A28438 No calculator permitted in this examination

THE UNIVERSITY OF BIRMINGHAM

THIS PAGE TO BE REPLACED BY OFFICE

06 23900

Network Security

RESIT

September 2015 1 hour 30 minutes

[Answer ALL questions]

Turn Over

1. WEP, WPA and WPA2 are protocols used to secure wireless networks.

   (a) WPA2 comes in two versions, one aimed at small networks, one aimed at larger networks. Name the two versions and explain the difference between them. **[6%]**

   (b) An optional part of WPA2 is the WPS mechanism for associating consumer devices with a network. It is very weak, because of its method for verifying PINs. Explain the weakness, and why it reduces the security to approximately the square root of the intended level. **[8%]**

2. Intrusion detection systems can be used at the edge of a network where it joins the internet, or on internal links.

   (a) Suggest two advantages of using an IDS on internal links, where they can observe some or all internal traffic. **[4%]**

   (b) Suggest two problems likely to be caused by running an IDS on a busy internal network. **[5%]**

   (c) When an IDS is placed at the edge of a network, It could be located in front of (where it is not protected by) a firewall, or behind (where it is protected by) a firewall. Discuss the merits of both locations, outlining the different information the two placements would provide. **[10%]**

3. TLS and SSL are related technologies which encrypt data in transit over the Internet.

   (a) Define a man in the middle attack against an encrypted connection. **[3%]**

   (b) Describe the use of server certificates in TLS connections and how they provide protection against man in the middle attacks. **[6%]**

   (c) Explain why an attacker who is able to force a certificate authority to issue certificates for chosen domains can in many cases still perform a man in the middle attack. **[8%]**

   (d) Explain two countermeasures that browser vendors have implemented that reduce this risk. **[8%]**

4. IPSec is a set of protocols that perform encryption and other security tasks on IP packets.

   (a) Explain the difference between AH and ESP in the context of IPSec. **[4%]**

   (b) IPSec can operate in "transport" or "tunnel" mode. Explain the difference, and outline two scenarios, one for each mode, where the modes would be used. **[6%]**

   (c) IPSec can be statically or automatically keyed. Explain the difference between the two techniques for key management. **[4%]**

   (d) Why might a network designer with very high security requirements opt for static keying? **[6%]**

5. An amplification attack is one in which an attacker is able to use a third party to send more traffic to a victim than the attacker themselves sends.

   (a) Explain the feature in UDP which make protocols operating over UDP prone to this problem. **[6%]**

   (b) Suggest measures that a network designer might take to reduce the chances of their network being used as the innocent third party in an amplification attack. **[4%]**

   (c) Suggest measures that a network designer might take to reduce the chances of their network being used by an attacker to launch an amplification attack. **[4%]**

   (d) Suggest measures that protocol designers chould take to reduce the risk that their protocol is used in such an attack. **[8%]**