A28438 No calculator permitted in this examination

THE UNIVERSITY OF BIRMINGHAM

THIS PAGE TO BE REPLACED BY OFFICE

06 23900

Network Security

RESIT

September 2016 1 hour 30 minutes

[Answer ALL questions]

Turn Over

1. WEP, WPA and WPA2 are protocols used to encrypt wireless networks. You are managing a network which is using "WPA2-PSK".

   (a) Name two advantages you would get from switching to using the "WPA2-Enterprise" mechanism. **[6%]**

   (b) What additional resources would you need in order to deploy this version of WPA2? **[4%]**

   (c) WEP is notoriously weak, in part because of its poor choice of initialisation vectors for encryption. Why are encryption protocols that depend on random IVs problematic on devices such as wireless access points? How might this problem be reduced or mitigated? **[6%]**

2. Network proxies can be used at the edge of a network, as part of an overall security solution.

   (a) Distinguish between "inbound" and "outbound" proxies. Explain a practical use for each case. **[8%]**

   (b) Proxies are particularly beneficial when protecting older, less familiar or otherwise non-mainstream resources. Explain how a proxy offers security benefits to an elderly system which is no longer maintained, but which needs still to be connected to the Internet. **[6%]**

   (c) Proxies can provide additional functionality to operate as data diodes, which enforce the flow of information in only one direction. Outline why a data diode might be required, and how a proxy architecture could be extended so as to function in this manner. **[10%]**

3. TLS and SSL are related technologies which encrypt data in transit over the Internet. For our purposes we refer to both as TLS.

   (a) TLS uses certificates, with their associated private keys, to help generate and secure session keys. What is a session key? **[2%]**

   (b) In one popular mode of operation, TLS uses the RSA algorithm to establish a session key. Outline how it does this. **[6%]**

   (c) In the context of TLS, define "forward secrecy" and explain why the use of RSA makes forward secrecy impossible. **[6%]**

   (d) Explain the use that can be made by an attacker of a certificate for `www.google.com` signed by a certificate authority trusted by a client and to which the attacker knows the private key. **[6%]**

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

(a) IPSec is commonly used in conjunction with L2TP. Why is this easier for building VPNs than the use of IPSec alone? **[4%]**

(b) IPSec offers IKE, a protocol for agreeing session keys between participants. What mechanisms can it use to secure the exchange? **[4%]**

(c) IPSec is sometimes used between proxies and the resources they are proxying for, even when the machines are located in the same building. Why might this be done? **[6%]**

(d) IPSec can be used in ESP and AH modes. AH does not encrypt the traffic: describe a scenario when this might be useful. **[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) Amplification attacks do not just increase the volume, they also conceal the attacker's identity. Why? **[6%]**

(b) Amplification attacks are often associated with the DNS protocol. What precautions should be used on recursive nameservers to avoid their involvement in amplification attacks? **[6%]**

(c) TCP is much less prone to amplification attacks than UDP. Explain why, and explain the role of sequence numbers. **[8%]**