
ESTD1845
QUEEN'S
UNIVERSITY
BELFAST

Revision Session

Dr. Sandra Scott-Hayward

CSC3064 Revision Session

School of Electronics, Electrical Engineering and Computer Science

CSC3064 Schedule

Week 1 (14): Introduction to Network Security	Week 2 (15): Network Security Architecture	Week 3 (16): Security of Internet Protocols	Week 4 (17): Security of Internet Protocols
Week 5 (18): Tunneling and VPNs	Week 6 (19): AAA and Firewalls	Week 7 (20): Intrusion Detection/ Protection Systems	Week 8 (21): Network Security Administration
Week 9 (22): Incident Mgmt./ Network Forensics	Week 10 (23) Denial of Service	Week 11 (24): Cloud/Virtualization Wireless/Mobile	Week 12 (25): Review/Q&A

QUEEN'S UNIVERSITY BELFAST

Content for final class test

- Tunneling and VPNs
- AAA and Firewalls
- IDPS
- DoS
- Cloud/Virtualization
- Wireless/Mobile

QUEEN'S UNIVERSITY BELFAST

Tunneling and VPNs - Summary

- IP Filtering
- Network Address Translation – Static, Dynamic
- Virtual Private Networks
  - Types e.g. Network-to-network etc.
  - Point-to Point Tunneling Protocol
  - PPTP vs. L2TP

- IPSec
  - Security Objectives
  - Security Association, Security Policy Definition, SA Database
  - Transport/Tunnel Mode
  - Authentication Header/Encapsulating Security Payload
  - Issues with IPSec

QUEEN'S UNIVERSITY BELFAST

How to study/revise Tunneling and VPNs

- Can you explain how to filter packets?

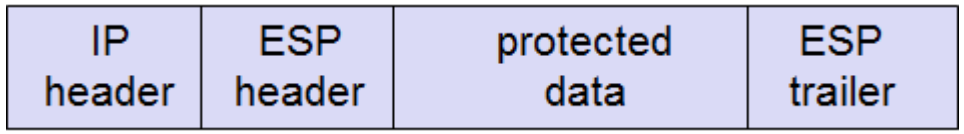
- Can you explain how Network Address Translation (NAT) works?
- Could you draw a picture of a network with the location of NAT on it?
- Can you identify a private IP address?

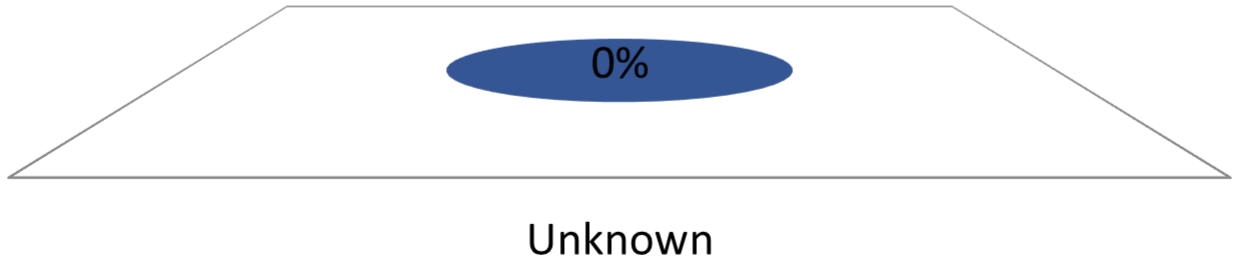
- Can you describe what a virtual private network is for?
- Could you list the VPN protocols that we discussed?
- Do you understand what part of the communication path is protected with the VPN?
  - i.e. depending on where the tunneling protocol is applied

- Can you explain the security objectives of IPSec?
- Can you explain the difference between IPSec transport mode and tunnel mode?
- Can you explain the difference between Authentication Header and Encapsulating Security Payload?
- Could you identify the protocol and mode to apply for a specific communication e.g. POP3 example?
- Could you describe IPSec replay protection?
- Can you identify the issues with IPSec?

QUEEN'S UNIVERSITY BELFAST

Which IPSec packet type is shown in the figure and what security protection does it provide?





AAA and Firewalls - Summary

- Network Access Control
- Authentication, Authorization, Accounting
    - RADIUS - Networking protocol providing centralized AAA services
    - Kerberos – Network Authentication Protocol
- Network Access Enforcement
    - IEEE 802.1X port-based Network Access Control
    - IEEE 802.1Q virtual local area networks (VLANs)
- Firewalls
    - What they can and can’t do
    - Default permit/default deny strategies
    - Types: Packet Filtering, Stateful Inspection, Application Proxy, Next Generation Firewalls
    - Deployment: Bastion Host/DMZ
    - Example Ruleset

QUEEN'S UNIVERSITY BELFAST

How to study/revise AAA and Firewalls

- Can you explain network access control?
- Can you define AAA i.e. what does each A mean?
- Can you briefly explain the steps in a AAA service such as RADIUS or Kerberos?

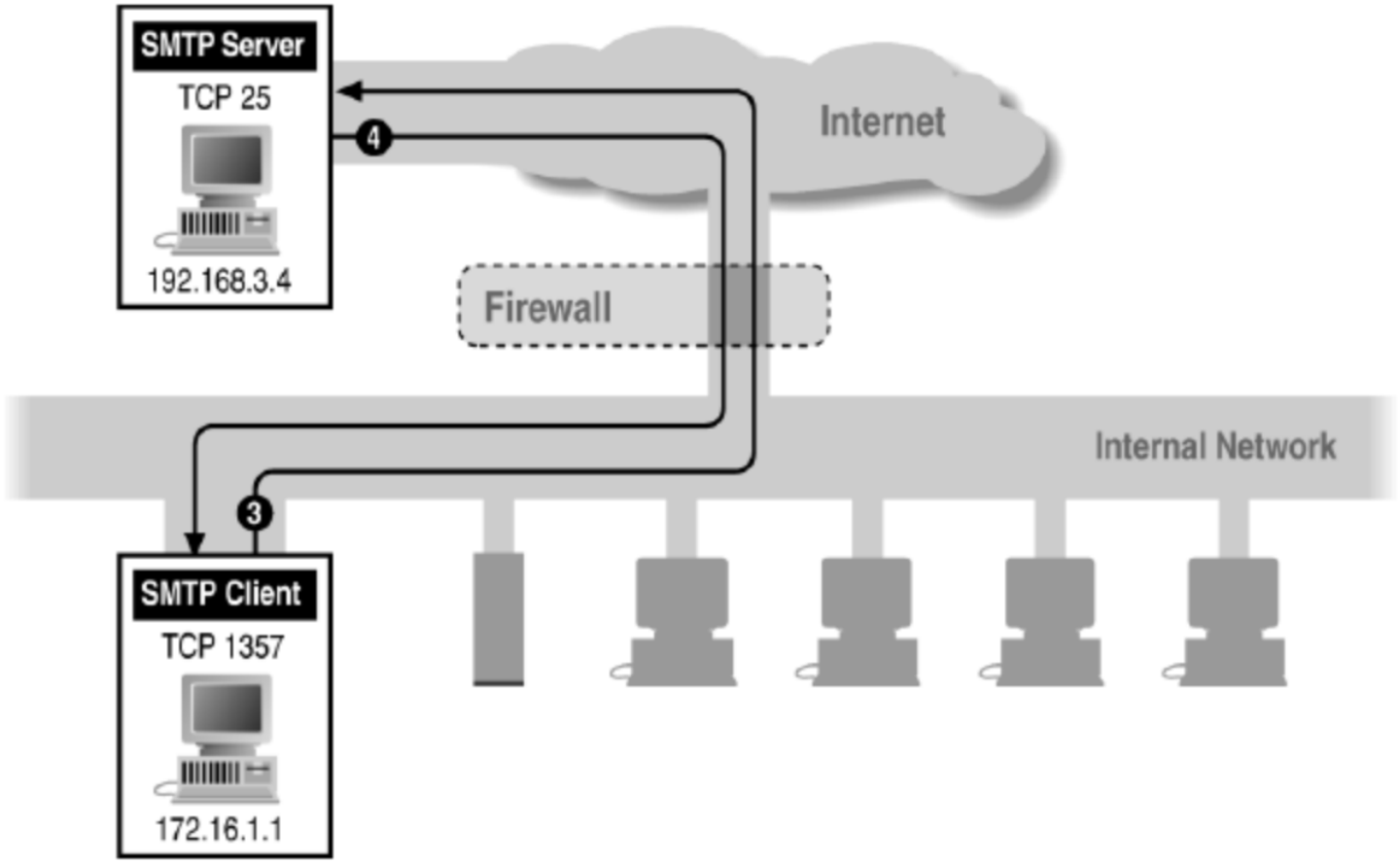
- Can you explain how port-based network access control (IEEE 802.1X) works?
- Can you describe what a virtual local area network (IEEE 802.1Q) is for?

- Can you explain what firewalls can and cannot do?
- Do you understand the differences between the various firewall types e.g. which firewall would you use for different types of protection?
- Can you explain the De-militarized zone (DMZ)?
- Given a firewall rule, could you explain what traffic is allowed/denied at the firewall?

QUEEN'S UNIVERSITY BELFAST

Example Question

Write the firewall rule to enable outbound SMTP traffic as shown in the figure. Fill in the blanks to create the firewall rule. Src Address: [ ], Dst Address: [ ], Protocol: TCP, Src. Port: [ ], Dst. Port [ ], Action: [ ]. Fill in the blanks to identify what additional fields should be set to improve the filter protection. The [ ] of the traffic should be added and the [ ] should be checked. [3 marks]



IDPS - Summary

- Intrusion Detection Systems
  - Host-based (HIDS), Network-based (NIDS)
  - Signature-based detection
  - Anomaly-based detection
- IDS Evasion
- Problems of IDS
- Intrusion Prevention System Approaches
- Unified Threat Management

QUEEN'S UNIVERSITY BELFAST

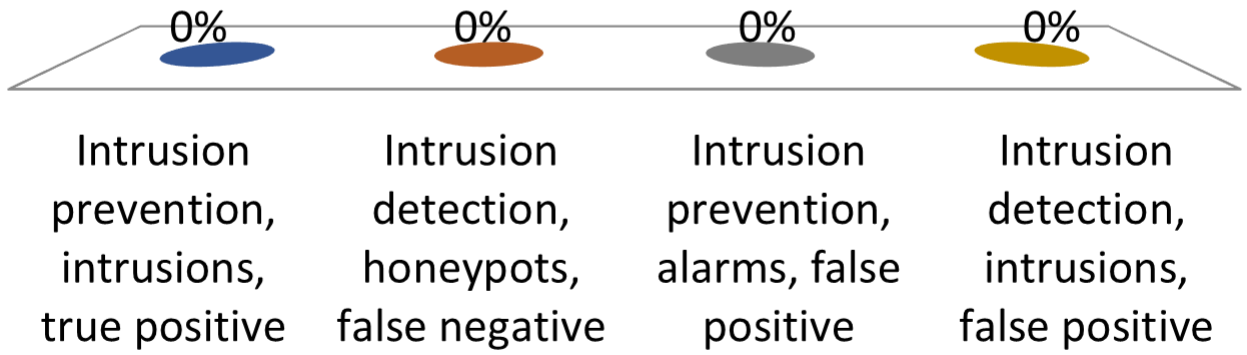
How to study/revise IDPS

- Can you define a network intrusion?
- Can you identify examples of intrusions?
- Can you explain the goals/objectives of network intrusion detection systems?
- Can you explain detection quality i.e. accuracy, sensitivity, precision and FP/FN/TP/TN?
- Can you compare host-based IDS with network-based IDS?
- Can you explain the difference between signature-based detection and anomaly-based detection?

- Can you identify and describe some of the problems with IDS?
- Can you explain the pros/cons of intrusion prevention systems e.g. race conditions?
- Can you describe a honeypot?
- Can you describe unified threat management?

To be of practical use, an _____ _____ system should detect a substantial percentage of _____ while keeping the _____ _____ rate at an acceptable level.

A. Intrusion prevention, intrusions, true positive
B. Intrusion detection, honeypots, false negative
C. Intrusion prevention, alarms, false positive
✓ D. Intrusion detection, intrusions, false positive



(D)DoS - Summary

- What is a (D)DoS?
- Attack techniques: Resource destruction, reservation, depletion
- Attack types: Amplification attacks, SYN Flooding attacks – low rate, massive, DNS DoS, DoS via route hijacking, DoS at higher layers
- Attack network topologies

- DDoS Countermeasures/Defences
  - Client Puzzles
  - Ingress Filtering
  - Traceback/Edge Sampling
  - Rate-Limiting
- Recent DDoS attack methods

QUEEN'S UNIVERSITY BELFAST

How to study/revise (D)DoS

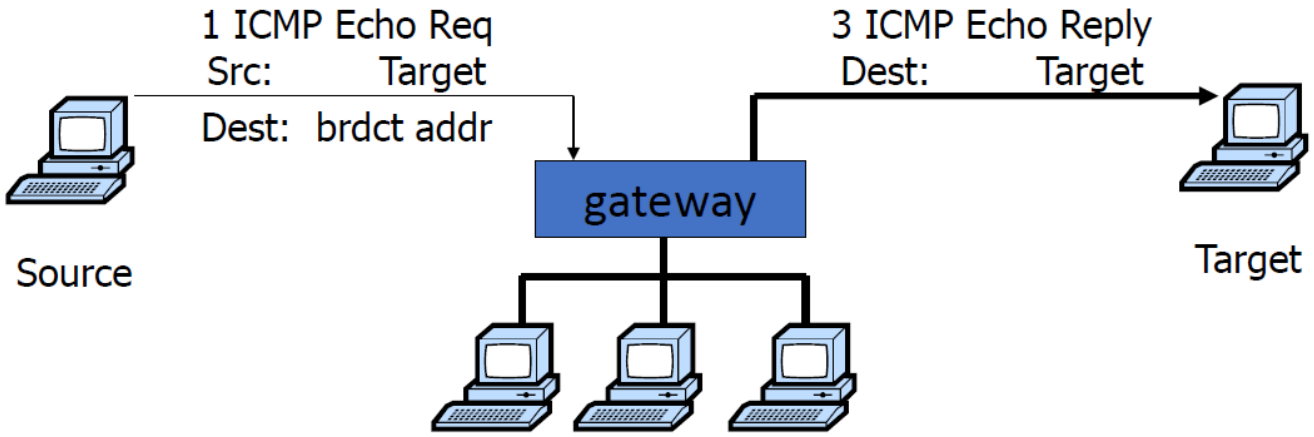
- Can you describe a denial-of-service attack?
- Can you explain the DoS attack techniques e.g. resource destruction, reservation and depletion?
- Can you describe some (D)DoS attacks e.g. amplification, reflection etc.?
- Can you describe the operation of a botnet?

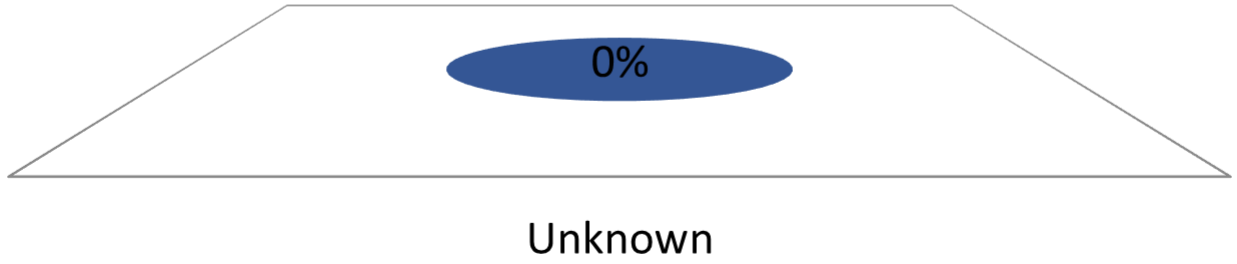
- Can you identify the stages of DDoS defense i.e. before, during and after attack?
- Can you describe some defenses against DoS attack techniques e.g. resource destruction etc.?
- Can you explain the pros/cons of where you place the DDoS defense?

- Can you explain how a client puzzle works?
- Can you explain how ingress filtering works?
- Can you explain how traceback/edge sampling works?
- Can you explain how rate limiting works?

QUEEN'S UNIVERSITY BELFAST

What specific network attack is shown in the figure?





Cloud/Virtualization Security - Summary

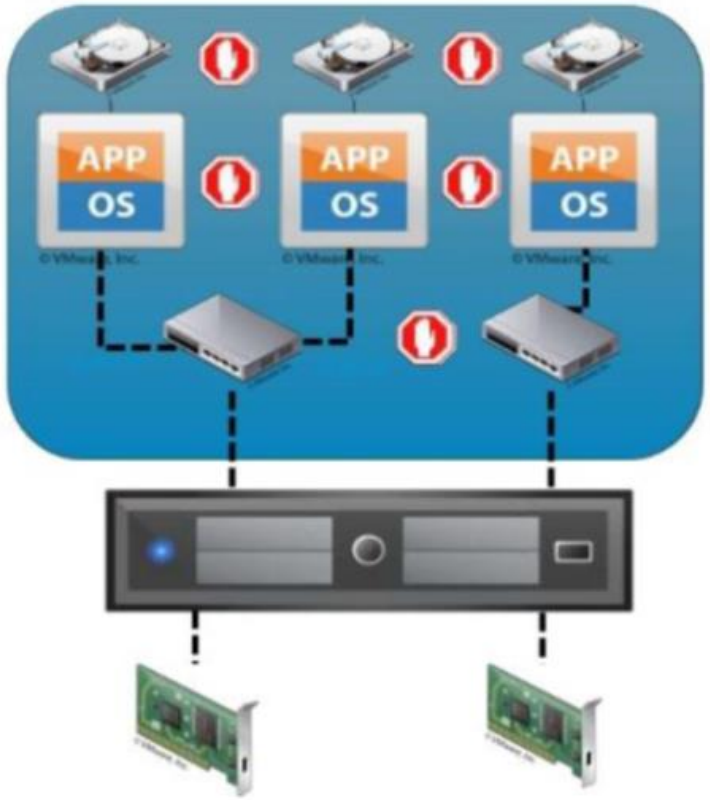
- Cloud Computing – Definition, Elements, Roles
- Cloud security threats and countermeasures
- Cloud Security Alliance – Security Guidance
    - Virtualization and Containers
    - Incident Response
    - Security as a Service

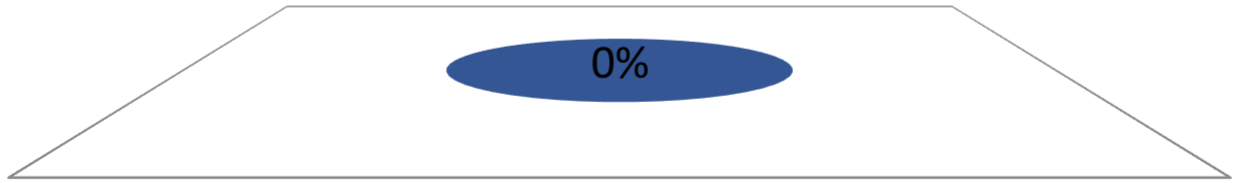
QUEEN'S UNIVERSITY BELFAST

How to study/revise cloud/virtualization security

- Can you identify the five essential characteristics, three service models, and four deployment models of cloud computing?
- Can you identify the cloud actors and their roles?
- Do you understand the security responsibility with respect to the three cloud computing service models?
- Can you identify the cloud security threats and their relevant countermeasures?
- Can you describe the security challenges in virtualization and the security recommendations?
- Can you explain the security recommendations if adopting cloud security as a service?

What virtual network security recommendation is illustrated in the figure?





1

Wireless/Mobile Security - Summary

- Security aspects of mobile communication
- Security aspects of wireless communication
- IEEE 802.11 security claims/issues
- IEEE 802.11i (Robust Security Network)

How to study/revise wireless/mobile security

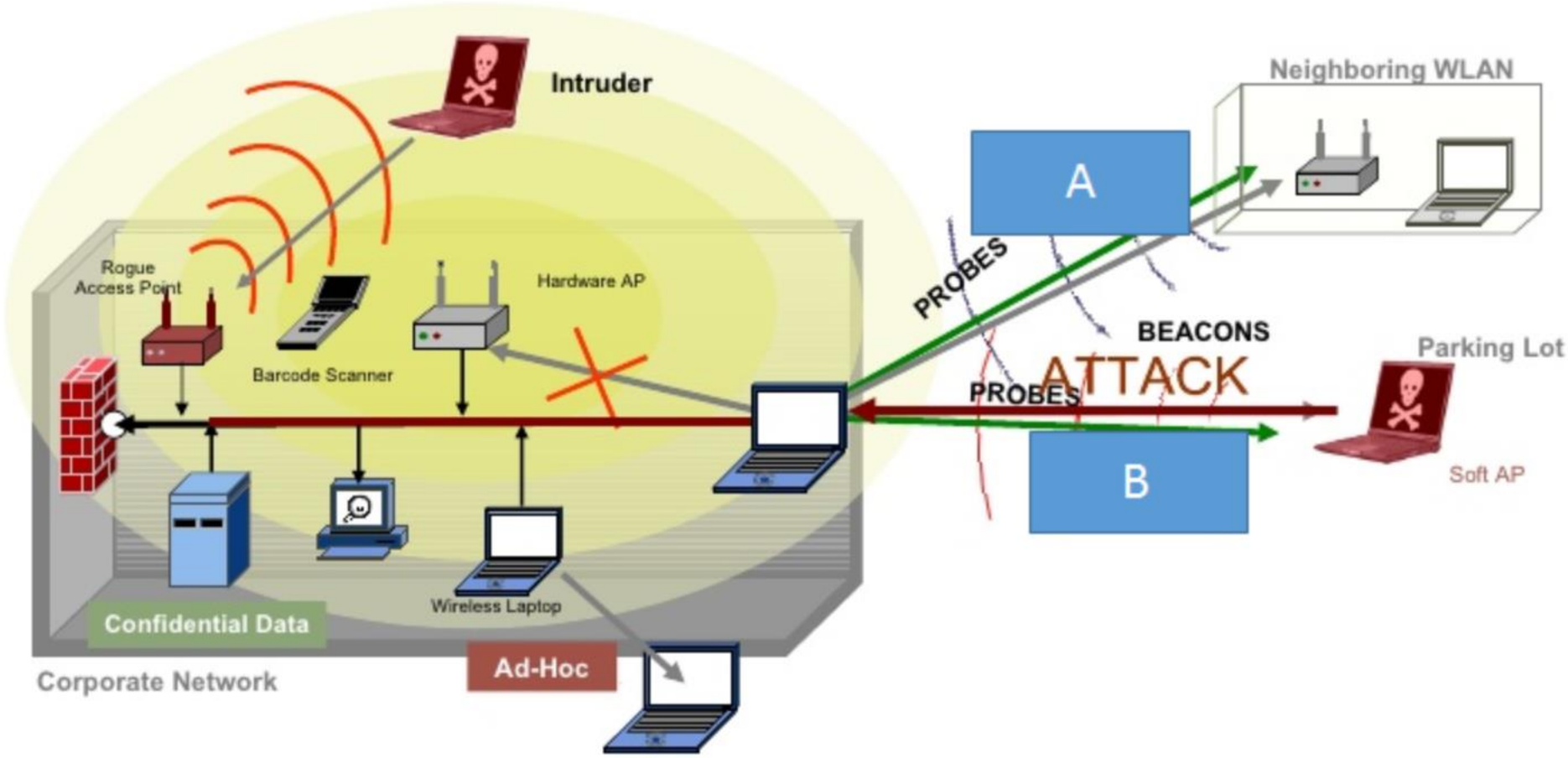
- Can you identify the main security issues with mobile devices?
- Can you identify the main security issues with wireless devices?
- Can you identify threats unique to the wireless network?

- Can you explain the security claims of IEEE 802.11 and the issue with these claims?
- Can you describe the security provided by Robust Security Network (RSN)/IEEE 802.11i?

QUEEN'S UNIVERSITY BELFAST

Example question

Identify and briefly describe the two wireless network threats indicated by Boxes A and B in the figure. [4 marks]



QUEEN'S UNIVERSITY BELFAST

Test Structure

- 1 hour
- 20 Questions
- QuestionMark e.g. Multiple Choice, Matching, Short Essay Response

QUEEN'S UNIVERSITY BELFAST

Questions?

QUEEN'S UNIVERSITY BELFAST