Understanding Android's Security Framework

William Enck and Patrick McDaniel
Systems and Internet Infrastructure Security Laboratory (SIIS)
Computer Science and Engineering Department, The Pennsylvania State University
{enck,mcdaniel}@cse.psu.edu

Overview – The Google Android mobile phone platform is one of the most anticipated smartphone operating systems. Android defines a new component-based framework for developing mobile applications, where each application is comprised of different numbers and types of components. *Activity* components form the basis of the user interface; each screen presented to the user is a different Activity. *Service* components provide background processing that continues even after its application loses focus. Services also define arbitrary interfaces for communicating with other applications. *Content Provider* components share information in relational database form. For instance, the system includes an application with a Content Provider devoted to sharing the user's address book upon which other applications can query. Finally, *Broadcast Receiver* components act as an asynchronous mailbox for messages from the system and other applications. As a whole, this application framework supports a flexible degree of collaboration between applications, where dependencies can be as simple or complex as a situation requires.

In this tutorial, we will overview the mechanisms required to develop secure applications within the Android development framework, indicating how the environment has evolved with recent releases of the SDK. We will begin with the basics of building an Android application; no prior knowledge of Android is required. From this base, we will demonstrate how applications can communicate and provide services to one another. However, these interfaces must be carefully secured to defend against general malfeasance. We show how Android's security model aims to provide mechanisms for requisite protection of applications and critical smartphone functionality and present a number of "best practices" for secure application development within the environment.

Speakers – William Enck is a doctoral candidate researching network and systems security in the SIIS Lab in the Computer Science and Engineering Department at Penn State University. William's research efforts have included telecommunications security, specifically modeling and characterizing SMS vulnerabilities, systems and hardware security, and large-scale network configuration. His work has appeared in many major conferences and journals and has received national and international press coverage.

Patrick McDaniel is an Associate Professor in the Computer Science and Engineering Department at the Pennsylvania State University and co-director of the Systems and Internet Infrastructure Security Laboratory. Patrick's research efforts centrally focus on network, telecommunications, and systems security, language-based security, and technical and public policy issues in digital media. Patrick was awarded the National Science Foundation CAREER Award and has chaired several top conferences in security including, among others, the 2007 and 2008 IEEE Symposium on Security and Privacy and the 2005 USENIX Security Symposium. Patrick is the editor-in-chief of the ACM Journal Transactions on Internet Technology (TOIT), and serves as associate editor of the journals ACM Transactions on Information and System Security and IEEE Transactions on Software Engineering. Prior to pursuing his Ph.D. in 1996 at the University of Michigan, Patrick was a software architect and program manager in the telecommunications industry.