

CS 493

Secure Software Systems

Midterm review – question format

Dr. Williams

Central Connecticut State University

Agenda

- Question formats
- Sample problems/questions

Question formats

- Multiple choice
- Short answer
- Given description of application
 - Identify a functional requirement that has associated security requirements and why
- Given a functional requirement
 - Do a security requirements analysis (fail case/consequence/risk)

Question formats cont.

- Given a use case diagram
 - Add security annotations where appropriate (internal/external/confidential)
 - Apply Misuse Management Method (MMM) to diagram security operations of the use case
- Given a rough application architecture description and a sequence diagram
 - Label vulnerability mapping (V3, V2, V1)
- Given a application architecture description (1-tier, 2-tier, 3-tier, n-tier) and a description of the process
 - Create first order scope map

Sample questions

- (Circle all that apply) The type of architecture that abstracts the business logic from the client side is:
 - a) monolithic b) 2-tier c) 3-tier
- What are the risks associated with directly executing user input?
- Explain the purpose and principles of a boundary class

Identify security considerations

- Given description of application
 - Identify a functional requirement that has associated security requirements and why
- Same format as Homework 2 part 1 – description of application, identify functional requirement with security implications – but focus on being able to explain why it has security implications (rather than just identifying a fail case)

Security requirement analysis

- Same format as Homework 2 part 2 –
Description of application if needed and
requirement
 - Perform security requirement analysis
 - Identify a security fail case
 - Associated security consequence
 - Associated risk

Annotate and perform MMM

