COMP 61421

Two hours

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Cyber Security

Date: Monday 14th January 2019

Time: 14:00 - 16:00

Please answer all THREE Questions

Each question is worth 20 marks

This is a CLOSED book examination

The use of electronic calculators is NOT permitted

[PTO]

1. SSL (Secure Sockets Layer) is commonly used for establishing a secure link between a web server and a web browser. Answer the following questions.

   a) What protocols does SSL comprise and what they are each used for? (8 marks)

   b) Name all the security properties that SSL supports. (4 marks)

   c) For each of the properties you have named in b), describe *how* the property is achieved in SSL. (8 marks)

2. An access control system includes the functions of authentication and authorisation. Answer the following questions.

   a) What does the authentication function accomplish? Propose three different methods of implementing the authentication function in a networked environment. Highlight any major differences among the three authentication methods you propose and name an application scenario or environment for which each method is most suited to. (10 marks)

   b) Use a diagram to illustrate the functional components of an access control system and explain how these components inter-work to accomplish the task of access control. In your explanation, you should make clear the names of the functional components, the sequence of operations undertaken by the access control system when serving an access request, and the functions the access control system provides and how the functions are provided. (7 marks)

   b) *Enforce Least Privilege* is a security goal one should achieve when designing an access control system. Explain what it means and why it is necessary. (3 marks)

[Please Turn Over]

3. There are *n* client nodes and a Server in a network. Every client node in the network needs to have *private and confidential* communication with every other client node in the network. In other words, for each communication session between a pair of client nodes in the network, a secret session key (i.e. a symmetric key valid for one communication session only) is required. It is assumed that *n* is large and there is no prior shared secret between any two of the client nodes. Answer the following questions.

   a) Design an *efficient* session key establishment protocol for any pair of the client nodes, e.g. A and B, to establish a secret *session* key *without* any assistance of a public-key cryptosystem. Your protocol should be able to thwart any security attacks on the protocol, and it should also be efficient in that the number of required protocol messages is minimal. Clearly state any assumptions that you use in your design. (8 marks)

   b) Identify any threats or attacks that may be mounted to the session key establishment process, and highlight any measure you have taken in your design in a) to thwart the threats or attacks. (6 marks)

   c) Name any factors that may affect the security of the protocol you have designed in a). (6 marks)

END OF EXAMINATION