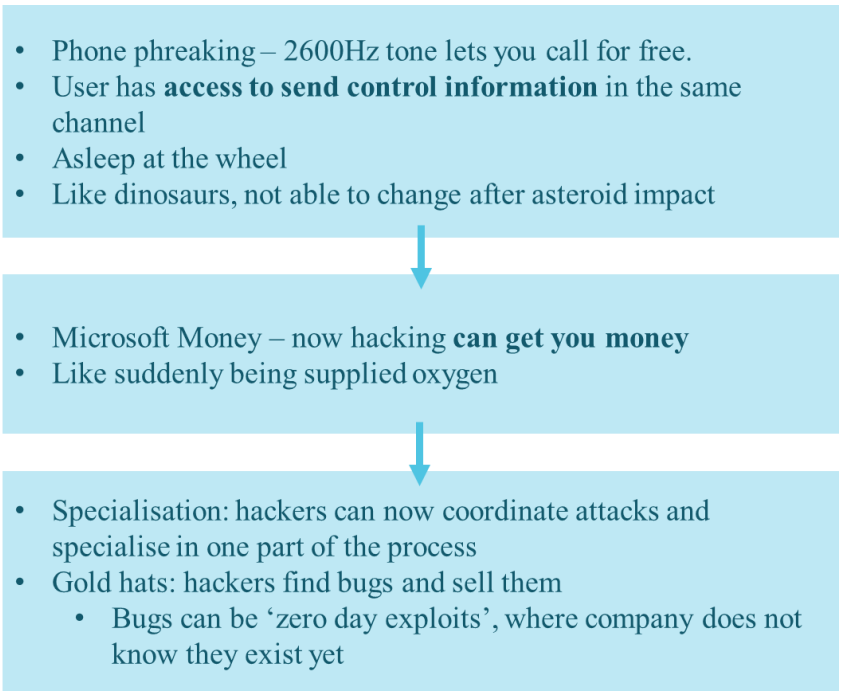
COMP6441 • KC Notes

1.1 Introduction to Security Engineering

- In civil engineering, bridges rarely fall down, people trust bridges.
  - Apply engineering skills and theories into computer security
- Consider differences between civil and security in terms of:
  - Attackers
  - Complexity and abstraction
  - Errors and controlling errors
  - Proving a bridge or program will work – or prove mathematically that it has problems?
- Think like an attacker
  - As a defender, you see only **the strengths** of a house, as an attacker you see **weaknesses**
  - **Question everything**, everything is vulnerable
  - Attackers can pick at one thing, defenders must defend all things.

1.2 History of Hacking

- History is very similar to the history of life.



1.3 Targets

- **Complexity**: a complex system is difficult to secure
- **Out of specification**: when building software, you usually test for situations within the spec
    - Person looking for exploits look **out of the spec** and use systems in unintended ways
    - **WEP Insecurity**: initialisation vectors within packets
        - Again, control data was accessible (in this case, the destination address), and is accessible in inbound data

1.4 Case Study: Halifax Explosion

- Case studies are thinking problems – think analytically about how a problem can be fixed.
- Rather than **who to blame**, focus on **how to fix the problem**
    - Treat the problem as **a systemic failure** rather than an **isolated failure**