Two hours

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Computer Network Security

Date:  Friday 28th 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. BobVideo Ltd, an online video vendor, sells video programmes on the Internet. Customers can purchase video programmes using their credit cards or electronic cash. As customers are increasingly worrying about the security of the Internet due to numerous security incidents, the company has decided to enhance the security of its online services. To achieve secure communications, BobVideo plans to require each customer, say Carol, to register a RSA public key (say $KU_c$) with the company, to inform the customer of the company’s public key (e.g. $KU_b$), and to provide the customer with symmetric and asymmetric cryptosystems and secure hash functions freely.

a) Suggest the most efficient method for BobVideo to send a video programme to the consumer with the assurance of message secrecy (i.e. confidentiality), integrity, authenticity, and freshness. Justify your suggestion. (6 marks)

b) You are given two large primes, $p$ and $q$.

   (i) Explain how the consumer’s RSA public and private keys (i.e. $KU_c$ and $KR_c$) are generated, and give the equations. (4 marks)

   (ii) Explain how a RSA digital signature is generated and verified. Give the necessary equations using the prime numbers given. (2 marks)

c) Design a digital signature protocol using symmetric encryption and an arbiter, but do not expose the content of the message to be signed to the arbiter (in other words, you should NOT use any public-key cryptosystem to design this protocol). You can assume that the two parties (say Carol and Bob) engaging in a communication have a shared symmetric key, and that each of the two parties also has a shared symmetric key with the arbiter. (4 marks)

d) Contrast the signature scheme in question c) with the RSA based signature scheme in question b) in terms of their respective strengths and limitations. (4 marks)
2. Client-server authentication can be achieved by using any one of the following three types of authentication methods: password based authentication, symmetric key based authentication and X.509 certificate-based authentication. Answer the following questions.

   a) The password based authentication method is particularly vulnerable to off-line password guessing attacks. Name and explain two methods by which off-line password guessing attacks are performed, and describe two countermeasures taken by the UNIX authentication system to thwart such attacks. (6 marks)

   b) Explain how a symmetric key based authentication method may be implemented using smart cards. Name two benefits for using the smart card based authentication solution. (4 marks)

   c) Design a X.509 certificate-based authentication method to support mutual authentication between a client and a server. (4 marks)

   d) Is PKI (Public Key Infrastructure) necessary to support certificate-based authentication? Justify your answer by (i) explaining what PKI is for, and (ii) by outlining main PKI functions. (6 marks)

3. Wired Equivalent Privacy (WEP) is the original 802.11 security proposal, whereas WAP2 (Wireless Protected Access) is the full implementation of IEEE 802.11i proposal (which is the WLAN Security Standard). IEEE 802.11i uses AES (Advanced Encryption Standard) based CCM (Counter-Mode/Cipher-Block-Chaining Message-Authentication-Code) protocol to achieve message confidentiality and integrity. Answer the following questions.

   a) Name three main weaknesses of WEP, and explain what measures are taken in the design of WAP2 to overcome these weaknesses. (6 marks)

   b) Use block diagrams to illustrate how a message is encrypted and decrypted using AES (Advanced Encryption Standard) Counter Mode and outline two main advantages of this mode of operation. (6 marks)

   c) Use a block diagram to illustrate how a Cipher-Block-Chaining Message-Authentication-Code (CBC-MAC) is generated and also explain how such a Message-Authentication-Code (MAC) is verified. (4 marks)

   d) What are the key features of the 802.1x Authentication Standard? What advantages do these key features bring? (4 marks)
4. IPsec is a network level security solution, whereas SSL is a transport level security solution. Answer the following questions.

a) What protocols does SSL comprise? Outline the functions or services provided by EACH of the SSL protocols.  

b) Outline SSL Record Protocol outbound (i.e. data transfer) and inbound (i.e. data reception) data processing operations and contrast them with IPSec ESP outbound and inbound packet processing operations.

(8 marks)

6 marks)

(6 marks)

(2 marks)

(4 marks)

(ii) Contrast these three key exchange methods, i.e. Fixed DH (Diffie-Hellman), Ephemeral DH, and Anonymous DH.
5. The following gives a credit card based e-payment protocol:

<table>
<thead>
<tr>
<th>Initiation</th>
<th>$C$</th>
<th>$M$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purchase request</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Invoice</th>
<th>$C$</th>
<th>$M$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purchase details including prices</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Payment</th>
<th>$C$</th>
<th>$M$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E(pk_A, Slip)$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authorisation request</th>
<th>$M$</th>
<th>$A$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purchase details, $E(pk_A, Slip)$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authorisation response</th>
<th>$M$</th>
<th>$A$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Sig(sk_A, C</td>
<td></td>
<td>M</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Confirmation</th>
<th>$C$</th>
<th>$M$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Sig(sk_A, C</td>
<td></td>
<td>M</td>
</tr>
</tbody>
</table>

Here, $C$, $M$, and $A$ represent a customer, a merchant, and an acquirer (i.e. the merchant's bank), respectively. $pk_A$ and $sk_A$ are $A$’s public and private keys, $E(pk, x)$ denotes the encryption of $x$ with key $pk$, $Sig(sk, x)$ denotes $x$ signed with key $sk$ (i.e. $Sig(sk, x) = x \parallel E(sk, H(x))$), $H(x)$ is cryptographic hash function, $x\parallel y$ is the concatenation of data items $x$ and $y$, and $Slip = \{\text{the description of goods to purchase, prices to pay, } C\text{'s credit card number}\}$, $Decision = \text{yes or no}$.

a) Discuss in general terms two security threats to credit card based electronic payment.
   (4 marks)

b) Discuss whether or not the above protocol can prevent each of the two security threats described in 5 (a).
   (6 marks)

c) Customer $C$ wants to purchase electronic goods from merchant $M$, and wishes to have a fair trade in the sense that either $C$ receives the goods and $M$ receives the payment, or neither of them gets anything from the other. Extend the above protocol to achieve this fair trade, stating any assumptions you make, and justify how the extended protocol can achieve the fairness.
   (10 marks)