OLLSCOIL NA hÉIREANN
THE NATIONAL UNIVERSITY OF IRELAND, CORK

COLÁISTE NA hOLLSCOILE, CORCAIGH
UNIVERSITY COLLEGE, CORK

SUMMER EXAMINATION 2014

CS4614: Introductory Network Security

Professor I. Gent,
Professor B. O'Sullivan,
Dr. S.N. Foley

Answer *all* questions
Maximum marks: 80

1.5 Hours
(Note 80 marks/90 minutes = 1.125 minutes per mark)

PLEASE DO NOT TURN THIS PAGE UNTIL INSTRUCTED TO DO SO

ENSURE THAT YOU HAVE THE CORRECT EXAM PAPER

1. a) Define the properties of a one-way hash function. *(6 marks)*

b) Following an intrusion at Adobe (October 2013), attackers gained access to a user password file. It is believed that each password p was stored in encrypted form in the file as $E^{ecb}_{des}(K_A, p)$ using triple DES (ECB mode) where K_A is a secret Adobe master key. Describe two security weaknesses of this scheme. *(6 marks)*

c) Continuing Question 1(b), describe how the passwords should have been stored and explain how your scheme defends against a pre-computation dictionary attack. *(6 marks)*

d) The following Java code generates a symmetric cipher based on a random session key.

```
KeyGenerator kg= KeyGenerator.getInstance("DES");
kg.init(new Random(0));
SecretKey key= kg.generateKey();
Cipher cipher= Cipher.getInstance("DES/ECB/PKCS5Padding");
cipher.init(Cipher.ENCRYPT_MODE,key);
```

Give a Java code fragment that encrypts the contents of a file using this key. *(6 marks)*

e) Identify and explain any security vulnerabilities in the code in Question 1(d) above. *(6 marks)*

(30 Total marks)

---

2. Consider the following Needham-Schroeder style authentication protocol, whereby initiator A asks Authentication Server T for a session key K_{AB} that it can use with service B.

$$\begin{array}{lll} \text{Msg1} & A \rightarrow T: & A, B, N_A \\ \text{Msg2} & T \rightarrow A: & \{N_A, B, K_{AB}, \{K_{AB}\}_{K_{BT}}\}_{K_{AT}} \\ \text{Msg3} & A \rightarrow B: & A, \{K_{AB}\}_{K_{BT}} \end{array}$$

Principals A and B share long-term secret keys K_{AT} and K_{BT} with server T, respectively; N_A is a nonce, and $\{\ldots\}_K$ denotes symmetric key encryption with secret key K.

a) Describe an attack on the protocol whereby Eve can masquerade as A to B. *(10 marks)*

b) Revise the protocol so that: it eliminates the vulnerability in Question 2(a); provides mutual authentication between A and B, and supports key revocation in the event that K_{AT} is compromised. *(10 marks)*

c) Alice logs into the workstation corresponding to Principal A and K_{AT} is determined by her password. Alice does not want to give her password every time she uses the protocol to request services, however, she is concerned about the workstation storing long-term key K_{AT} for the duration of her login session. Describe how the protocol can be revised to provide single-sign-on for Alice while addressing her password security concerns. *(5 marks)*

(25 Total marks)

Continued on next page

3. The following SSL-style protocol fragment establishes a secure connection between browser B and web-server A:

$$\begin{aligned} \text{Msg 1:} \quad & B \rightarrow A \quad : \{B, K_{ab}, N_A\}_{K_A} \\ \text{Msg 2:} \quad & A \rightarrow B \quad : \{N_B + 1\}_{K_{ab}} \end{aligned}$$

where K_A is the public key owned by A, K_{ab} is a symmetric session key proposed by A and N_B is a nonce. In Protocol Msg 1, $\{\ldots\}_{K_A}$ denotes public key encryption, while $\{\ldots\}_{K_{ab}}$ denotes symmetric key encryption in Protocol Msg 2.

a) Explain how the protocol should be extended to support public key certificates. Your answer should include a revision of the protocol, description of certificate(s) content and how it is used by the browser/web-server. *(10 marks)*

b) The protocol assumes that B is competent to generate a good session key K_{ab}. Give an example of why this might not be the case. Revise the protocol so it uses a Diffie-Hellman key exchange to establish the session key K_{ab}. *(10 marks)*

c) Apple iOS comes with a pre-installed trusted Certification Authority (CA) certificate from a foreign military agency. Describe how this agency might spy on a user's secure (HTTPS) web browsing. *(5 marks)*

(25 Total marks)

PLEASE DO NOT TURN THIS PAGE UNTIL INSTRUCTED TO DO SO.

THEN ENSURE THAT YOU HAVE THE CORRECT PAPER.