COMP 38411

Two hours

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Cryptography and Network Security

Date: Tuesday 22nd January 2019

Time: 14:00 - 16:00

Please answer all THREE Questions.

© The University of Manchester, 2019

This is a CLOSED book examination

The use of electronic calculators is NOT permitted

[PTO]

1. In many distributed systems, users are identified and authenticated by using a username/password based authentication service. Challenge-response is a commonly used approach to authentication protocol design for this service. Answer the following questions.

   a) What is the benefit of using the challenge-response approach? (2 marks)

   b) There are multiple ways of implementing the challenge-response approach. Describe *three* different implementations of this approach by designing *three* password-based challenge-response authentication protocols that allow an authentication server, *AS*, to authenticate a remote user, *U*. For each designed protocol, you should clearly explain what is in the Challenge, what is in the Response and how the Response is verified. You should also make clear any assumptions if they are used in your design. (12 marks)

   c) Contrast the three protocols you have designed by discussing their respective strengths, weaknesses and/or limitations. Also identify any factors that may impact on the security of your designed protocols. (6 marks)

2. Ensuring the security of messages in-transit is one of the most important security requirements in a networked environment, such as the Internet. Answer the following questions.

   a) Name and explain *four* security properties for ensuring the security of messages in-transit. (4 marks)

   b) Describe three message authentication methods. In your description, you should give any equations or diagrams used and clearly explain how authentication token is generated and how it is verified. Highlight their respective strengths, weaknesses and/or limitations. Also for each method, identify an application area it is most suited to. (12 marks)

   c) Name and explain all the properties a hash function should have for it to be cryptographically secure and of practical application in providing message security. (4 marks)

3. IPSec is a security framework for providing security at the IP (Internet Protocol) layer.

   a) Explain why a Security Association (SA) is needed, and with the help of a diagram, show how an SA is established between two parties. (8 marks)

   b) The process of establishing a shared secret key between two remote entities is particularly vulnerable to a Man-in-the-Middle (MitM) attack. Describe how an MitM attack may be mounted during the process when a shared secret key is being established between two remote entities, and propose a countermeasure to thwart the attack. (6 marks)

   c) List the major security services provided by AH (Authentication Header) and ESP (Encapsulating Security Payload), respectively. Use an example to explain why the security services provided by the two protocols (i.e. AH and ESP) may need to be combined to protect a data flow, and describe how to combine the services in your example. (6 marks)

END OF EXAMINATION