Network Security – Class Test Review

Dr. Sandra Scott-Hayward

CSC3064 Week 6 Assessment Update

School of Electronics, Electrical Engineering and Computer Science

CSC3064 – Class Test 1 Review

The CIA triad comprises what elements? Lecture 3

Availability, confidentiality, integrity

- ☐ Authenticity, authorization, accountability
- ☐ Capable, available, integral
- ☐ Confidentiality, integrity, authenticity
- ☐ Availability, confidentiality, integrity

Fill in the blanks in the following sentence: As a consequence of traffic [ ], if a security policy requires a more differentiated traffic treatment, it is better to implement it at a [ ] level. [2 marks]

Lecture 4

Mixing/multiplexing, higher

QUEEN'S UNIVERSITY BELFAST

CSC3064 – Class Test 1 Review

What are the consequences of a BGP Hijack attack? Lecture 7

Mis-deliver internet traffic to malicious endpoints

Cause routing instability in the Internet

- [ ] Mis-deliver internet traffic to malicious endpoints
- [ ] Cause routing instability in the Internet
- [ ] Improve routing stability in the Internet
- [ ] The attacker's MAC address becomes linked with the IP address of a legitimate computer

QUEEN'S UNIVERSITY BELFAST

CSC3064 – Class Test 1 Review

What are the components of Secure Inter Domain Routing (SIDR)? Lecture 7

Resource Public Key Infrastructure, BGP Path Validation, BGP Origin Validation

- ○ Resource Public Key Infrastructure, BGP Path Validation, BGP Origin Validation
- ○ Resource Public Key Infrastructure, BGP Origin Validation, BGP Source Validation
- ○ Resource Public Key Infrastructure, Resource Private Key Infrastructure, BGP Origin Validation
- ○ BGP Path Validation, BGP Origin Validation, BGP Secret Key Exchange

Identify the security challenges with Software-Defined Networking (SDN). Select all that apply. [3 marks] Lecture 5

- ☐ Controller Flow Table Flooding
- ☐ Switch Flow Table Flooding
- ☐ Malicious Applications
- ☐ Controller Hijacking
- ☐ Flow Table Policy Conflicts

QUEEN'S UNIVERSITY BELFAST

All except Controller flow table flooding

CSC3064 – Class Test 1 Review

List (in order) the 6 steps in a high level systems engineering process to provide network system security.

A high level systems engineering process

Lecture 2

Specify system architecture:

- Identify components and interrelations

Identify threats, vulnerabilities and attack techniques:

- The threat tree technique provides help for this step

Estimate component risks by adding attributes to the threat tree:

- However, removing subjectivity from initial assessments is often impossible and other attributes than criticality and effort (e.g. risk of detection) might have to be considered as well

Prioritize vulnerabilities:

- Taking into account the components' importance

Identify and install safeguards:

- Apply protection techniques to counter high priority vulnerabilities

Perform potential iterations of this process

- Re-assess risks of the modified system and decide if more iterations are required

QUEEN'S UNIVERSITY BELFAST

QUEEN'S UNIVERSITY BELFAST

CSC3064 – Class Test 1 Review

Identify the security issues with DNS. Lecture 8

DNS does not support data origin authentication

DNS does not support data integrity

- [ ] DNS does not support data integrity
- [ ] DNS does not support route attestation
- [ ] DNS does not support tunneling
- [ ] DNS does not support data origin authentication

Fill in the blanks in the following sentence: DNSSEC introduces added [ ] with the requirement to sign and check DNS records and to manage [ ]. This makes it [ ] to perform DoS attacks on DNS servers. [3 marks]

QUEEN'S UNIVERSITY BELFAST

complexity, key distribution, easier

CSC3064 – Class Test 1 Review

Malicious modification of patient information stored in a database is a breach of which security objective?

Integrity/Data Integrity

Lecture 2/3

What is the proper sequence of the TCP three-way-handshake?

Lecture 6

- ○ ACK, SYN-ACK, SYN
- ○ SYN-SYN, SYN-ACK, SYN
- ○ SYN-ACK, ACK, ACK
- ○ SYN, SYN-ACK, ACK

SYN, SYN-ACK, ACK

QUEEN'S UNIVERSITY BELFAST

CSC3064 – Class Test 1 Review

Match the threats to the correct description.

Lecture 2

Masquerade:

- An entity claims to be another entity

Eavesdropping:

- An entity reads information it is not intended to read

Authorization Violation:

- An entity uses a service or resources it is not intended to use

Loss or Modification of (transmitted) Information:

- Data is being altered or destroyed

Denial of Communication Acts (Repudiation):

- An entity falsely denies its' participation in a communication act

Forgery of Information:

- An entity creates new information in the name of another entity

Sabotage (Denial of Service):

- Any action that aims to reduce the availability and / or correct functioning of services or systems

QUEEN'S UNIVERSITY BELFAST

CSC3064 – Class Test 1 Review

Calculate the risk value given that the attacker effort to conduct the attack is 5 and the criticality of the network threat has a value of 15. Enter your answer as a numeric value.

Lecture 2

3

(Risk = Criticality/Effort)

What are the main characteristics of Software-Defined Networking (SDN) generally considered for improving network security? [1 mark]

Lecture 5

- ◯ Programmability and logically centralized control
- ◯ Programmability and logically distributed control
- ◯ Open interfaces and built-in AAA
- ◯ Built-in AAA and 3rd party applications

Programmability and logically centralized control

QUEEN'S UNIVERSITY BELFAST

CSC3064 – Class Test 1 Review

Which tool can trace the path of a packet?

Lecture 6/Practical 1

- ping
- Tracert
- whois
- DNS

Tracert

A SYN cookie is used as a defence against SYN flood attacks. True or False?

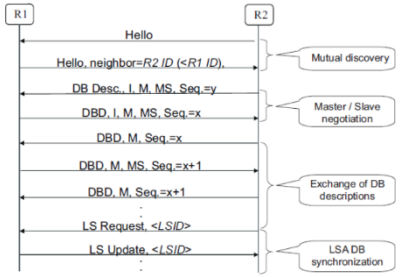
Lecture 6

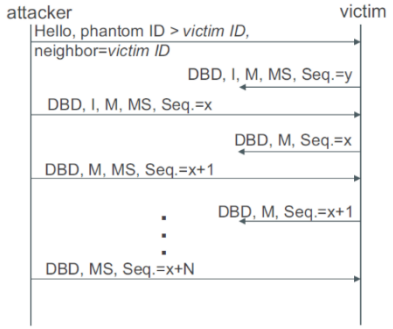
True

QUEEN'S UNIVERSITY BELFAST

CSC3064 – Class Test 1 Review

Briefly (in a few sentences) describe the OSPF Remote False Adjacency Attack. Lecture 7





OSPF – Remote False Adjacency Attack

Attacker sends packets that appear to come from the phantom router (i.e. spoofed src IP) destined to the victim router

Step 1: Attacker sends hello message to victim (phantom ID numerically larger than victim ID)

Step 2: Victim starts adjacency setup with phantom (sending Database Description (DBD) message with arbitrary sequence number). This message and other messages are not received by the attacker.

Step 3: Attacker sends a DBD message claiming to be master of the exchange and suggests a different sequence number. The phantom is elected to be master as it has a higher ID (see step 1).

Step 4: Victim adopts the sequence number and attacker continues to send empty DBD messages with increasing sequence number.

To complete the protocol, attacker must complete the exchange after the victim has sent out all its DBD messages but the attacker is not receiving these messages. However, the attacker is on the same AS as the victim so knows roughly how many DBD messages would be required to convey the database content.

Step 5: The attacker sends its final DBD message, the victim does not request LSAs from the phantom because it assumes the database is empty (see Step 4) and the victim ends the adjacency setup.

Step 6: The victim advertises a link to the phantom on behalf of its network.

QUEEN'S UNIVERSITY BELFAST

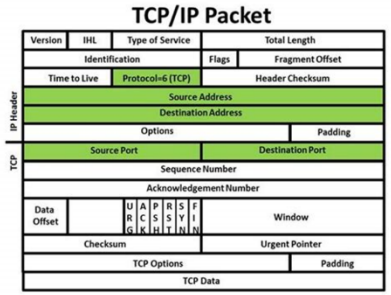
QUEEN'S UNIVERSITY BELFAST

CSC3064 – Class Test 1 Review

Give an example of a header-based attack. You should name the attack and briefly describe it in 1/2 sentences. [3 marks]

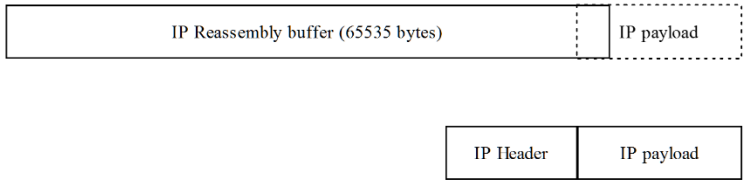
Lecture 3

- Creation of invalid packets, different protocols handle bad packets differently
- Source and destination address manipulation
  - Device can be confused by setting source and destination to the same address
- Setting bits in the header that should not be set
- Putting values in the header that are above or below the level specified in the standard



Header based – Example: Ping of Death

- Correctly formed ping is 64 bytes including IP header
- IPv4 packet may be as large as 65,535 bytes



For a detailed description, see:
https://www.cloudflare.com/learning/ddos/ping-of-death-ddos-attack/

offset = 65528 (max value)
length = 100

QUEEN'S UNIVERSITY BELFAST

CSC3064 – Class Test 1 Review

Lecture 6

What is the main vulnerability of the Internet Protocol from a network security perspective?

- ○ No ordering or delivery guarantees
- ○ No error reporting
- ○ No dst IP authentication
- ○ No src IP authentication

No Src IP authentication

In the layered network model, security protection at higher levels can be used to protect protocol headers of lower protocol layers. True or False? [1 mark]

Lecture 4

- ○ True
- ○ False

False

QUEEN'S UNIVERSITY BELFAST

CSC3064 – Class Test 1 Review

List the 4 levels at which distinct requirements for security protocol elements arise.

Lecture 4

End system, Link, Subnetwork, Application

QUEEN'S UNIVERSITY BELFAST