Assignment 1 : NWEN 405 Security Engineering

August 16th 2017

Due 15th September

Question 1 Computer Security Concepts [30 marks]

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

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

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

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.

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

f. [10 marks] Read Bruce Schneier's classic paper "Attack Trees" (1999).

https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Based upon this paper, create an attack tree capturing possible attacks that have the goal of discovering the content of the 2017 NWEN 405 examination. A hard copy of this is stored in a locked cabinet in my office and I keep the keys on me. I prepared the exam using latex on the School machines and the files are stored securely on state-opera.

Completeness, correctness and creativity count for this question.

Question 2 Malware [30 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.

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

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? Explain why.

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

(iii) What types of malware might it be? Explain why.

d. [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.

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.

f. [10 marks] Read this case study "Understanding Persistent Threats" by Ned Moran (2011): https://www.usenix.org/system/files/login/articles/105484-Moran.pdf

and also this blog entry "Top 10 Banking Trojans for 2017" by Jonathon Crowe (2017).

Compare these two types of threat in terms of:

(i) Methods of propagation and likelihood of success.

(ii) Role and types of payloads.

(iii) Effectiveness of technical and non-technical countermeasures.

Question 3 Denial-of-Service (DoS) attacks [35 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.

b. [5 marks] Describe the general principles behind a reflection attack.

c. [5 marks] Describe the NTP reflection attack (use a diagram to illustrate the exchange of messages).

d. [5 marks] Discuss why “backscatter traffic” is generated by some types of denial-of-service attack but not by other DoS attacks.

d. [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.

(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?

(iii) Why doesn’t a TCP SYN attack prevent connections to all servers hosted on a single machine?

d. [10 marks] Read this description of how CloudFlare works (https://www.quora.com/How-does-Cloudflare-work-Does-CloudFlare-just-divert-malicious-traffic) and answer the following questions.

(i) Why is CloudFlare considered a proxy service rather than just a pure CDN?

(ii) What security risks does (make sure you use the right terms here) using CloudFlare introduce? Would using https mitigate against these?

(iii) How do you configure your domain to use CloudFlare? Explain how this works to ensure that you use a datacenter close to your location.