Curry College
Curriculum Course Description

IT xxx
Engineering of Secure Mobile Applications

Contact Hours: 4/wk Credit Hours: 3

COURSE DESCRIPTION:

This is the xxx course of a xxxx xxxx sequence. The Engineering of Secure Mobile Applications (ESMA) course introduces concepts related to creating secure mobile applications including principles of secure design, development, testing and maintenance of secure mobile applications. The course will be comprised of three primary areas including:

1. Lectures
2. Hands on activities & discussions.
3. Significantly sized team projects.

Prerequisite: xxxx

LEVEL

The course assumes students have a basic understanding of mobile development, and writing code. While some security and basic Software Engineering background is encouraged, it is not required for the course.

RATIONALE

Creating software which is on time, on budget and is high quality is paramount for any successful software project. This difficult balance requires the developer(s) to follow sound Software Engineering practices such as proper requirements elicitation, software design, software development, testing, deployment and maintenance. An area that has become prominent in recent years is software security. Developers and customers are both realizing that it is not only enough to create good software, but secure software was well. Software vulnerabilities have the ability to lead to a total project failure from both an ethical and monetary perspective.

In this course, students will learn to create secure mobile applications using the proper software engineering mindset required to be successful projects. While software engineering terms and practices will be lightly discussed, the primary emphasis will be on mobile security.

COMPLETION CRITERIA

Upon successfully completing this course, the student should be able to design, implement, verify and maintain secure mobile applications using the proper software engineering processes.

TEACHING SUGGESTIONS

Mobile software development and security are extremely fast moving topics. What was important several months ago may no longer be relevant today. Conversely, security principles such as the principle of least privilege which were important aspects of software security are still relevant today. The instructor will need to balance the instruction of fundamental aspects of security, along with cutting edge and relevant topics. Focusing too much on fundamental aspects of security will not only lose student interest, but will not get them ready for the real world. Conversely, not giving the students a good, fundamental background understanding of these principles will only ready students for the "now", which will become quickly outdated and irrelevant before the students even graduate.

A good balance of theoretical lectures and current hands on activities and readings should be used in this course.

TEXTS

Text book(s) will be selected based upon their A) Relevance B) Understandability. Due to the fast moving nature of mobile development and malware, examples will be taken from the web and external readings, while the textbook will be expected to provide a firm theoretical foundation.

TERMINAL COURSE OBJECTIVES

1. Students should be able to design a secure application. This includes, but is not limited to
2. Students should be able to implement a secure application from a design. This includes, but is not limited to the adherence to the principle of least privilege, secure data storage and transmission, and ability to create secure interprocess communications.
3. Given an application, students should be able to test it for vulnerabilities using a mixture of existing tools and manual analysis. Some of which include automated and manual fuzz testing and existing risk assessment tools.
4. Given an application with vulnerabilities, students should be able to repair these issues and demonstrate that the vulnerability has been eliminated.

5. Students should be able to create mobile applications which are maintainable from both a design and requirements perspective, but also from a security perspective as well.
6. Students should be knowledgeable about relevant resources for both providing information on current vulnerabilities and defensive programming practices, as well as current vulnerabilities.

POSSIBLE ENABLING OBJECTIVES

1. Provided a set of vulnerable applications
   a. Demonstrate why they are malicious
   b. Discuss their vulnerabilities
   c. Discuss how they should be repaired to eliminate their vulnerabilities
   d. Implement necessary fixes

2. Provided requirements
   a. Create proper application design
   b. Create secure application using proper software development techniques and guidelines.
   c. Demonstrate and discuss why it is secure.

3. Use of existing security tools
   a. Students should be able to find new
   b. Student should be able to use a variety of security testing tools including, but not limited to Stowaway, Androrisk, and Robotium
4. Security practices
   a. Find them
   b. Use them
   c. Check for them
   d. Understand their importance
   e. Ability to identify over & underused permissions and how they create vulnerabilities

5. Use of relevant websites
   a. Know where to find

6. Understand general security principles
   a. iOS, Windows, Android
   b. Fuzz Testing

7. Understand and demonstrate secure data storage
   a. Local
   b. Transmission
   c. Cloud

A. Vulnerability of the Day: Study a variety of small case studies related to mobile security. These activities are intended to be fairly short case studies (10-15 minutes total) where the students are provided a brief case study about an interesting, current or relevant mobile vulnerability. When possible, The primary objectives of this activity are:
    a. Acclimate students with current vulnerabilities and vulnerable areas of mobile software.
    b. Demonstrate the importance of secure mobile software development.
    c. Understand how mobile vulnerabilities are detected and solved.