Two hours

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Computer and Network Security

Date: Friday 21st January 2011
Time: 14:00 - 16:00

Please answer any THREE questions from the FIVE questions provided

For full marks your answers should be concise as well as accurate.
Marks will be awarded for reasoning and method as well as being correct.

This is a CLOSED book examination
The use of electronic calculators is NOT permitted
1. A firewall is a perimeter defence mechanism commonly used to protect a private network against external attacks. Answer the following questions.

   a) Outline two functions (i.e. protections) a firewall can provide and three limitations in the use of a firewall to protect a private network against security attacks in general. (5 marks)

   b) Describe and contrast the working mechanisms of the following three types of firewalls:
      (i) stateless packet filtering firewall,
      (ii) stateful packet filtering firewall, and
      (iii) application-level proxy firewall. (6 marks)

   c) Describe what a Smurf attack is, and explain how a firewall can be used to protect against this attack (i.e. what filtering rule(s) may be used to counter this attack). (4 marks)

   d) Explain how to use IP Fragmentation to launch a DoS attack on a host and how a firewall may be used to counter this attack. (5 marks)
2. Bob’s company has a distributed set of services interconnected by a communication network. The access to these services should be controlled by an authentication service run on an Authentication Server. There are two proposed solutions for this authentication service. One is to use the AuthN protocol designed by a company employee (as detailed in the table below). The other is to use the Kerberos authentication system. Answer the following questions.

<table>
<thead>
<tr>
<th>Notation:</th>
<th>The AuthN Protocol:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• $C$ = Client/User</td>
<td>(1) $C \rightarrow AS$: $ID_c</td>
</tr>
<tr>
<td>• $AS$ = Authentication Server</td>
<td>(2) $AS \rightarrow C$: Ticket</td>
</tr>
<tr>
<td>• $V$ = Service Server</td>
<td>(3) $C \rightarrow V$: $ID_c</td>
</tr>
<tr>
<td>• $ID_c$ = Identity of $C$</td>
<td>$Ticket = E_{K_v}[ID_c</td>
</tr>
<tr>
<td>• $ID_v$ = Identity of $V$</td>
<td></td>
</tr>
<tr>
<td>• $P_c$ = $C$’s password</td>
<td></td>
</tr>
<tr>
<td>• $K_v$ = Secret (symmetric key) shared between AS and V</td>
<td></td>
</tr>
<tr>
<td>• $TS$ = timestamp</td>
<td></td>
</tr>
<tr>
<td>• $</td>
<td></td>
</tr>
<tr>
<td>• $E_{K_v}$ = Encryption using key $K_v$</td>
<td></td>
</tr>
</tbody>
</table>

a) The AuthN Protocol says: to access the service running on server $V$, the user/client, $C$, should first authenticate herself to $AS$ using her password, $P_c$. Upon successful authentication, $AS$ sends $C$ a ticket (in message (2)), so that $C$ could use this ticket to access the service on $V$ (message (3)). Identify five security flaws in this protocol. (5 marks)

b) Describe Kerberos v4 (version 4) protocol. (5 marks)

c) Describe the role of the authenticator used in the Kerberos protocol, and explain why an authenticator is NOT required when a client requests a ticket-granting ticket from an authentication server. (4 marks)

d) To support business expansion, Bob’s company may need to reorganise his IT services into two realms, $A$ and $B$. Extend the Kerberos v4 protocol to allow a client $C$ in a realm $A$ to access a service in realm $B$. You should clearly describe your protocol extension and explain why your extended protocol could support this controlled access of services provided by another realm. (6 marks)
3. IEEE802.11 is a standard for WLANs (Wireless Local Area Networks). ABC Solicitors Ltd has already got a wired network in the building, and now the company has decided to install an IEEE802.11 hub to support service access by mobile users. This wireless LAN facility is to be integrated with the existing wired network. Answer the following questions.

a) Identify three security threats that could be introduced as the result of this wireless network installation and integration, and outline security services that are necessary to counter each of the threats you identify. (6 marks)

b) Describe key features of the IEEE802.1x authentication standard, and outline the benefits of having these key features. (4 marks)

c) Wired Equivalent Privacy (WEP) is the original IEEE802.11 Security proposal, whereas WAP2 (Wireless Protected Access) is the full implementation of IEEE 802.11i proposal (which is the WLAN Security Standard).

(i) Name four security services that are specified in IEEE802.11i. (4 marks)

(ii) Use a table to contrast the two security proposals (WEP and WAP2) in terms of key size, key management method, and security services that they each support. You should also indicate (where appropriate) how the security services are provided in these proposals. (6 marks)

4. IPSec (Internet Protocol Security) is a network layer security solution, whereas SSL (Secure Socket Layer) is a transport layer security solution. Answer the following questions.

a) IPSec defines a concept of a Security Association (SA). What is an SA? With the help of a diagram, explain how an SA is negotiated. In your explanation, you should also make clear what an SA negotiation process accomplishes. (5 marks)

b) What protocols does SSL comprise? Outline the functions or services provided by EACH of the SSL protocols. (8 marks)

c) Outline SSL Record Protocol outbound (i.e. data transfer) and inbound (i.e. data reception) data processing operations and compare them with IPSec ESP (Encapsulating Security Payload) outbound and inbound packet processing operations. What major observation(s) can you make from this comparison? (7 marks)
5. A personal health monitor worn by a patient transmits collected health data through wireless communication to a software system $P$ running on a trusted network host in the vicinity of the patient’s location, to produce the patient’s health monitoring reports. Another software system $G$ operating on a networked computer or a mobile device such as PDA (Personal Digital Assistant) used by the patient’s GP (or doctor) can request the latest health monitoring report from the patient’s system $P$ to allow the GP to check the report and take necessary actions when needed.

- a) Identify two security threats to the communications between the two software systems $P$ and $G$ mentioned above, and explain the consequences that could be caused by each of the identified threats. (6 marks)

- b) Design an efficient communication protocol to allow only system $G$ to request and read the patient’s health monitoring reports from system $P$ with the assurance of confidentiality, authenticity and integrity, where both symmetric and asymmetric (or public-key) cryptosystems including secure hash functions are available for the protocol design. State any assumptions you use for the design, and explain how the designed protocol operates. (10 marks)

- c) Explain how the protocol produced in (b) can prevent each of the two security threats identified in (a). (4 marks)