Engineering of Secure Mobile Applications

Summary

Blah

- Provide an Introduction/Summary to the project
- How mobile applications differ from conventional software
-

Project Description

Blah

Proposed Research

Blah

- Provide an introduction to the course & project
- Drive home why this work is needed & important
-

Course

Engineering of Secure Mobile Applications will combine three existing disciplines, Computer Science, Software Security and Software Engineering. The primary objective of the course will be to instruct students in building a robust mobile application using the Software Engineering mindset needed to deliver it on time, on budget and high quality; but with a continuing focus on ensuring its security not only for its initial release, but for future releases as well.

Mobile applications create a unique opportunity for software developers in that they allow access to information and features which not possible in conventional, desktop applications. Additionally, mobile applications allow the relatively mechanism for updating software for feature enhancements, bug fixes, or support for hardware devices. Finally, small development teams or even individuals have the capability to create, release and support “apps” used by millions of mobile users.

However, these benefits also create a unique set of challenges for mobile developers. The access to information and mobile features also creates an attack mechanism and honey pot for

malicious users who can use this data to their advantage in a variety of ways including data theft, …… Developers are also tasked rolling out new software versions in an extremely expedited fashion…. Add more to this

The Engineering of Secure Mobile Applications course would help to prepare to students for overcoming these challenges. Students would optimally first take an introductory course in computing security. At RIT, that may be a course such as our "Engineering of Secure Software" (http://www.se.rit.edu/~swen-331/01/index.html) course. This would provide students a firm foundation for the more advanced and specialized topics which would be discussed in the Engineering of Secure Mobile Applications course.

While the course would cover a wide array of topics, some of the most prominent would be:

1. Testing for Security
    a. Automated
    b. Developing a process
    c. How to ensure that a defect has been repaired
2. Design of Secure Mobile Software
3. Protect against clones? – Not sure if this is possible
4. Create maintainable software from a security perspective
    a. Fix vulnerabilities fast and cheaply
5. Resources for learning about new vulnerabilities
6. Resources for learning how to fix vulnerabilities

- Expand upon all of these above

While a large portion of the course would be lecture based, there would be a significant amount of hands on activities for the students. Some of these would include:

Real World Case studies:
The students would routinely study examples of security vulnerabilities in mobile applications. Optimally, these would be relatively current examples, but important legacy examples would be examined and discussed as well. These case studies would serve several purposes including:

- The demonstration of the importance of creating secure software and the negative implications of vulnerabilities from a technical, ethnical, and business perspective.
- Learn from the experiences of others, in creating secure mobile software, but how to properly fix vulnerabilities as well.
- Keep the course relevant and demonstrate the importance of creating secure mobile applications.

Class Activities & Homework Assignments:

Students will be asked to deliver short homework assignments and in class activities. These will serve to reinforce the lecture topics and introduce students to concepts in a more hands on manner.

Semester Long Project:
A significant portion of the course will be devoted to two team based projects over the 15 week long semester. The project will consist of two phases, with the first phase lasting approximately 10 weeks, with the second lasting the remaining 5. For each component, teams will consist of approximately 4-6 students, as this is the team <cite> size typically used in industry.

Project A (5 weeks) – Repairing vulnerabilities in existing application.

Each student team will examine an open source mobile application with a publicly accessible version control system which contains known vulnerabilities. Students will be asked to repair the vulnerabilities in the open source projects in addition to providing justification why it was a vulnerability, how they identified the vulnerability, why the vulnerability was introduced (to the best of their ability), and how they made the project more secure. At the conclusion of the project component, students will be encouraged to submit their results to the authors of the original open source project.

The primary learning objective of the project will be to instruct students how to repair vulnerabilities in mobile software. This will also serve as a basic introduction to mobile application development, which the students will need for the second project.

Project B (10 weeks) – Developing a secure mobile application

Teams will be provided with specific requirements for a small to medium sized mobile application. Teams will be expected to deliver defined sets of functionality for each release in order to mimic the frequent release structure of a real world project. This would also serve as a demonstration of the importance of a good system design and in creating software that was not only secure for each release, but for future releases as well. Additionally, for each release teams will be expected to use a myriad of existing security tools and techniques to demonstrate that their application has been designed and implemented in a secure manner. The following will be significant deliverables required by each Team

Week 2: Initial Application Design

Students will present their design to the instructor and their classmates who will provide feedback and ask the presenting teams to justify their design from a security perspective. Students will be evaluated upon their overall system design, but largely through a security perspective.

Week 4: Release 1

- Deliver initial working version of mobile application. Application shall be runnable on an actual mobile device.

Week 5: Cross Team Testing

Each team's projects will be evaluated by another team from a security perspective. The teams will test out each other's works using a variety of methods including, but not limited to:

- Security testing using a variety of existing tools
- Perform a code review to find security vulnerabilities & defects.
- Recognize points of strength in the design and implementation from a security perspective.

Week 6: Release 2

- Presentation: Demonstration and presentation of application and security design, process and structure will be delivered to the instructor and classmates. Teams will be expected to justify and defend their design and implementation form a security perspective.
- Deliver initial working version of mobile application. Application shall be runnable on an actual mobile device.

Week 8: Release 3

- Deliver initial working version of mobile application. Application shall be runnable on an actual mobile device.

Week 10: Final Release

- <<Same as week 6>>

The primary learning objective of this activity will be instruct students in designing, creating and maintaining secure mobile applications with the proper software engineering mindset.

Darwin

Darwin

- Describe the Darwin Project
- Why is it important
- Why help is of the utmost importance in order to continue this research
- What are some preliminary findings

Biographical Sketch

Blah

Budget Justifications

Blah

This course would offer the unique opportunity to allow the instruction of students……

- Rapid releases mean security testing needs to be fast
- Quick remediation method for releases

- Talk about how it will do each of the primary areas

    - Who the course is geared toward
        - 2 course sequence
    - Most mobile courses are housed in a computer science program. Teach programming, not engineering.
    - Only a handful of Mobile security programs (check this)
    - What work still needs to be done. Why the need for the research

    - All course materials & results would be publicly available for use at other institutions.

- Make sure to state why this course is different than anything else out there. Maybe have a special section for this & compare to what other classes & universities do.
- For the cost analysis, break this down for the course and the project.
-