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

EXAMINATIONS – 2014
TRIMESTER 2

NWEN405

Security Engineering

Time Allowed: THREE HOURS

Instructions: Closed Book.
There are 150 possible marks on the exam.

You should plan on spending 30 minutes reading the exam and reviewing your answers.

No calculators permitted.
Make sure you show your working.
Non-electronic Foreign language dictionaries are allowed.

No reference material is allowed.

Question	Topic	Marks
1.	Security Models and Policies	30
2.	Social Engineering and Physical Protection	30
3.	Software Vulnerabilties and Attacks	30
4.	Network Vulnerabilities and Attacks	30
5.	Crimeware and Exploitation	30
	Total	150

Question 1. Security Models and Policies [30 marks]

(a) [5 marks] Using an example, briefly describe the relationship between a *security policy* and *security mechanism*.

A security mechanism is a means for implementing a security policy. Example of a security policy might be that only authorized people are allowed access to the server room while an example of a security mechanism might be a locked door.

(b) [5 marks] Define the terms *Discretionary Access Control* and *Mandatory Access Control*.

DAC = owner specifies access rights for a protected object, MAC = system specifies access rights for a protected object. Other definitions exist but I am happy as long as they understand the main difference in terms of the locus of control.

(c) [5 marks] Briefly explain why the *Chinese-Wall security model* is an example of a Mandatory Access Control security model.

Current access defined by previous history of accesses. The system enforces this and there is no way that a user can grant access to another user and bypass the system controls.

(d) [5 marks] The *University of Belfuscu* provides access to a database containing salary data of its staff but does not allow queries that identify particular rows. However, it does allow averages based upon characteristics of staff to be calculated. Furthermore the averages cannot be calculated on the basis of a single individual.

Despite the inference controls, an attacker has succeeded in determining the salary of the *only Liliputian professor* in the University.

Name the type of query used to carry out this attack and outline how it might have been applied.

The technique is called a tracker. The general idea is to add additional circumstantial information to defeat averaging and other controls. For example, to find out the salary of a particular staff member who is is in the minority you can determine their salary by adding a query that finds out the population average and the population average for the group minus the minority.

(e) Consider a General using a computer system secured using the *Bell-LaPadula security model*. Imagine that she is required to issue written orders to her Lieutenant Generals.

(i) [5 marks] Explain why the computer system would prevent her from issuing the orders?

Answer must include discussion of clearances and classifications, identify the function of the no write rule and why it would prevent an information flow from high to low in this case

(ii) [5 marks] Outline TWO possible additions to the security model that would allow subjects such as the General to escape from this restriction and discuss the potential risks of adopting these.

*Outline the possibility of either making the generals trusted subjects who are exempted from the * property or doing a temporary downgrade. An exceptional answer would mention the problem with trust subjects is that they can do anything and this is usually a bad idea in any security system and that the temporary downgrade requires a mind wipe when applied to a live human being (in theory).*

Question 2. Social Engineering and Physical Protection [30 marks]

(a) You have been asked to give advice to staff running a medical center who often handle legitimate requests for patient information over the telephone from Accident Compensation Corporation (ACC) staff. Unfortunately, private investigators have been impersonating ACC staff in order to illegally access this information.

(i) [5 marks] Identify the type of social engineering technique being used by the private investigators and briefly explain how the technique relates to findings from experimental social psychology.

This is pre-texting. Gaining information by pretending to be someone authorized to be told it. People are naturally trusting and this exploits it. Exploits the fact that people will do immoral things and obey authority rather than their conscience. Stanley Milgram experiments. I DON'T EXPECT MANY PEOPLE TO GET THE MILGRAM LINK – GETTING TWO MARKS IS EASY, THREE MARKS IS HARD

(ii) [5 marks] Briefly explain what is *phishing* and how it differs from the attack used in this particular case.

Phishing is over the web, phishing is an attack on an individual in most cases

(iii) [5 marks] Outline a procedure based upon the concept of *operational security* that could be used to protect against this type of attack.

Whenever receive a request ask the caller which office they are calling from and ring them back. Make sure that the number that is rung back is the official number by checking against a trusted source.

(b) [15 marks] You have been hired as a security consultant for a controversial multi-millionaire who wishes to setup a data center in Wellington but is concerned about attacks by two main groups of people: (i) casual attackers who might wish to vandalize the installation; and, (ii) politically motivated individuals who wish to break into the data center.

You can assume that the neighbours will also be data center providers in an area zoned only for data center businesses.

Propose and evaluate the effectiveness of at least THREE different approaches to deterring potential attacks. Each approach should vary in terms of visibility (visible/invisible) and whether a mechanism is actually present or not.

When evaluating approaches you should consider the motivations of the attackers. You may wish to quote results from studies discussed in class or the readings.

Three scenarios. (1) Visible protection mechanism such as guards. (2) Advertise the presence of a mechanism but don't actually have it. (3) Don't advertise a mechanism. An excellent answer would draw upon the studies on the carjack system, discuss the role of free riders and evaluate what might work in terms of how many of the neighbours do have effective mechanisms and the motivations/resources of our two types of attacker.

Question 3. Software Vulnerabilities and Attacks [30 marks]

(a) Consider a program that is only provided to you as a binary.

(i) [2 marks] Briefly describe a security technique that could be used to locate security protections in the client program despite not having access to its source code.

The technique is reverse engineering, takes binary and allows you to step through the code.

(ii) [3 marks] Outline the steps involved in applying the security technique identified above to bypass the requirement for a special product activation key.

Solve using a reverse engineering tool such as IDA pro. You would step through the execution of the code as you run the system. The aim would be to identify where in the code that the check takes place and either bypass it or to find the password

(b) You have been given the task of advising a company on how to build a secure server that will be accessible over a public network such as the Internet.

(i) [5 marks] Briefly describe how the steps involved in a malicious *buffer overflow* for the x86 architecture.

Attacker calls the function with a long message, ending with the address of some code that gives her a shell. Arc and EIP written to stack. Attackers value is copied over the old EIP. Function runs and when function returns the attackers code is run.

(ii) [5 marks] Name and briefly explain at least ONE defence against *buffer overflows* that can be implemented without requiring the programmer to either modify their code or check the inputs to the program.

Stack canaries – values placed on a stack, later tested. if stack is overwritten the value test will fail. Randomization – layout of memory is randomized, makes it very hard for the attack to find the memory to overwrite or code to jump to. Input sanitization is another defence by it is not implemented within the compiler

(c) Attacks against web applications.

(i) [5 marks] Briefly describe a simple authentication scheme based upon cookies that is resistant to an eavesdropping attack.

Web application verifies username and password. Generates a cookie which is sent back to the user. Set-Cookie: auth=secret. When browser contacts the web site again, it includes the session authenticator. Eavesdropping is where the attacker listens on the network and steals the cookie information. Protect against this by either always using HTTPS or setting the secure flag on the cookie.

(ii) [5 marks] Outline how a *cross-site request forgery* or *CSRF attack* could allow an attacker to invoke the web application with the victim's privileges.

Victim is logged into the vulnerable web site. Victim visits malicious page on attacker web site. Malicious content is delivered to victim. Victim involuntarily sends a request to the vulnerable website. Browser sends the authentication cookie along with the request so it appears valid.

(iii) [5 marks] The *same-origin policy* has been implemented to prevent *CSRF attacks*. Explain why this technique does not work well for web applications that make extensive use of content distribution networks or web accelerators.

Toughie. Its in my notes. Unlike the other answers it requires them to do the reading. In this case same origin prevents a request to a website from coming from a script sourced from anywhere except the same domain. Problem is that content distributors (say for a jquery script) have different domains although being trusted and this prevents them from making invocations

Question 4. Network Vulnerabilities and Attacks [30 marks]

(a) Consider a *SYN flood denial-of-service* attack.

(i) [2 marks] What resource is being exhausted in this type of attack and what effect does it have on other clients of a server that is under attack?

Queue for tracking half-open connections, other connections on the same port will be rejected, only new ones though on the same port

(ii) [3 marks] Outline the role played by a *SYN flood* attack in a successful TCP/IP session hijack.

Success for session hijack requires preventing the target server from sending packets that would cause the victim from winning the race between the injected packet and the real packet. A denial-of-service attack that targets the TCP/IP connection between the server and client.

(iii) [5 marks] Briefly explain how *SYN cookies* work.

Client has to maintain the state on behalf of the server, the connection state is encoded and returned into the ISN field returned to the client, when the client completes the connection they provide that field value plus one and the server reconstructs the missing state by extracting this (minus one)

(b) Consider the *Domain Name System*.

(i) [10 marks] A friend has noticed that whenever they enter their bank's URL into their web browser that they are redirected to a site with the same domain name but different content.

Your investigations reveal that the domain name (`gbank.com`) is being resolved to a different IP address than the one associated with the real bank.

This only occurs on their machine on their home network and occurs irrespective of the client program being used to access the website.

Identify at least THREE techniques that an attacker might have used to achieve this behaviour, outline how each technique might have been implemented and propose a plan to determine which of these techniques is being used.

(1) host settings on the machine itself have been modified to include a static route. common method is malware. (2) home router has been reconfigured to use a DNS server under their control. possibly malware internally makes a UPnP request(3) DNS cache poisoning, number of approaches and a reasonable description of any of them would be acceptable. Essentially each technique is distinguishable by varying where in the system is that you try out your resolution. Test at different points along the path between the user's computer and the DNS server.

(ii) [5 marks] Briefly evaluate whether requiring the use of the TCP protocol instead of the UDP protocol would prevent DNS amplification attacks.

Ability to redirect the traffic to the victim server via spoofing with UDP. Requiring a connection to be setup would prevent this from happening at the cost of efficiency.

(c) [5 marks] You have been given the task of designing the replacement for an existing vulnerable network protocol. The replacement uses cryptographic mechanisms to protect nonces passed between the parties. Briefly outline some barriers to widespread adoption of the new protocol.

This is a pretty open question. In class we discussed that authentication requires some way to distribute and manage cryptographic keys, that the impact on performance has to be carefully managed and its impact on scale, that a simultaneous upgrade might be important so some way to allow adoption without immediately breaking clients and servers is required.

Question 5. Crimeware and Exploitation [30 marks]

(a) Consider the *Crimeware Ecosystem*.

(i) [5 marks] Describe a typical recruitment strategy for *money mules* and outline their role in the process of safely extracting money from a victim's bank account.

Target people with money problems – students etc. Send spam email outlining a job offer where they can work from home. Money mule has an account in same country as the victim. Hacker recruits the money mule. Hacker transfers money to mule's account. Mule transfers via a mechanism such as western union from the their account to the hacker.

(ii) [5 marks] Briefly compare and contrast the capabilities and approaches used by *criminal gangs* and groups deploying *advanced persistent threats*. How are they similar and how are they different in terms of resources, how they target and exploit their victims.

Criminal gang will used skilled programmers as will the ADT group. ADT will have greater resources because backed by government rather than criminal gang. ADT might also be able to influence the providers of infrastructure directly rather than having to subvert their systems. Criminal gang will spread their net wide, for example using spam to deliver attacks and exploit a large number of victims rather than just one. ADT will focus on a particular individual or organization, highly targeted attacks and will spend considerable time placing their tools in place and when they attack it will likely to be just once rather than repeatedly.

(b) Consider *Worms* and *Drive-by-Downloads*.

(i) [5 marks] Contrast these two attacks in terms of how they propagate and exploit vulnerabilities present in a victim's system.

Worm is self-propagating, searches out network vulnerabilities and attempts to exploit them in order to travel to a new host. Drive-by-download relies upon a user visiting a website and the code on the website exploiting a vulnerability in a user's computer.

(ii) [10 marks] You have been called in to consult on a strategy that has the goal of protecting a corporate network against the threats posed by worms and drive-by-downloads.

The strategy has FOUR main features: (1) remove the ability to plug USB sticks into workstations; (2) install signature-based antivirus scanners on workstations; (3) install a firewall at the border between the corporate network and the Internet; and, (4) enforce automatic operating system updates across all the machines on the network.

Briefly evaluate this strategy against its goals. Make sure you justify why you believe each of the features might be applicable or not applicable to countering the spread and effect of worms and drive-by-downloads.

(1) good for worms, no effect on drive-by-downloads because they propose via the web. (2) potentially good for both because will identify worms or the payload delivered by the drive by download. (3) good for worms, stops them getting out or coming in but no effect on drive by download because you cannot close down port 80. (4) good for worms and dvd because removes potential vulnerabilities exploited by both.

(c) [5 marks] A problem for any long running advanced persistent threat is how to receive software updates without revealing either that the updating process is happening or the source of the updates. Outline a process based upon the concept of a *dead drop* that could be used to deliver updates via photo sharing site.

I am looking for knowledge of what a dead drop site is or isn't and some technical knowledge. In particular how they hide the updates. Answer would be to encode in the headers if the photo sharing site is under your control or by encoding in the JPEG using stenography. Also an excellent answer would consider traffic analysis.

* * * * * * * * * * * * * * *