1. MULTICS ring mechanism
   a. Rings, gates, ring-crossing faults
   b. Used for both data and procedures; rights are REWA
      \((b_1, b_2)\) access bracket—can access freely; \((b_3, b_4)\) call bracket—can call segment through gate; so if \(a\)’s access bracket is \((32, 35)\) and its call bracket is \((36, 39)\), then assuming permission mode (REWA) allows access, a procedure in:
         rings 0–31: can access \(a\), but ring-crossing fault occurs
         rings 32–35: can access \(a\), no ring-crossing fault
         rings 36–39: can access \(a\), provided a valid gate is used as an entry point
         rings 40–63: cannot access \(a\)
   c. If the procedure is accessing a data segment \(d\), no call bracket allowed; given the above, assuming permission mode (REWA) allows access, a procedure in:
      rings 0–32: can access \(d\)
      rings 33–35: can access \(d\), but cannot write to it (\(W\) or \(A\))
      rings 36–63: cannot access \(d\)

2. Malware, malicious logic

3. Trojan horse
   a. Rootkits
   b. Replicating Trojan horse
   c. Thompson’s compiler-based replicating Trojan horse

4. Computer virus
   a. Boot sector infector
   b. Executable infector
   c. Multipartite
   d. TSR (terminate and stay resident)
   e. Stealth
   f. Encrypted
   g. Polymorphic
   h. Metamorphic
   i. Macro

5. Computer worm

6. Bots, botnets

7. Bacterium, rabbit

8. Logic bomb

9. Adware, spyware

10. Ransomware

11. Phishing