CSC 438/539 Systems and Software Security

Instructor: Dr. Natarajan Meghanathan

Spring 2014

Question Bank for Module 8 – Secure Software Development Lifecycle – Requirements and Design Principles

1) Draw the diagram for the Secure SDLC and identify the different stages. Also indicate the additional stages that need to be implement post-software development.

2) Draw a use case/misuse case diagram for the design of a secure communication channel (involving cryptography and steganography). Show how steganography can complement cryptography. Use the following relation types wherever appropriate: *includes*, *extends*, *threaten* and *mitigate* relation types.

3) Draw a use case/misuse case diagram for the design of a web forum that is resistant to any XSS attacks. Use the following relation types wherever appropriate: *includes*, *extends*, *threaten* and *mitigate* relation types.

4) Briefly state/explain the security requirement for each of the following application scenarios:
   (i) Application stores sensitive information that must be protected for HIPAA compliance

   (ii) The application transmits sensitive user information across potentially untrusted or unsecured networks

   (iii) The application must remain available to legitimate users

   (iv) The application supports multiple users with different levels of privilege.

(v) The application is written in C or C++.

(vi) The application uses cryptography

(vii) The application opens files that are typically exchanged over untrusted links such as a media file over the Internet

(viii) The system needs to keep track of individual users and authentication must be enforced

5) What is an "Attack Surface" in the context of secure software design? Explain its significance and how is it related to accessibility of the system.

6) Explain the relation between attack surface, code quality and the risk associated with software?

7) Between UDP and TCP, which transport layer protocol provides a smaller attack surface and why? Justify your answer.

8) Compare and contrast the "Defense in depth" and "Secure the weakest link" principles for secure design?

9) Compare and contrast the "Secure by default" and "Fail securely" principles for secure design.

10) What is the vulnerability in caching access control decisions? Explain using an example.

11) Which access control model would you use to implement the "principle of least privilege" and why?