TE WHARE WĀNANGA O TE ŪPOKO O TE IKA A MĀUI
VICTORIA
UNIVERSITY OF WELLINGTON

TERMS TEST #1 — 2016
TRIMESTER TWO

NWEN 405
Security Engineering

Time allowed: TWO HOURS

Instructions: There are 90 possible marks on the terms test.

You should allow roughly one minute per mark.

Many of the questions require you to discuss an issue, compare options or evaluate a situation. For such questions, the assessment will take into account the evidence you present and any insight you demonstrate.

If additional space is required you may ask for a separate answer booklet.

The examination contains FOUR questions.

You must attempt ALL questions.

Question	Marks
1. Computer Security Concepts	25
2. Cryptographic Tools	20
3. Malware and Countermeasures	25
4. Denial-of-Service Attacks	20

Question 1 Computer Security Concepts **[20 marks]**

(a) [5 marks] Indicate the key differences between *data confidentiality* and *privacy*.

With privacy the individual is in charge (not necessarily so for confidentiality) and goes beyond confidentiality which is just about access because privacy includes whether there is a right to collect it in the first place (marks for definitions too).

(b) [2 marks] Describe a business application or service that would only require a moderate level of availability, make sure you justify your answer.

Recall question. Differences in impact.

Moderate - significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced.

Book had example of public website of a University. Can still carry out core business but can cause embarrassment affecting the "brand".

(c) [5 marks] Evaluate whether the use of message encryption would successfully prevent *release of message contents* and *traffic analysis* attacks.

Recall question. Learning objective: Give examples of the types of threats and attacks that apply to different categories of computer and network assets.

Release of message contents: eavesdropping on communication to learn its contents.

Traffic analysis: using information such as the pattern of communication to infer the nature of the communication taking place.

Encryption will be more successful preventing the release of message contents than traffic analysis because traffic analysis does not rely on knowing the message contents.

(d) [5 marks] Consider a situation where a user has been tricked into installing ransomware that encrypts all of the user's files and demands a ransom payment to decrypt them. Note that when the attack happened that the user was logged on as a system administrator despite rarely needing to perform system maintenance tasks.

Explain how the principle of *least privilege* could have been applied to improve security of the operating system and evaluate whether doing so would have been able to prevent this attack.

[5 marks]

Least privilege -- could have been applied by giving the user only rights necessary to do the job they were doing at the time of the installation of the ransomware.

Would prevent the ransomware encrypting any system files but would not have prevented encryption of the user's own files (we assume they are not privileged).

Possibly if the ransomware requires system rights to install, least privilege would have prevented the user downloading and installing it themselves.

(e) [5 marks] Explain the difference between an attack surface and an attack tree.

Hard = 4 marks (synthesis)

Attack trees consider how patterns of exploitation of vulnerabilities can be used together to achieve a goal -- this is a structured analysis.

Attack surface does not consider how vulnerabilities may be combined, it provides a flat analysis.

Question 2 Cryptographic Tools **[20 marks]**

(a) [5 marks] Discuss some possible problems that would have to be solved when automating *brute-force attacks* on a symmetric encryption schemes where a known plaintext is not available.

Recall question. Differences in impact.

A block cipher processes the input one block of elements at a time, producing an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along. Block cipher uses the same encryption key whereas the stream cipher using a varying keystream.

(c) [2 marks] Outline TWO situation where message authentication is more appropriate than message confidentiality. Justify your answer.

Recall question. Learning objective: Give examples of the types of threats and attacks that apply to different categories of computer and network assets.

There are a number of applications in which the same message is broadcast to a number of destinations. Two examples are notification to users that the network is now unavailable, and an

alarm signal in a control center. It is cheaper and more reliable to have only one destination responsible for monitoring authenticity. Thus, the message must be broadcast in plaintext with an associated message authentication tag. The responsible system performs authentication. If a violation occurs, the other destination systems are alerted by a general alarm.

Another possible scenario is an exchange in which one side has a heavy load and cannot afford the time to decrypt all incoming messages. Authentication is carried out on a selective basis, with messages being chosen at random for checking.

Authentication of a computer program in plaintext is an attractive service. The computer program can be executed without having to decrypt it every time, which would be wasteful of processor resources. However, if a message authentication tag were attached to the program, it could be checked whenever assurance is required of the integrity of the program.

(d) [10 marks] In this problem we will compare the security services that are provided by digital signatures (DS) and message authentication codes (MAC).

We assume that Oscar is able to observe all messages sent from Alice to Bob and vice versa.

Oscar has no knowledge of any keys but the public one in case of DS.

State whether and how (i) DS and (ii) MAC protect against each attack. The value auth(x) is computed with a DS or a MAC algorithm, respectively.

(i) (Message integrity) Alice sends a message x = "Transfer $1000 to Mark" in the clear and also sends auth(x) to Bob. Oscar intercepts the message and replaces "Mark" with "Oscar." Will Bob detect this?

Intermediate

Will be detected with both (i) DS and (ii) MAC.

(ii) (Replay) Alice sends a message x = "Transfer $1000 to Oscar" in the clear and also sends auth(x) to Bob. Oscar observes the message and signature and sends them 100 times to Bob. Will Bob detect this?

Intermediate = 10 marks (application)

Won't be detected by either (Remark: use timestamps).

(iii) (Sender authentication with cheating third party) Oscar claims that he sent some message x with a valid auth(x) to Bob but Alice claims the same. Can Bob clear the question in either case? Justify your answers.

Intermediate = 10 marks (application)

(i) DS: Bob simply has to verify the message with the public key from both. Obviously, only Alice's public key results in a successful verification.

(ii) MAC: Bob has to challenge both, Oscar and Bob, to reveal their secret key to him (which he knows anyway). Only Bob can do that.

(iv) (Authentication with Bob cheating) Bob claims that he received a message x with a valid signature auth(x) from Alice (e.g., "Transfer $1000 from Alice to Bob") but Alice claims she has never sent it. Can Alice clear this question in either case?

Intermediate = 10 marks (application)

(i) DS: Alice has to force Bob to prove his claim by sending her a copy of the message in question with the signature. Then Alice can show that message and signature can be verified with Bob's public key) Bob must have generated the message.
(ii) MAC: No, Bob can claim that Alice generated this message.

(e) [4 marks] Explain why a *keystreams* must have the property of being unpredictable but not necessarily statistically random.

Hard = 4 marks (synthesis)

In applications such as reciprocal authentication and session key generation, the requirement is not so much that the sequence of numbers be statistically random but that the successive members of the sequence are unpredictable.

With "true" random sequences, each number is statistically independent of other numbers in the sequence and therefore unpredictable.

However, true random numbers are not always used; rather, sequences of numbers that appear to be random are generated by some algorithm. In this latter case, care must be taken that an opponent not be able to predict future elements of the sequence on the basis of earlier elements.

Within context, a predictable keystream would allow an attacker to guess the future keystream and xor this against the ciphertext to reveal the plaintext.

Question 3 Malware **[20 marks]**

(a) [5 marks] Briefly describe the THREE main propagation mechanisms used by malware. Each description should identify the general principle, give an example of type of malware that uses the technique and some examples of how the propagation mechanisms might work.

Recall question.

1 Parasitic software fragments such as viruses that attach themselves to some existing executable content. The fragment may be machine code that infects some existing application, utility, or system program, or even the code used to boot a computer system. (2)

2. Worm programs exploit software vulnerabilities in client or server programs to gain access to each new system. They can use network connections to spread from system to system. They can also spread through shared media, such as USB drives or CD and DVD data disks. E-mail worms spread in macro or script code included in documents attached to e-mail or to instant messenger file transfers. (2)

3. Social engineering, "tricking" users to assist in the compromise of their own systems or personal information. Trojan horse and banking malware Trick someone to run a program with a tempting offer. (1)

(b) [2 marks] List FOUR mechanisms a virus can use to conceal itself.

Recall question.

Some mechanisms a virus can use to conceal itself include: encryption, stealth, polymorphism, metamorphism.

(c) [5 marks] Suppose you have a new smartphone and are excited about the range of apps available for it.

You read about a really interesting new game that is available for your phone. You do a quick Web search for it, and see that a version is available from one of the free marketplaces.

When you download and start to install this app, you are asked to approve the access permissions granted to it. You see that it wants permission to "Send SMS messages" and to "Access your address-book".

(i) Should you be suspicious that a game wants these types of permissions?

(ii) What threat might the app pose to your smartphone, should you grant these permissions and proceed to install it?

(iii) What types of malware might it be?

Recall question. Application of knowledge.

(i) If when you download and start to install some game app,youare asked to approve the access permissions "Send SMS messages" and to "Access your address-book", you should indeed be suspicious that a game wants these types of permissions, as it would not seem needed just for a game.

(ii) Rather it could be malware that wants to collect details of all your contacts, and either return them to the attacker via SMS, or allow the code to send SMS messages to your contacts, perhaps enticing them to also download and install this malware.

(iii) Such code is a trojan horse, since it contains covert functions as well as the advertised functionality.

(c) [5 marks] Consider the use of a (host-based) personal firewall and anti-virus software deployed as countermeasures against malware on a personal computer.

(i) Which of these countermeasures would help block the spread of macro viruses spread using email attachments? Justify your answer.

(ii) Which would block the use of backdoors on the system? Justify your answer.

Evaluation question (higher order thinking)

(i) Anti-virus software helps block the spread of macro viruses spread using email attachment -- because it would identify the virus in the incoming email and block it.

Firewall would block access to disallowed services, macro virus exploits permitted services.

(ii) A (host-based) personal firewall could block the use of backdoors on the system -- because would close down ports used for access.

Anti-virus hopefully would detect the backdoor virus or trojan but could do nothing once it is installed and running.

(e) [5 marks] Many antivirus programs combine both heuristic scanners and activity traps. Explain why such an antivirus program might be able to detect that a program has been infected but not be able to identify the virus.

Hard =5 marks (synthesis)

Activity traps identify malware by its actions rather than its structure in an infected program.

These programs watch for the small set of actions that indicate malicious activity is being attempted and then to intervene.

This set of actions is not sufficient to identify a given virus, they merely identify a potential miusue pattern.

A heuristic scanner uses rules to search for probable malware instances.

One class of such scanners looks for fragments of code that are often associated with malware.

A scanner may look for the beginning of an encryption loop used in a polymorphic virus and discover the encryption key. Once the key is discovered, the scanner can decrypt the malware to identify it, then remove the infection and return the program to service.

A phishing attack uses a spam e-mail to exploit social engineering to leverage user's trust by masquerading as communications from a trusted source, that may direct a user to a fake Web site, or to complete some enclosed form and return in an e-mail accessible to the attacker. A more dangerous variant of this is the spear-phishing attack. This again is an e-mail claiming to be from a trusted source. However, the recipients are carefully researched by the attacker, and each e-mail is carefully crafted to suit its recipient specifically, often quoting a range of information to convince them of its authenticity. This greatly increases the likelihood of the recipient responding as desired by the attacker.

Question 4 Denial-of-Service (DoS) attacks **[20 marks]**

(a) [5 marks] Outline the aim of a denial-of-service attack (DoS) that targets the following categories of resources: network bandwidth; system resources; and application resources.

Recall question.

Network bandwidth -- overload the organization's link to the Internet. In a DoS attack, the vast majority of traffic directed at the target server is malicious, generated either directly or indirectly by the attacker. This traffic overwhelms any legitimate traffic, effectively denying legitimate users access to the server.

System resources -- Aims to overload or crash the network handling software. Rather than consuming bandwidth with large volumes of traffic, specific types of packets are sent that consume the limited resources available on the system.

Application resources -- Aim is to consume application resources, for example in a webserver to fill up queue of outstanding requests. Typically involves a number of valid requests, each of which consumes significant resources, thus limiting the ability of the server to respond to requests from other users.

(b) [5 marks] Define a reflection attack.

Recall question.

The attacker sends a network packet with a spoofed source address to a service running on some network server.

Spoofed source address belongs to the actual attack target.

Service responds to the spoofed source address.

Attacker sends a number of such spoofed requests to a number of servers with aim of generating a resulting flood of responses can overwhelm the target's network link.

(c) [5 marks] Discuss why "backscatter traffic" is generated by some types of denial-of-service attack but not by other DoS attacks.

Analysis question.

"backscatter traffic" are packets generated in response to a DoS attack packet with a forged random source address, e.g. the ICMP echo response from an ICMP echo request being used to flood a link.

Monitoring these packets, which are randomly distributed over the Internet, gives valuable information on the type and scale of attacks.

This backscatter traffic provides information on any DoS attacks that use a forged random source address with the destination address being the target, including various single and distributed flooding attacks, and syn spoofing attacks. It does not provide information on attacks that do not use randomly forged source addresses, or reflection or amplification attacks where the forged source address is that of the desired target.

(c) [5 marks] Using a TCP SYN spoofing attack, the attacker aims to flood the table of TCP connection requests on a system so that it is unable to respond to legitimate connection requests.

Consider a server system with a table for 256 connection requests.

This system will retry sending the SYN-ACK packet five times when it fails to receive an ACK packet in response, at 30 second intervals, before purging the request from its table.

Assume that no additional countermeasures are used against this attack and that the attacker has filled this table with an initial flood of connection requests.

(i) Calculate the rate at which the attacker must continue to send TCP connection requests to this system in order to ensure that the table remains full. Show your calculations.

Recall question.

Each connection request can occupy an entry up to six times with each entry lifetime being 30 seconds.

This is a total of 6 × 30 secs (initial + 5 repeats) = 3 min.

In order to ensure that the table remains full, the attacker must continue to send 256/ 3 or about 86 TCP connection requests per minute.

(ii) Assuming that the TCP SYN packet is 40 bytes in size (ignoring framing overhead), how much bandwidth (in bits per second) does the attacker consume to continue this attack?

Recall question.

Assuming the TCP SYN packet is 40 bytes in size, this consumes about 86 × 40 × 8 / 60, which is about 459 bits per second, a negligible amount.

(c) [5 marks] Suppose you have a new smartphone and are excited about the range of apps available for it.

You read about a really interesting new game that is available for your phone. You do a quick Web search for it, and see that a version is available from one of the free marketplaces.

When you download and start to install this app, you are asked to approve the access permissions granted to it. You see that it wants permission to "Send SMS messages" and to "Access your address-book".

(i) Should you be suspicious that a game wants these types of permissions?

(ii) What threat might the app pose to your smartphone, should you grant these permissions and proceed to install it?

(iii) What types of malware might it be?

Recall question. Application of knowledge.

(i) If when you download and start to install some game app,youare asked to approve the access permissions "Send SMS messages" and to "Access your address-book", you should indeed be suspicious that a game wants these types of permissions, as it would not seem needed just for a game.

(ii) Rather it could be malware that wants to collect details of all your contacts, and either return them to the attacker via SMS, or allow the code to send SMS messages to your contacts, perhaps enticing them to also download and install this malware.

(iii) Such code is a trojan horse, since it contains covert functions as well as the advertised functionality.

(c) [5 marks] Consider the use of a (host-based) personal firewall and anti-virus software deployed as countermeasures against malware on a personal computer.

(i) Which of these countermeasures would help block the spread of macro viruses spread using email attachments? Justify your answer.

(ii) Which would block the use of backdoors on the system? Justify your answer.

Evaluation question (higher order thinking)

(i) Anti-virus software helps block the spread of macro viruses spread using email attachment -- because it would identify the virus in the incoming email and block it.

Firewall would block access to disallowed services, macro virus exploits permitted services.

(ii) A (host-based) personal firewall could block the use of backdoors on the system -- because would close down ports used for access.

Anti-virus hopefully would detect the backdoor virus or trojan but could do nothing once it is installed and running.

(e) [5 marks] Many antivirus programs combine both heuristic scanners and activity traps. Explain why such an antivirus program might be able to detect that a program has been infected but not be able to identify the virus.

Hard =5 marks (synthesis)

Activity traps identify malware by its actions rather than its structure in an infected program.

These programs watch for the small set of actions that indicate malicious activity is being attempted and then to intervene.

This set of actions is not sufficient to identify a given virus, they merely identify a potential miusue pattern.

A heuristic scanner uses rules to search for probable malware instances.

One class of such scanners looks for fragments of code that are often associated with malware.

A scanner may look for the beginning of an encryption loop used in a polymorphic virus and discover the encryption key. Once the key is discovered, the scanner can decrypt the malware to identify it, then remove the infection and return the program to service.