REVIEW NOTES
October 2017

Security Engineering Concepts

- CIA triad
- Owners
- Countermeasures
- Assets
- Rsks
- Threats
- Attacks
- Threat agents

Malware and anti malware

- Virus, worms, trojans, bots, spyware, keyloggers
- Virus lifecycle and propogation techniques
- Methods used by viruses to evade detection
- Anti-virus techniques

Network attacks and defences

- Arp spoofing
- Tcp sequence number attacks
- Denial-of-service: flood, reflection and amplification
- Denial-of-service: detection and filtering
- Concept of IDS and IPS
- Types of firewalls: packet, stateful, application-level, host-based, personal
- Firewall topologies

Software vulnerabilities and countermeasures

- Overflows (buffer, heap)
- Defences (compile time, runtime)
- Quality and reliability (unit testing versus security testing)
- Defensive programming
- Input validation and input fuzzing

Security usability and psychology

- Common attacks such as phishing or pre-texting
- Social psychology and its relationship to social engineering attacks