UNIVERSITY OF BIRMINGHAM

School of Computer Science

MSc Computer Science
MSc Advanced Computer Science
MSc Computer Security
First Year – UG Affiliate Computer Science/Software Engineering
Fourth Year – MSci Computer Science
Fourth Year – MEng Computer Science/Software Engineering
First Year – UG Affiliate Science without Boarders Computer Science

06 23900

Network Security

Summer Examinations 2015

Time allowed: 1 hour 30 minutes

[Answer ALL Questions]

1. In the context of network security, the *attack surface* of a computer includes the set of services and applications that an attacker can communicate with.

   (a) Describe two ways to determine which applications running on a computer are exposed to an attacker. **[8%]**

   (b) Describe two techniques to reduce the number of applications that are exposed to an attacker. **[12%]**

2. Most firewalls today are *stateful*, otherwise known as *connection tracking*.

   (a) Describe how a stateful firewall handles TCP connections. What protection does this offer to the machines inside the firewall? **[6%]**

   (b) Describe how a stateful firewall processes outgoing UDP packets (for example, DNS queries) to permit replies to be received? **[6%]**

   (c) You become aware of an attempted denial of service attack on a network you control. It appears that machines are struggling to deal with a large number of incomplete TCP connection requests. Without suggesting changes to the machines behind the firewall, explain how a stateful firewall can reduce the effect of this attack. **[8%]**

3. An *intrusion detection systems* (IDS) examines network activity and attempts to identify attacks. An *intrusion prevention system* (IPS) takes active counter-measures when such an attack is detected.

   (a) Although IDSes can be installed in-line with traffic, they are more commonly fed a copy of the traffic on a network via a *mirror port* on an ethernet switch. What problem does this cause if there is a requirement to upgrade an IDS to act as an IPS? How can this problem be overcome? **[6%]**

   (b) List two attacks that an IDS based on using attack signatures might detect, and two attacks which it cannot detect. Briefly explain your choices. **[8%]**

   (c) IDS detection is not totally accurate, and can both over- and under-report issues. Briefly describe the problems that each can cause. **[6%]**

4. The WEP (*Wired Equivalent Privacy*) protocol proved to be extremely insecure, in part because of the problems of generating initialisation vectors. Similar problems arise with the generation of key material in other contexts.

   (a) Explain why it is difficult to generate random numbers on typical networking hardware and other embedded systems. **[6%]**

   (b) WEP was replaced with WPA2 (the second version of *Wireless Protected Access*. WPA2 is available in two versions, "Personal" (also known as "PSK") and "Enterprise". How do these differ from the perspective of a user needing to connect a computer to the network? **[4%]**?

(c) An organisation with about one hundred users is using WPA2-Personal. You can been asked to advise them on wireless security. Give two advantages of moving to WPA2-Enterprise. Explain the possible additional costs, both in terms of equipment and operational complexity, of moving to WPA2-Enterprise. **[10%]**

5. A *virtual private network* (VPN) can be used to connect a remote user to a corporate network.

   (a) VPNs are often secured with *one time passwords* generated by some sort of hardware token. Outline how these one-time passwords are generated and checked. **[6%]**

   (b) Suggest three reasons why a VPN is preferable to granting access to individual services. **[6%]**

   (c) Sketch an *attack tree* showing how an attacker might attempt to break into a VPN service. **[8%]**