UNIVERSITY OF SOUTHAMPTON COMP6224W1

SEMESTER 1 EXAMINATION 2014 - 2015

FOUNDATIONS OF CYBER SECURITY

DURATION 120 MINS (2 Hours)

This paper contains 6 questions

Answer THREE questions, TWO questions from Section A and *one* from Section B.

An outline marking scheme is shown in brackets to the right of each question.

Each question is worth 25 marks. The overall mark out of 75 will then be scaled up to 100.

University approved calculators MAY be used.

A foreign language translation dictionary (paper version) is permitted provided it contains no notes, additions or annotations.

Page 1 of 7

Section A

Question A1.

(a) ‘APT’ stands for ‘*Advanced Persistent Threat*,’ a terminology introduced by Mandiant to refer to what?

[5 marks]

(b) Illustrate the *APT Attack Lifecycle* model (as presented in the Mandiant report on APT1, a particular APT group in China). What are the typical attack vectors for the first phase of the lifecycle model, the so-called ‘*Initial Compromise*’?

[10 marks]

(c) With reference to the APT1 Attack Lifecycle described above and other reports from Mandiant discussed in class, explain why it is crucial to protect information about the internal structure of a local network and of the organisation to which it belongs. Give some examples of the kind of information to protect.

[10 marks]

Question A2.

(a) What is meant by ‘*Multilevel Security*’? Describe the notion, explain why it is important, and list some of its existing applications.

[5 marks]

(b) Describe the notion of ‘*Information Flow Control*’ and illustrate the ‘*Bell-LaPadula*’ model. What are the main criticisms to such security model?

[10 marks]

(c) What does ‘RBAC’ stand for? How does it differ from the multilevel security model? What are its advantages?

[5 marks]

(d) What is meant by the term ‘*covert channel*’? List some examples of covert channels.

[5 marks]

TURN OVER

Question A3.

(a) Illustrate the ‘*GSM authentication protocol*’ for mobile phones, and explain why it makes phone cloning difficult. What are the main known vulnerabilities of the protocol? Explain.

[10 marks]

(b) Besides authentication, what other two security features are supposedly provided by the GSM system? Discuss the extent to which they are met.

[10 marks]

(c) Explain how *3G* improves the confidentiality of mobile communications with respect to GSM. What does it mean that 3G is a ‘*key escrow*’ system?

[5 marks]

Question A4.

The Bitcoin is the best known, most successful and diffused crypto-currency in existence.

(a) Explain why Bitcoin transactions need to be verified, and how the Bitcoin system achieves that. You may find it useful to make reference to the notion of *blockchain*, why and how it is built and kept consistent, and how it achieves its purpose.

[10 marks]

(b) Are there deficiencies of the *proof-of-work* concept as implemented in the Bitcoin system? Explain which and discuss potential remedies and/or alternatives.

[5 marks]

(c) What are the main risks to user security, privacy and anonymity in the Bitcoin system? Describe and illustrate potential attacks and known countermeasures.

[10 marks]

TURN OVER

Section B

Question B1.

As distributed denial of service (DDoS) attacks have become more common, attackers have sought to find the means to maximise the impact of their attacks, and - generally - to minimise the chances of attacks being traced back to them. The DNS has been used in recent years as one such means.

(a) What do you consider are the main reasons for individuals or groups to want to conduct denial of service attacks?

[4 marks]

(b) Describe how under normal operation a DNS resolver would perform a recursive lookup on the hostname `www.bbc.co.uk` to return the IPv4 address of that hostname. It may be useful to illustrate your answer with a diagram.

[5 marks]

(c) In early 2013, a large distributed denial of service (DDoS) attack took place against Spamhaus, in what was termed a 'DNS amplification attack.' Describe how the DDoS attack was believed to have been made, explaining clearly how the DNS was 'abused' to make the attack so effective, and the role of IP spoofing in the attack.

[8 marks]

(d) How would the use of a content delivery network, based on IP anycast or an equivalent technology, help mitigate such DDoS attacks for a content provider, and what other benefits might that use bring?

[4 marks]

(e) A generic problem in DDoS attacks is the ability of attackers to use IP spoofing. How might that problem be addressed by ISPs and operators of commercial or academic enterprise sites, and why do you think it has not been addressed seriously enough to date?

[4 marks]

Question B2.

The term "pervasive passive monitoring" has come to the fore since the recent Snowden revelations. It has become clearer that network traffic is being observed in transit between users and the services they are accessing, not only by Internet Service Providers (ISPs), but also by government agencies.

(a) Briefly describe the the naming and addressing schemes used at each layer of the TCP/IP networking model.

[4 marks]

(b) Different network security appliances operate at different layers, and therefore need to inspect different layers of the traffic passing through them. Explain the difference in the layers inspected for a device collecting network flow data (e.g. a Netflow collector) and a device doing deep packet inspection (e.g. an Intrusion Detection System, IDS).

[8 marks]

(c) There is a tension between a user's desire for privacy, and both an ISP's desire to be able to inspect traffic for network security purposes and a government's desire to counter terrorism. What do you think are the issues involved, and how should these be balanced?

[13 marks]

END OF PAPER