Mobile Platform Security

N. Asokan

Univeristy of Helsinki
n.asokan@cs.helsinki.fi

Abstract. In the past few years, there has been a dramatic increase in the popularity of the category of mobile phones commonly known as "smartphones". Consequently there is increased interest in the security and privacy research community in "smartphone security". All dominant smartphone platforms, or more generally, mobile phone application platforms, incorporate platform security architectures that are widely deployed.

In this talk, I will first discuss the reasons why mobile platform security has seen such widespread deployment: in contrast to PC platforms, mobile phones began as closed systems with limited functionality but right from the beginning different stakeholders had certain clear security requirements for mobile devices. For example, regulators required that a mobile phone must have unique device identifier and must incorporate technical mechanisms to resist modification of this identifier; mobile operators required technical means to enforce subsidy locks.

I will then discuss and compare some of the mobile platform security architectures in more detail. All of them make use of several common techniques that date back several decades but have also adapted them for the particular needs of the mobile device setting. I will present a common framework and highlight some of the different design choices made in different platform security architectures.

I will conclude by pointing out some open problems.