SWINBURNE UNIVERSITY OF TECHNOLOGY

TNE20003 – Internet and Cybersecurity for Engineering Applications

Cybersecurity

Aims:

To improve you understanding of Access control, VPNs & Cryptography

Preparation:

View “Cybersecurity”

Due Date:

Nil. In-class activity.

AAA: Authentication - Authorization - Accounting

SWINBURNE UNIVERSITY OF TECHNOLOGY

Using the lecture notes and pre-recordings of lecture 10 please answer the following questions

Question 1

What is the difference between authentication and authorization?

authentication: to confirm the identity of a user

authorization: determinr what resources or actions an authenticated user is allowed to access

Question 2

What is the correct order for the steps (authorization, identification and authentication) in gaining access control to a resource?

identification -> authentication -> authorization

Question 3

Under multi-factor authentication how would you describe the list items under the heading "Something someone has"?

Security token, smart card, access card, etc.

Question 4

What is the challenge response process and when is it used?

The challenge-response process is an authentication method where a server sends a unique challenge, and the user provides a calculated response based on a secret (like a password or key). It prevents replay attacks and is commonly used in systems requiring enhanced security, such as password authentication and two-factor authentication.

Question 5

What is the difference between IDS and IPS?

IDS: only identify and alert
IPS: prevent

Question 6

It is good cryptographic practice to never store a password in plain text. Usually the hash of the password (along with additional information called “salt”) is stored rather than the password. Why is this more secure than storing a password in plain text?

Question 7

Hash functions combine multiple rounds of modulo arithmetic with logical operations to convert a variable length input into a fixed length hash value. Modulo arithmetic is very difficult to reverse. Consider a simple hash function F(X) = 5 X mod 9. What is the smallest value of X which would produce an output of 7?

Question 8

Consider a simple challenge-response mechanism used for authentication. To calculate the response to the challenge, the key is added to the challenge and the hash is calculated. The hash is then returned as the response to the challenge.

The hash function is F(X) = 5 X mod 9. Each party has a shared secret key of 15. The challenge is an integer between 10 and 20.

What will be the response to a challenge of 11?

Question 9

Bob wishes to send a message to Alice. He wants to encrypt it and digitally sign it using public key encryption.

a. Which key will Bob use to encrypt the message?

b. Which key will Bob use to sign the message?

c. Which key will Alice use to decrypt the message?

d. Which key will Alice use to validate the digital signature?