A28437

Calculators may be used in this examination but must not be used to store text. Calculators with the ability to store text should have their memories deleted prior to the start of the examination.

UNIVERSITY OF
BIRMINGHAM

School of Computer Science

First Year – MSc in Computer Science
First Year – MSc in Advanced Computer Science
First Year – Computer Security
Fifth Year – MEng Electronic and Software Engineering

06 23899

Computer Security

Summer Examinations 2013

Time Allowed: 1.30 hours

[Answer 3 out of 4 Questions]

[Marks add up to 99%, an additional 1% will be added to your mark if you do not try to answer 4 Questions]

TURN OVER

1. Block ciphers, such as AES, can be used in a range of modes of operation. Some of the most popular are Electronic codebook mode (ECB), Cipher-block chaining mode (CBC) and Counter mode (CTR).

   (a) Describe how each of these modes of operation work (you may find it helpful to draw diagrams to illustrate your answers).

   [9%]

   (b) Explain why Cipher-block chaining mode (CBC) is more secure than Electronic codebook mode (ECB). **[2%]**

   (c) Give two advantages that Counter mode (CTR) has over Cipher-block chaining mode (CBC).

   [4%]

   A security researcher proposes a new mode of operation that works as follows: Given a plain text $P_1, P_2, \ldots, P_n$ it produces a cipher text $C_1, C_2, \ldots, C_n$ by encrypting the first block, $C_1 = E_K(P_1)$ then the following plain test blocks are xored with the previous plain text block before encryption: $C_{n+1} = E_K(P_{n+1} \oplus P_n)$

   (d) How would you decrypt a cipher text $(C_1, C_2, \ldots, C_n\ )$ encrypted with this mode of operation (give your answer as equations using D_K, C_i, P_i and $\oplus$).

   [4%]

   (e) Packet loss affects this new mode of operation more than other modes. Explain why.

   [4%]

   (f) How would you rate the security of this new mode of operation as compared to Counter mode (CTR) and Cipher-block chaining mode (CBC).

   [10%]

2. (a) ISO 27001 and PCI-DSS are two of the most common security standards. Describe the differences between them, and why a company might choose to implement these standards.

[5%]

(b) Imagine that you are carrying out an ISO 27001 style risk assessment for a small company that sells clothes on the Internet. Describe two of the most important assets that you might consider as part of a ISO 27001 audit.

[2%]

(c) Describe a different threat for each of these assets.

[2%]

(d) For each threat, describe a vulnerability that the small company's computer system or organisation might have that makes it more likely that the threat will cause harm.

[4%]

(e) For each of the two assets/threats pairs you have give, say how likely you think each is, what the impact of the threat would be to the company and what you believe the overall risk is.

[6%]

(f) Say how the two risks should be treated. Make it clear in your answer if you are suggesting the risks should be avoided, mitigated, transferred or accepted.

[8%]

(g) Give two examples of risks to the company that could still remain even if the company did correctly comply with both ISO 27001 and PCI-DSS.

[6%]

3. (a) Key establishment protocols are used when two parties (in this case Alice and Bob) want to agree on a new session key. In the following protocol Alice and Bob already have shared, symmetric keys with a **trusted** server S (K_{AS} & K_{BS}). Alice and Bob can then run the following protocol to set up a session key K_{AB}:

1. $A \rightarrow S: \quad A, \{B\}_{K_{AS}}$
2. $S \rightarrow A: \quad \{B, K_{AB}, \{K_{AB}\}_{K_{BS}}\}_{K_{AS}}$
3. $A \rightarrow B: \quad A, \{K_{AB}\}_{K_{BS}}$

Alice sends a message to the trusted server that includes her name and Bob's name encrypted with the key she shares with the server. The server generates a new key for Alice and Bob (K_{AB}) and sends this to Alice, along with Bob's name and a packet to forward to Bob. Alice then forwards this packet to Bob and Bob can decrypt it and learn the new session key.

We assume that the server S is completely trustworthy, but may run the same protocol with many other parties as well as Alice and Bob. We also assume Alice and Bob will not give away their keys. An attacker can observe many runs of the protocol, interact with Alice, Bob and the Server, interrupting and replaying messages. However we also assume that the encrypted messages cannot be broken and the message contents cannot be altered.

Say if the following properties hold:

i) Can Alice and Bob be sure that the key K_{AB} was generated by the trusted server? Give a brief justification of your answer. **[3%]**

ii) Can Alice and Bob be sure that the key K_{AB} was a new, fresh key? Give a brief justification of your answer. **[3%]**

iii) Can Alice be sure that she is sharing the key with no one other than Bob? Give a brief justification of your answer. **[3%]**

iv) Can Bob be sure that he is sharing the key with no one other than Alice? Give a brief justification of your answer. **[3%]**

(b) Next we consider an improved version of the protocol that runs as follows:

1. $A \rightarrow S: \quad A, \{B, N\}_{K_{AS}}$
2. $S \rightarrow A: \quad \{B, N, K_{AB}, \{K_{AB}, A\}_{K_{BS}}\}_{K_{AS}}$
3. $A \rightarrow B: \quad A, \{K_{AB}, A\}_{K_{BS}}$

N is a nonce generated randomly by Alice every time she runs the protocol. Alice checks that the N in message 2 is the same as the nonce she sent out in message 1, and if it is not she aborts the protocol. The server also adds Alice's name into the packet for Bob.

For this version of the protocol, say if the following properties hold:

i) Can Alice and Bob be sure that the key K_{AB} was generated by the trusted server? Give a brief justification of your answer. **[3%]**

ii) Can Alice be sure that the key K_{AB} is a new, fresh key? Give a brief justification of your answer. **[3%]**

iii) Can Bob be sure that the key K_{AB} is a new, fresh key? Give a brief justification of your answer. **[3%]**

iv) Can Alice be sure that she is sharing the key with no one other than Bob? Give a brief justification of your answer. **[3%]**

v) Can Bob be sure that he is sharing the key with no one other than Alice? Give a brief justification of your answer. **[3%]**

Hint: at least one of these properties doesn't hold

(c) Design an improved version of the protocol given in Question b that would ensure that all the properties requested in Question b hold.

[6%]

4. Common methods by which a computer become infected with malware include "Drive-by-dowload" attacks and "Trojan" attacks.

(a) i) Describe how "Drive-by-dowload" attacks can infect a computer and what vulnerabilities are necessary to enable them to happen. **[5%]**

ii) Describe how "Trojan" attacks can infect a computer and what vulnerabilities are necessary to enable them to happen. **[5%]**

(b) Malware will commonly turn a computer into a bot, which will operate as part of a botnet. Give three examples of what a botnet might be used for, and describe how each of these examples can make money for the botnet operator. **[9%]**

(c) Compare and contrast the different methods that might be used to stop a botnet from functioning. **[14%]**