CERIAS

The Center for Education and Research in Information Assurance and Security

PURDUE UNIVERSITY

Co-tenant Application Security on Mobile Devices

Pelin Angin, Bharat Bhargava

Department of Computer Science & The Center for Education and Research in Information Assurance and Security
Purdue University

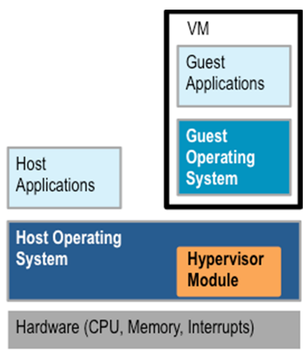
Main Security Issues for Mobile Devices:

1. **Multi-user support:** Each application might need a different security model so that the data from one does not get exposed to the other; however, because there is one user profile, the device may or may not be able to support the distinction.
2. **Secure data storage:** Many applications store sensitive information locally on the device in clear text. Other installed (malicious) applications running on the device could access this information and can send it to a remote server controlled by an attacker.
3. **Application isolation:** Applications on a mobile device and the people who use them require access to different types of data. The ability to isolate these applications and the data they require is an important step in ensuring a simple application does not have access to the confidential data of another application.

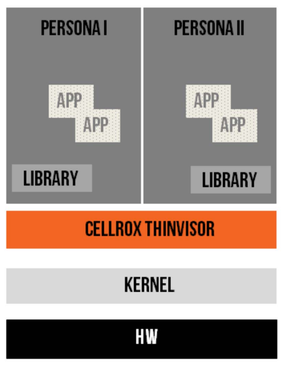
Application Co-tenancy

To keep the operating system (OS) clean and safe, it is better to isolate applications from each other. In addition to isolation, limiting the application's calls into the core OS is also important. In general, the application should only have access to the core OS in controlled and required areas, not the entire OS by default.

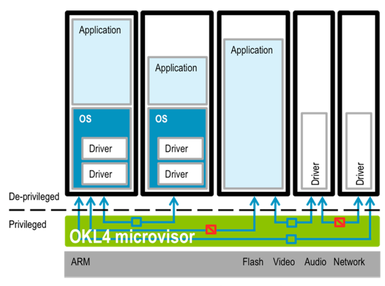
Existing Work in Mobile OS Virtualization:



VMWare MVP



Cellrox ThinVisor

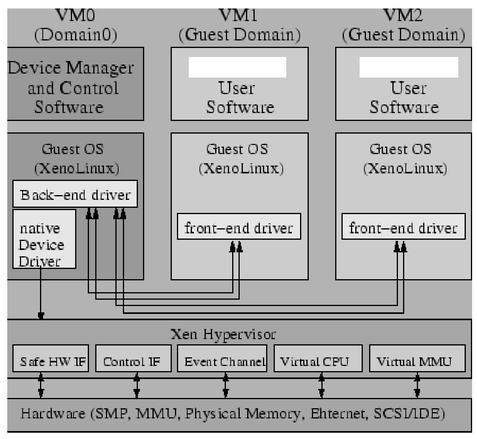


OKL4 Microvisor

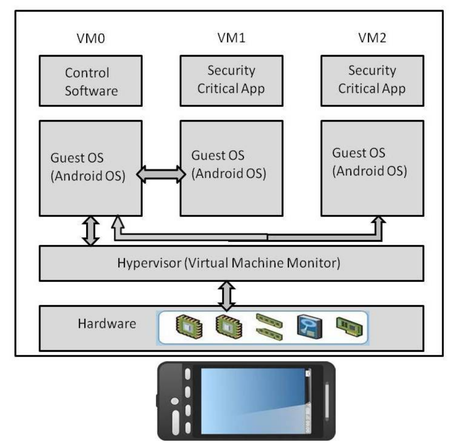
Virtualization-based Isolation of Security-Critical Applications

Our proposed approach for isolating applications on a mobile device is based on running security critical applications in their own virtual machines, which will allow for separation of the data space of these from that of other applications on the same device.

Mobile Virtualization Architecture:



Xen Virtualization Architecture



Virtualized Android Architecture

Under this modified system architecture, for each security-critical application installed on the device, a new virtual machine is instantiated under the control of the management virtual machine (VM0) upon application launch and the virtual machine is killed upon application termination. In order to keep performance penalties minimal, this architecture does not create virtual machines for applications not involving sensitive data and operations, therefore those applications run on VM0.

Dealing with Untrusted Management OS*:

To mitigate the security risks posed by an untrusted management VM, trusted execution of the virtual machines is assured by:

- Memory access from the management VM to any guest VM using foreign mapping (direct mapping of memory pages from other domains into the management VM's own address space) is prohibited except for saving, restoring and building of the guest VM.
- The hypervisor makes sure that it monitors every memory and virtual CPU (vCPU) access from the management VM to the guest VM, and encrypts all the memory pages and vCPU registers if they involve any private information of the guest VM.
- After the access of sensitive information or the execution of some security-critical domain management tasks, the hypervisor checks the integrity of the run time state of the guest VM.

Application Monitoring by VM0:

Monitoring module in VM0 in addition to control software:

1. Measure application behavior's deviation from normal (check for parameters like number of system calls, types of system calls, amount of data transfer, use of sensor data etc)
2. Track information sharing of applications with external services (taint analysis)

* Chunxiao Li, Anand Raghunathan, Niraj K. Jha. "Secure Virtual Machine Execution under an Untrusted Management OS". IEEE 3rd International Conference on Cloud Computing, 2010.

CERIAS

Discovery Park e-Enterprise Center