Cosc 362 Exam Past Exams

Data and Network Security (University of Canterbury)

2017 exam

Problem 1. [20 marks in total] [Intrusion Detection System (IDS)]

1. [6 marks] Which type of IDS would you deploy to detect the cyber-attack described in the box below? You have to answer the question using the IDS classification method and explain the reason why you have chosen that type(s).

A TCP open port scan is performed by an attacker to a specific target host; the traffic is not encrypted; the requirement is to detect known port scanning attacks.

2. [5 marks] Receiver Operating Characteristics (ROC) curves are often used to assess IDS quality. An example graph of two ROC curves is shown in Figure 1, where X axis represents false positive rate and Y axis represents true positive rate.

Assume that IDS A and IDS B have the ROC curve A (dotted line) and curve B (solid line), respectively.
Which IDS would you choose to use, IDS A or B? Explain the reason why. Which one has a higher false positive?

3. [5 marks] How can an IDS be used in conjunction with a packet filter firewall and security information and
event management (SIEM), respectively?

4. [4 marks] Explain two ideas that a Honeypot can be used to enhance cyber security.

Problem 2. [35 marks in total] [Cryptography Basics]

1. [5 marks] A researcher has developed a variant of the Caesar cipher as defined in equation (1).
C =E(P) = k*P mod 26 (1)
Where P denotes plaintext, C denotes ciphertext, k is the key and * means multiplication.
If k =5, compute the ciphertext for the following plaintext “This is a secret message”. Ignore the space
between words and the message is not a case sensitive.
2. [5 marks] Encrypt the same plaintext in the Problem 2.1 above using the Rail fence cipher (aka, a zigzag
cipher) with the depth (key) 4. Ignore the space between words.
3. [5 marks] Show how the principle of ciphers can be realised using the two ciphers in the Problems 2.1 & 2.2.
(Hint: product cipher and rounds). Make sure to show a concrete example.
4. [10 marks] Which mode of operation would you choose for a satellite communication, 3DES-ECB, AES128-
CTR, or AES128-CBC? Clearly state your assumption(s) and justify your answer.
5. [10 marks] Explain how a cryptographic hash function H can be used to enhance the password security,
and one of its drawbacks. You have to use all the keywords including password, salt, dictionary attack, and
rainbow table.

Problem 3. [45 marks in total] [Public key, PKI and Cryptographic Protocols]

1. [10 marks for the whole question] [RSA] A decryption key d of RSA will be calculated with two primes
p=17, q=31, and the encryption key e will be 5<e<9. (Show all of your work with all the relevant
mathematical equations).
a) [2 marks] Compute modulus n and totient ϕ(n), respectively.
b) [5 marks] choose an appropriate encryption key e (note that 5<e<9.) and find the decryption key d using the
extended Euclidean algorithm, and show the public key KU and private key KR, respectively.
c) [3 marks] Encrypt '5' using the public key (use an efficient power computation method) and decrypt the
ciphertext using the private key.
2. [10 marks] [PKI] Explain how to generate a public key certificate of using the following definitions of
notations/symbols in the box below. You may define and use other symbols and/or subscripts if necessary.
(Hint: 1. Creation of an unsigned certificate. 2. Generate a message digest. 3. Encrypt.)
Definitions
UC: an unsigned certificate,
H: a cryptographic hash function,
E: asymmetric encryption algorithm,
PUX: user X's public key, PRX: u ser X's private key.
3. [10 marks for the whole question] [SSL]
a) [6 marks] A web client and a web server have agreed to use the following cipher suite (cs) Y. What security
services can be provided? You have to explain specific cryptographic algorithms used.
cs Y: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
b) [4 marks] Explain the concept of "forward secrecy" using the procedure to generate key materials for SSL.
4. [15 marks for the whole question] [IPSec] Figure 2 is used for this question.
Figure 2. IPSec packet detail
a) [4 marks] What field(s) will be encrypted when IPSec ESP is used in transport mode? List the field number(s)
and justify your answer.
b) [4 marks] What field(s) will be authenticated when IPSec ESP is used in transport mode? List the field
number(s) and justify your answer.
c) [3 marks] What field(s) will NOT be needed when IPSec AH is used in transport mode? List the field
number(s) with the reason.
d) [4 marks] Why is Virtual Private Networks (VPN) used? What are one advantage and one disadvantage of
SSL VPN over IPSec VPN?

2016 exam

1. [14 marks for the whole question] [IPSec]

a) [2 marks] Why does IPSec need a security association (SA)?

b) [4 marks] Briefly explain how SPD and SAD in IPSec work.
c) [4 marks] Draw a figure to show an ESP packet created in transport mode. You need to include
the following words: IP header, transport header and payload. Also explain what information is
encrypted and/or authenticated.
d) [4 marks] Briefly compare and contrast SSL VPN and IPSec VPN.

2. [14 marks for the whole question] [Vulnerability Assessment]

a) [4 marks] What advantages does penetration testing provide compared to vulnerability
scanning? Why can't penetration testing be performed every day?
b) [4 marks] Compare UDP scan and TCP stealth scan when a target port is open by drawing two
figures.
c) [6 marks] What is CVE? What is the relationship between the CVE and NVD? What action(s)
does a system administrator (or a security decision maker) take if a CVSS BS of a CVE is
greater than 9?

3. [32 marks for the whole question] [Attacks]

a) [6 marks] Briefly explain the three characteristics of APT attacks. Why they are whard to
defend?
b) [4 marks] What kind of target discovery and propagation techniques does the Slammer worm
use? Why are they effective?
c) [2 marks] Describe the Clickjacking attack.
d) [4 marks] Explain the reason why "zero-day" vulnerabilities and attacks are hard to deal with.
e) [4 marks] Explain how TCP session hijacking can be performed between Alice and Bob using
IP spoofing attack and TCP Sequence prediction attack. You need to draw a figure to illustrate
them.
f) [4 marks] Describe how a Cross-Site Scripting attack can be launched using three entities
involved in communication.
g) [4 marks] Briefly describe SIP flooding attacks (hint: invite request).
h) [4 marks] Why are DNS amplification DDoS attacks effective?

4. [11 marks for the whole question] [firewalls]

SMTP (Simple Mail Transfer Protocol) is the standard protocol for transferring e-mails between
hosts over TCP. A TCP connection is set up between a user agent and a server program. The server

listens on TCP port 25 for incoming connection requests. The user end of the connection is on a
TCP port number above 1023. Suppose you wish to build a packet filter rule set allowing inbound
and outbound SMTP (Simple Mail Transfer Protocol) traffic as summarized in Table 1.

Table 1. Rule set.

Rule	Direction	Src Addr	Dest Addr	Protocol	Dest port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	In	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

Your email server host in this example has IP address 172.16.1.1. Someone tries to send e-mail
from a remote host with IP address 192.168.3.4. If successful, this generates a SMTP dialogue
between the remote user and the SMTP server on your host consisting of SMTP commands and
mail. Additionally, assume that a user on your host tries to send e-mail to the SMTP server on the
remote system. Table 2 shows typical packets from this scenario.

Table 2. Five packets information

Packet	Direction	Src Addr	Dest Addr	Protocol	Dest port	Action
P1	In	192.168.3.4	172.16.1.1	TCP	25	?
P2	Out	172.16.1.1	192.168.3.4	TCP	1021	?
P3	Out	172.16.1.1	192.168.3.4	UDP	25	?
P4	In	192.168.3.4	172.16.1.1	TCP	1357	?
P5	Out	192.168.3.4	172.16.1.1	TCP	28	?

a) [5 marks] Indicate which packets (in Table 2) are permitted or denied and which rule in Table
1 is used in each case.

P1 allow per rule A
P2 deny
P3 deny
P4 allow per rule D
P5 deny

b) [3 marks] Can a packet filter firewall be useful to block a TCP open scan? Why? Why not?
c) [3 marks] In order to counteract against TCP sequence prediction attacks will you use a packet
filter firewall or a stateful inspection firewall? Justify your answer.

5. [14 marks for the whole question] [IDS/IPS/ITS]

a) [4 marks] Classify Intrusion Detection Systems (IDS) according to two well-known criterion.
b) [4 marks] What are pros and cons of signature based intrusion detection techniques? Pros: We can detect signatures of malicious codes that has been seen before. Con: We cannot detect any future or never before seen malicious code.
c) [3 marks] We have discussed detection accuracy of intrusion detection systems. Which one
(false positive or false negative) is more critical to the system? Why? False negative. A false positive is just being 'too careful' but a false negative is being 'too careless', which means we are letting in something suspicious in our network.
d) [3 marks] Briefly compare IDS, Intrusion Prevention Systems (IPS) and Intrusion Tolerance
Systems (ITS).

6. [15 marks for the whole question] [Security Modelling and Assessment]

a) [6 marks] The items in the box below are actions to perform security risk assessment. You have to perform a security risk assessment for a smart phone. You need to come up with a
specific case and show how the security risk assessment can be carried out.

Analyzing existing controls, Analyzing risks, Asset identification, Assess risk likelihood,
Threat identification, Vulnerability identification

b) [5 marks] What are the advantages of using graphical models for security (e.g., attack
graphs) over typical vulnerability scanning (using OpenVAS or NESSUS)?
c) [4 marks] Determine the most appropriate location (from A through E) where each security
solution will be deployed at in the given enterprise network (e.g., S2 for A). You can use
only one security solution for one location. Also briefly explain the reason why you have
chosen to deploy them at such locations.

S1: An Anti-DDoS solution, S2: a Network Intrusion Detection System, S3: a packet filter
firewall, S4: a web-application firewall (WAF)

2015 exam

Section I. Internet Security Protocols [30 marks in total]

1. [5 marks for the whole question] [PKI]
a) [2 marks] What is X.509? Briefly explain.
b) [3 marks] Briefly list six key elements that are included in a X.509.
2. [14 marks for the whole question] [IPSec]
a) [2 marks] Why does IPSec need a security association (SA)?
b) [2 marks] How are SAs established? Briefly explain two phases to setup a SA.
c) [5 marks] Draw a figure to show an ESP packet is created in tunnel mode. You need to

include
the following words: IP header, transport header and payload. Also explain what information is
encrypted and/or authenticated.
d) [5 marks] Which security protocol would you use SSL or IPSec to implement VPN? Briefly compare and contrast SSL VPN and IPSec VPN.
3. [8 marks for the whole question] [SSL]
a) [1 mark] Can we use SSL with UDP? Why or why not? Explain.
b) [3 marks] What is the difference between a session and a connection in SSL? Also explain one
idea to speed up SSL.
c) [4 marks] Draw a figure that shows how the SSL record protocol works. You have to include
the following words (ciphertext, compression, fragment, MAC, Security parameter, SSL plaintext).
4. [3 marks for the whole question] [PGP]
a) [2 marks] Assume Alice needs to send an e-mail to Bob. Explain how the confidentiality of the
e-mail is achieved using PGP.
b) [1 mark] Does PGP use a PKI? Explain how PGP gets a public key.

Section II. Attacks [38 marks in total]

5. [10 marks for the whole question] [Vulnerability Assessment]
a) [2 marks] What are the differences between vulnerability scanning and penetration testing?
b) [4 marks] Compare TCP open scan and TCP stealth scan when a target port is closed. You
need to show two figures.
c) [2 marks] What is CVE? What is the relationship between the CVE and NVD?
d) [2 marks] In what situations a fragmentation scan is not effective?
6. [8 marks for the whole question] [Attacks 1]
Write the term that best represents each of the following descriptions (1 mark for each question).
a) An attack using code in compromised web site that exploits a browser vulnerability to attack a
client system when the site is viewed.
b) Any mechanisms that bypass a normal security check; it may allow unauthorized access to
functionality in a program, or onto a compromised system.
c) A code inserted into malware by an intruder. It lies dormant until a predefined condition is met;
the code then triggers an unauthorized act.
d) A set of hacker tools used after attackers have broken into a computer system and gained rootlevel
access.
e) A program activated on an infected machine that is activated to launch attacks on other machines.
f) This involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages.
g) A typical attack uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top level page.
h) It captures keystrokes on a compromised system.
7. [20 marks for the whole question] [Attacks 2]

a) [3 marks] Briefly explain the three characteristics of APT attacks.
b) [2 marks] Briefly explain two differences between computer viruses and worms.
c) [2 marks] What are “zero-day” attacks? List one example.
d) [2 marks] What is a Cross-Site Scripting attack?
e) [4 marks] Explain how TCP session hijacking can be performed between Alice and Bob using
IP spoofing and TCP Sequence attack.
f) [2 marks] Explain DNS amplification DoS attacks.
g) [5 marks] The following is a vulnerable C program. Explain how a stack-based bufferoverflow
attack can be carried out using the program.

```
#include <stdio.h>
main()
{
int buf3;
 int buf2;
 char buf1[20];
 fgets(buf1,48,stdin);
 if (buf2==0xbadc0ded)
 {
 setreuid(0,0);
 system("/bin/sh");
 }
}
```

Section III. Prevention, Detection and Management [32 marks in total]

8. [10 marks for the whole question] [firewalls]
SMTP (Simple Mail Transfer Protocol) is the standard protocol for transferring e-mails between
hosts over TCP. A TCP connection is set up between a user agent and a server program. The server
listens on TCP port 25 for incoming connection requests. The user end of the connection is on a
TCP port number above 1023. Suppose you wish to build a packet filter rule set allowing inbound
and outbound SMTP (Simple Mail Transfer Protocol) traffic as summarized in Table 1.

Table 1. Rule set.

Rule	Direction	Src Addr	Dest Addr	Protocol	Dest port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	In	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

Your email server host in this example has IP address 172.16.1.1. Someone tries to send e-mail
from a remote host with IP address 192.168.3.4. If successful, this generates a SMTP dialogue
between the remote user and the SMTP server on your host consisting of SMTP commands and
mail. Additionally, assume that a user on your host tries to send e-mail to the SMTP server on the
remote system. Table 2 shows typical packets from this scenario.

Table 2. Five packets information

Packet	Direction	Src Addr	Dest Addr	Protocol	Dest port	Action
P1	In	192.168.3.4	172.16.1.1	TCP	25	?
P2	Out	172.16.1.1	192.168.3.4	TCP	1023	?
P3	Out	172.16.1.1	192.168.3.4	TCP	25	?
P4	In	192.168.3.4	172.16.1.1	TCP	1357	?
P5	In	192.168.3.4	172.16.1.1	TCP	28	?

a) [5 marks] Indicate which packets (in Table 2) are permitted or denied and which rule in Table
1 is used in each case.

b) [3 marks] Explain how a stateful inspection firewall can overcome the drawbacks of a packet
filter firewall using a TCP sequence prediction attack.

c) [2 marks] How does a Network based Intrusion Prevention System differ from a packet filter
firewall? List two differences.

9. [10 marks for the whole question] [IDS]

a) [4 marks] What does the following Snort rule do? What is a drawback of this signature based
detection techniques?

```
alert tcp !$HOME_NET any -> $HOME_NET 80 (flags: S; msg:"Possible TCP
DoS"; flow: stateless; threshold: type both, track by_src, count 70, seconds 10;
sid:10001;rev:1;)
```

b) [3 marks] Describe how machine learning techniques (e.g. SVM) can be used for anomaly detection in Intrusion Detection Systems.

c) [3 marks] We have discussed detection accuracy of network intrusion detection systems (NIDS). Suppose you have a test of a NIDS that is 99.99% accurate in detection. Is this good enough? Discuss the performance of the NIDS in terms of false alarms (false positive and false
negative).

10. [12 marks for the whole question] [Security Modeling and Assessment]

Figure 1. A network

Suppose a network in Figure 1 under the following assumptions: A is an attacker host and the goal
of the attacker is to acquire the root privilege of the host F. Each host (host B, C, D, E and F) has
only one vulnerability (which allows the attacker to acquire a root privilege of the host), for instance, the host C has VC. If the attacker successfully exploits the vulnerability, the attacker can
get the root privilege of the host. FW represents a firewall and it has defined rules for reachability
(e.g. ‘Allow C > E’ means that C is allowed to connect to E via the firewall.).

a) [4 marks] Draw an attack graph for the network.

b) [1 mark] How can you get the probability value in practice?
c) [4 marks] Calculate the overall risk of the network using the attack graph and the values in Table 3. Ii represents an impact value of host i and pi represents the probability of attack success for the host (e.g. IB is the impact value of the host B and pB is the probability of attack
success to exploit the vulnerability of the host B).
d) [3 marks] List three possible security controls to reduce the overall risk for the network.

Table 3. Impact and Probability value of hosts

Host	Impact	Probability
B	1	0.4
C	2	0.7
D	3	0.5
E	5	0.5
F	10	0.2