

# Mobile Application Audit

---

## Overview

Throughout the Mobile Security course, students will apply what they're learning to a case study of a particular mobile application, either existing or envisioned. As part of each day's class material, we will hold a discussion of how developers and designers can consider security and privacy features related to the topic of the day into their products. Each student will take this discussion into the context of their chosen app, leading to a recommendation or design criterion for their app. By the end of the semester, each student will have a detailed "blueprint" of how their chosen app can be designed to handle a wide variety of vulnerabilities and system considerations.

## Requirements

Although the content is strongly based on in-class discussions, each student is responsible for their own app audit, and all documentation must be done individually. Every student is expected to participate and contribute to the in-class discussions. At the end of the semester, each student will submit a written report that 1) describes functionality, features, and interactions involved in the mobile application; 2) details the vulnerabilities and threats in specific smartphone system components that are relevant to the security of the chosen application; and 3) provides a list of recommendations or considerations that could be used to design and develop an improved app in the future.

## Deliverables

The sole deliverable of the mobile app audit is the written report. The report can be in any reasonable format and be written in a sufficiently deep level of detail, but it should not exceed 5 pages. The mobile app audit report is due on December 12, 2012.