DUBLIN INSTITUTE OF TECHNOLOGY

DT211C BSc. (Honours) Degree in Computer Science (Infrastructure)

Year 4

SUMMER EXAMINATIONS 2015/2016

ADVANCED SECURITY 2 [CMPU4008]

DR. FREDRICK MTENZI
DR. DEIRDRE LILLIS
MR. THOMAS NOLAN

WEDNESDAY 18TH MAY 1.00 P.M. – 3.00 P.M.

DURATION: 2 HOURS

ANSWER **THREE** QUESTIONS OUT OF **FOUR**.

ALL QUESTIONS CARRY EQUAL MARKS. One (1) complimentary mark will be given.

1 **(a)** Most software that has been built and released typically comes with a set of defects — implementation bugs and design flaws. To date, there has been a larger focus on finding implementation bugs rather than on identifying flaws. The IEEE Center for Secure Design (CSD) intends to shift some of the focus in security from finding bugs to identifying common design flaws in the hope that software architects can learn from others' mistakes. Discuss how to avoid the top ten software security design flaws identified by the IEEE CSD.

(20 marks)

(b) Suppose you observe that your home PC is responding very slowly to information requests from the net. And then you further observe that your network gateway shows high levels of network activity, even though you have closed your email client, web browser, and other programs that access the net. What type of malware could cause these symptoms? Discuss how the malware might have gained access to your system. What steps can you take to check whether this has occurred? If you do identify malware on your PC, how can you restore it to safe operation?

(13 marks)

2 **(a)** Some have argued that Unix/Linux systems reuse a small number of security features in many contexts across the system, while Windows systems provide a much larger number of more specific targeted security features used in the appropriate contexts. This may be seen as a trade-off between simplicity and lack of flexibility in the Unix/Linux approach, against a better targeted but more complex and harder to correctly configure approach in Windows. Discuss this trade-off as it impacts on the security of these respective systems, and the load placed on administrators in managing their security.

(10 marks)

(b) Discuss the main forms of attack strategies against password-based authentication and the countermeasures used to combat such attacks.

(11 marks)

(c) Explain why host hardening is needed? Briefly discuss each element of host hardening, giving examples where possible. Why do you think companies often fail to harden their servers and clients adequately?

(12 marks)

3. **(a)** Assume you have found a USB memory stick in your work parking area. Explain threats this might pose to your work computer should you just plug the memory stick in and examine its contents? In particular, consider whether each of the malware propagation mechanisms could use such a memory stick for transport. Explain the steps you could take to mitigate these threats, and safely determine the contents of the memory stick?

(9 marks)

(b) Bank customers can withdraw cash from Automated Teller Machines (ATMs) using a cash card and a Personal Identification Number (PIN).

Conduct a risk and threat analysis for this application, both from the point of view of the customers and the point of view of the bank.

(13 marks)

(c) **(i)** How can a firm obtain a good IT security staff?
(ii) Discuss the pros and cons of hiring reformed hackers.
(iii) Discuss the advantages and limitations of security training certifications.

(11 marks)

4. **(a)** Explain the strengths and weaknesses of each of the following firewall deployment scenarios in defending servers, desktop machines, and laptops against network threats.

a. A firewall at the network perimeter.
b. Firewalls on every end host machine.
c. A network perimeter firewall and firewalls on every host machine.

(13 marks)

(b) **(i)** Briefly explain what a DDoS attack is and give two examples of recent attacks.

(ii) In order to implement the classic DOS flood attack, the attacker must generate a sufficiently large volume of packets to exceed the capacity of the link to the target organization. Consider an attack using ICMP echo request (ping) packets that are 500 bytes in size (ignoring framing overhead). How many of these packets per second must the attacker send to flood a target organization using a 0.5 Mbps link?

(10 marks)

(c) In the last decade security threats and attacks on the Internet have increased significantly. Discuss whether or not building a new secure Internet is the answer.

(10 marks)