Title:
"Secure App Execution On Commercial Mobile Devices By Means Of Bare Metal Hypervisors"

Authors:
Katrin Hoeper, Matthew Pirretti, Kevin Gudeth and Ron Buskey (all Motorola Solutions, Inc)

Emerging Technology Space: "Mobile Devices"; more precisely running security sensitive apps on commercial mobile devices

Class of Cryptographic requirements: crypto engines, security policy enforcement, process and resource isolation

Mobile devices are quickly becoming the dominant computing platform. As such, the number of security sensitive applications that run on commercial off-the-shelf (COTS) mobile devices is growing steadily. This trend is prominently illustrated by the large number of personal mobile devices used to access enterprise email. Other emerging applications include, consumers using their phones as electronic wallets, health care providers looking up patient data on tablets, and law enforcement officers using commercial phones for official purposes. The motivations for this trend are diverse, including cost reduction, minimizing carried equipment, maintaining device familiarity, and the inconspicuous form factor.

Sensitive applications have security requirements that have traditionally only been satisfied by running hardened operating systems on top of specially built devices. We foresee bare metal virtualization as being capable of providing the necessary process separation to provide an alternate system architecture that satisfies the security requirements of sensitive applications without the significant costs associated with special purpose hardware. In addition, this architecture provides all the previously mentioned benefits of using COTS devices.

We advise the use of bare metal hypervisors which directly run on the hardware with all guest OSs and optionally individual applications and drivers running in their own virtual machine. For instance sensitive applications can utilize a common, trusted, and possibly formally verified partition to perform cryptographic operations, leveraging the strong isolation provided by the virtualized environment. This enables sensitive apps to securely execute on COTS mobile devices despite OS compromise and in the presence of malicious or exploitable applications. Another aspect is the ability to provide a policy enforcement engine that is isolated from the COTS OS, and thus providing a tool for meeting security and privacy standards and implementation guidelines.