Isolation using virtualization on mobile devices


Project Description
Trust-worthy computing on mobile systems can help enable deployment of security-conscious applications. Isolation offered by virtual machines can assist to offer the protection level necessary for e-payment, protection of information, and rights management. Strict isolation between virtual machines can allow for more flexibility in the application OS which cannot interfere with critical services.

Architecture
Three key domains need to be isolated: Applications running open source software under Linux, Software radio, and a trusted application VM. Effective isolation between partitions will help to protect each partition against information leakage due to software errors and external attacks.

Approach
A virtual machine platform, such as L4/Wombat or Xen will provide the basic virtualization framework necessary for this project. Special needs of mobile systems will be accommodated by improving the subsystems as necessary to attain the desired performance, isolation, and other specific needs of the applications.

Challenges
- **Overhead**
  - Embedded systems require low overhead high-performance mechanisms.
  - Performance has an impact on battery life.
  - Low-overhead inter-VM communication mechanisms.

- **Security**
  - Performance/security tradeoffs
  - Trustzone enhancements
  - Inter-VM access controls
  - Secure messaging among virtual machines
  - Policies to govern sharing of data

- **Real-time**
  - Critical periodic tasks such as the radio need to remain operational.
  - VMM control of real-time scheduling
  - Multimedia
  - Power management

Funded by Motorola through the Motorola Communications Center (MCC) Project #34. Fall 2006 - Fall 2007.