

Syllabus for SE525 Software Security Architecture, Winter 2014

Corin Pitcher

29 December 2013

Overview

NOTE: this class can count for the Software and Systems Development area of the MS CS (it is not listed, but the change has been approved, ask the instructor for details). It can also count for the Security and Software Engineering areas of the MS CS.

Bulletin Description

Students in this course will learn architectural patterns for integrating security into software.

Topics include:

- an overview of software security;
- integration of authentication, access control, and auditing into software;
- programming with symmetric-key and asymmetric-key cryptography, including key distribution and key management, use of certificates, and SSL/TLS;
- security mechanisms in modern runtime environments, e.g., code signing, code verification, access control, and security policies.

Students will get hands-on experience designing and implementing secure software.

Further Information for Winter 2014 Section

The Winter 2014 section of SE525 will cover software architecture for secure operating systems and applications. The focus is on architecture that supports established security principles such as:

- access control, accountability, and usage control for data, computational resources, network resources, and power.
- least privilege and defense in depth.
- cryptography and key management to provide confidentiality, integrity, and privacy guarantees.

Students will develop their understanding of these security principles by analysis of the architecture of existing software, and by the design and development of new architectural components.

The investigation will be carried out in the context of the Android platform <http://www.android.com>. The Android platform has the largest share of the US smartphone market at the time of writing (see, e.g., <http://www.engadget.com/2012/11/02/comscore-us-smartphone-share-leveled-off-in-september/>). A range of Android phones and tablets are available from manufacturers including Acer, Asus, HTC, LG, Motorola, Samsung, Sony Ericsson, etc. Other form factors are emerging that use Android, e.g., developer boards <https://www.miniand.com/products/Hackberry%20A10%20Developer%20Board> and HDMI sticks <https://www.miniand.com/products/MK803%20Android%20Mini%20PC>.

Android uses a Linux kernel with user applications (mostly) written in Java. The lifecycle, inter-process communication, protection domains, and access control for Android applications differs significantly from those found in other operating systems for desktop and server computing.

The key attributes that make the Android platform useful for this class are:

- Open source and free tools.
- Readily available documentation.
- Timeliness.
- A relatively small system and applications (in comparison to desktop/server operating systems and their applications).

- A modern design with security in mind.
- Can focus on security architecture rather than low-level vulnerabilities, because low-level vulnerabilities are minimized by the use of a modern programming language and runtime.
- Some security and privacy problems are particularly acute in a mobile setting, e.g., loss of physical device, location tracking, etc.

Prerequisites

Contact the instructor at least 72 hours before the last date to drop without penalty if you have any doubt about whether you have satisfied the prerequisites listed below.

Course prerequisites

The following courses are prerequisites:

- CSC435 Distributed Systems I
- CSC447 Concepts of Programming Languages OR SE 450 Object-Oriented Software Development

Other Prerequisite Skills

Students are expected to have the following skills prior to starting this class:

- Java development competency
- Elementary socket programming
- Familiarity with UNIX shell
- Familiarity with integrated development environments (such as Eclipse, Visual Studio, NetBeans, etc.) and ability to learn the Eclipse IDE on your own.

Other Prerequisites

- NOTE: It is NOT necessary to have an Android device for this class. The Android emulator can be used instead.
- A reasonably modern computer that can run Java 6 or Java 7, the Eclipse IDE, and the Android development tools (see the supported platforms at <http://developer.android.com/sdk/index.html>). Windows, OS X, and Linux are all supported. 2GB or more of RAM is recommended for reasonable Eclipse performance.

Textbooks

There are two required textbooks. The first textbook is a general systems account of Android. The second textbook discusses security in the context of Android systems.

The textbooks are available in paperback. Additionally, both textbooks are available for direct purchase from their publishers as DRM-free PDFs, or with DRM from other sellers.

- <http://www.manning.com/collins/> Android in Practice, by Charlie Collins, Michael Galpin, Matthias Kaeppler. Publisher: Manning Publications; 1 edition (October 7, 2011). ISBN-10: 1935182927. ISBN-13: 978-1935182924.
- <http://shop.oreilly.com/product/0636920022596.do> Application Security for the Android Platform: Processes, Permissions, and Other Safeguards, by Jeff Six. Publisher: O'Reilly Media (December 10, 2011). ISBN-10: 1449315070. ISBN-13: 978-1449315078.

Assessment

COMPONENT	PERCENTAGE
Homework assignments (3)	45% (15% each)
Team research project	55%

Policies

- Students are required to attend lectures or watch them online within 48 hours of posting (generally posted the day after the class).

- Students are required to subscribe to and read the class mailing list.
- Students must keep backup copies of all submitted work.
- Students must test submitted assignments to verify that they are properly submitted.
- Late submissions will not be accepted without a serious documented excuse.
- Late submissions without a serious documented excuse will only be accepted if a request is made at least 24 hours prior to the exam and prior permission is given by the instructor. Note that the most likely response will be to submit what you have on time instead of a late submission.
- Homework deadline extensions will not be given for enrolling in the class after the quarter has begun or for being out of the country at the beginning of class.
- In-class and OL students will need to keep in contact with one another outside class using technology to be mutually agreed upon.
- The CDM and University policies on instructor evaluation, email, plagiarism and incompletes apply to this class. In particular, note that plagiarism is a violation of the university's policy on academic integrity. Violators will receive a 0 for the corresponding assignment and will be reported as **required** by the University plagiarism policy.
- Online students should review the CDM Online Learning Policies which apply to this class. See <http://www.cdm.depaul.edu/onlinelearning/Pages/OnlinePolicies.aspx>