Network Security – Class Test Update

Dr. Sandra Scott-Hayward

CSC3064 Week 4 Assessment Update

School of Electronics, Electrical Engineering and Computer Science

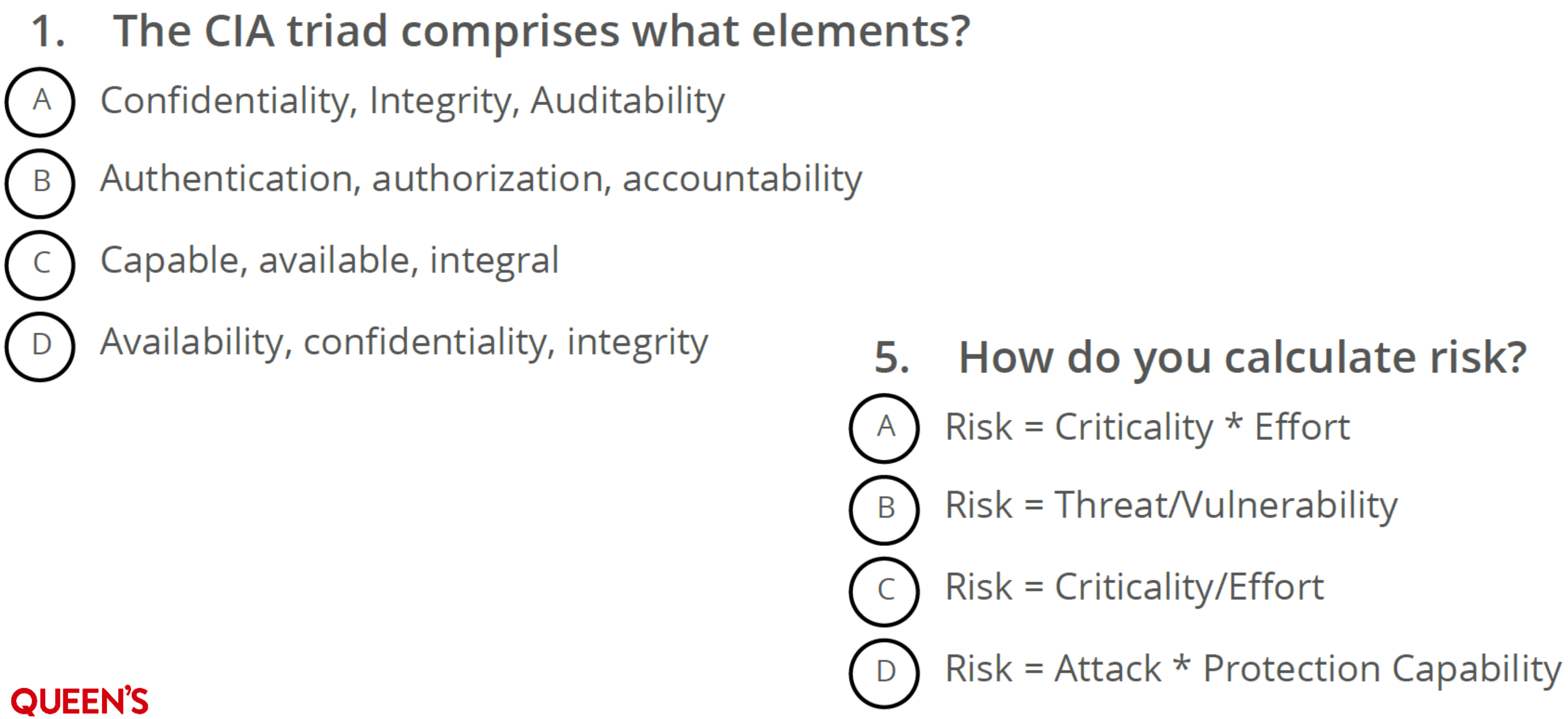
CSC3064 – Class Test Update

Class Test – 15 February 2019 – 1pm

- 1 hour
- 20 Questions
- QuestionMark e.g. Multiple Choice, Matching, Short Essay Response
- Topics:
  - Introduction to Network Security
  - Network security architecture
  - Security issues in internet protocols
  - NAT/Tunneling/VPN (Week 4 material only)

Example Questions/Question Style

Remember the Pop Quizzes:



1. The CIA triad comprises what elements?

○ A Confidentiality, Integrity, Auditability

○ B Authentication, authorization, accountability

○ C Capable, available, integral

○ D Availability, confidentiality, integrity

5. How do you calculate risk?

○ A Risk = Criticality * Effort

○ B Risk = Threat/Vulnerability

○ C Risk = Criticality/Effort

○ D Risk = Attack * Protection Capability

QUEEN'S UNIVERSITY BELFAST

Example Questions/Question Style

Match the security goals to the description (Lecture02 – Slide 9)

E.g. Two drop-down lists and you have to match up the security goal with the definition/description provided.

Give an example of a header-based attack. (Lecture03 – Slides 24/25)

E.g. The Ping of Death is a header-based attack. A malicious user sends a malformed ping packet with the fragment offset value set to the maximum and more data than the maximum packet length. When the receiver reassembles the IP fragments, it has a packet larger than the max. IP packet size (i.e. > 65,535 bytes), which leads to a buffer overflow.

Example Questions/Question Style

What are the two main security issues with ARP? (Lecture06 – Slide 23)

E.g.

(1) ARP is a stateless protocol, which means that ARP requests and replies are treated independently. As a result, information from gratuitous ARP replies are accepted.

(2) There is no mechanism to authenticate the sender of an ARP request/reply message or to check the integrity or validity of provided information so it is possible to poison a host's ARP cache with a false IP-MAC address mapping.

Identify the drawbacks of DNSSEC. (Lecture08 – Slide 43)

E.g.

(1) DNSSEC introduces added complexity with the requirement to sign and check DNS records and to manage key distribution. This makes it easier to perform DoS attacks on DNS servers.

(2) The requirement for zones to be completely signed introduces an overhead that can be a performance challenge for large companies or registries.

(3) The distribution of anchor keys is still a manual task, which allows for human error and threats from social engineering.