WIND RIVER SECURE ANDROID CAPABILITY

Cyber warfare has swiftly migrated from hacking into enterprise networks and the Internet to targeting, and being triggered from, mobile devices. With the recent explosion in the number of connected devices, security attacks can now be launched from anywhere, targeting any place. Securing mobile devices is crucial because the same capabilities that increase our social interactions and business effectiveness can be subverted and used for unintended and unapproved uses. As a widely deployed and robust open source platform, Android provides the ideal foundation for the integration of appropriate security controls for personal and business device protection as well as high-assurance and battlefield use cases.

Wind River® has combined our extensive experience in commercial Android with our capabilities in secure certified embedded systems to develop an advanced security strategy for Android platforms that also ensures compatibility with the commercial Android development model. This comprehensive strategy includes attack detection and prevention, device integrity, isolation techniques, and infrastructure security to protect data and devices from multiple threat vectors.

Wind River Android Security Strategy

| Attack Detection and Prevention | • SE Android with enhancements  
|                               | • Selective permissions  
|                               | • Pre-install filter  
| Device Integrity              | • Secure boot  
|                               | • Secure firmware management  
|                               | • Cryptography  
| Isolation                     | • Lightweight partitioning  
|                               | • Hypervisor  
| Infrastructure Security       | • Mobile device management  
|                               | • Integrity and attestation  
|                               | • Forensics  
| Secure Android Deployment     | • Testing and Android compliance  
|                               | • Certification and validation  
|                               | • Audit  

ATTACK DETECTION AND PREVENTION

Security threats against Android-based devices are extensive and include unauthorized access, data and device destruction, information disclosure, modification of information, and denial of service.

Security Enhanced (SE) Android identifies and addresses critical gaps in the security of Android. Released by the National Security Agency (NSA), it consists of Linux kernel and Android user space modifications. Wind River enhances SE Android by implementing additional features to remove vulnerabilities and allow more specialized policy for a given use case, including the following:

- Semi-custom policy for downloaded applications
- Restricted privileges as demanded by most enterprises and IT organizations
- Code extensions to support standard Android drivers
- Initial security policies with Android Compatibility Test Suite (CTS) and Wind River Test Management for Android

SE Android was released with a reference implementation to open source, and the Wind River enhancements fill the gaps between that release and the requirements of a commercial product.

Further precautions can be implemented with deployment of pre-install filters managed by customizable policy to inspect software installation requirements and disallow installation of applications requiring access to restricted device capabilities like cameras, network access, or recording features.

DEVICE INTEGRITY

Mobile device software stacks consist of many layers of software, from low-level boot firmware through operating system kernels, system services, middleware, and applications. Attackers can exploit vulnerabilities in any of these areas to turn a threat into a successful attack.

Secure boot provides the foundation of security by verifying each stage of the boot process before it is executed. This mechanism allows only authenticated software and prevents malicious code from being executed. Secure boot implements a chain of trust in which every component in the boot process measures the next one; if any component fails to pass signature verification, the boot process will respond appropriately.

Secure Android firmware management is integrated with secure boot and provides additional protection with error tolerance for power off, low battery, corrupt package, and memory error, as well as policy that allows only authorized and signed update packages to access the device.

Integrity mechanisms require robust cryptography features to ensure digital signatures and other protections are appropriately verified. Robust cryptography is not only essential to support integrity verification, it is also essential to fully protect data, software, device access, and communications.
ISOLATION

Android is designed for a single domain where installed applications share system resources, limiting its flexibility for reusing the device for multiple purposes that span multiple domains or multiple users. Some existing multi-domain solutions rely on virtualization, with guests corresponding to different protected domains, typically causing significant overhead and complications whenever there is a need to share hardware resources.

Lightweight partitioning (LWP) is a security isolation strategy that provides multiple encrypted partitions, keeping information safe and secure between them. For example, a project team sharing a tablet can set up multiple users, or one partition can be set up to secure personal information and another to secure corporate information.

LWP protects data from “leaking” across partitions so that secure applications and data can be kept separate (isolated) from other partitions.

For more concurrent partitioning, Wind River delivers virtualization for Android with a type 1 real-time embedded hypervisor, providing a virtualization layer that partitions a single- or multi-core chip into multiple partitions with varying levels of protection and capabilities. With a small footprint and high performance, Wind River Hypervisor offers all the benefits of embedded virtualization for Android:

- A faster and more reliable virtualization environment
- Lightweight and easy configuration and deployment on complex devices
- Secure environment separation between different operating systems, components, and applications
INFRASTRUCTURE SECURITY

A comprehensive Android security strategy needs to address operation of the device within a greater networked system. Mobile device management (MDM) systems deliver important security features such as Android firmware distribution, security policy distribution, device inventory, and remote lock and wipe to stolen devices. These MDM capabilities ensure that system threat detection and prevention goals can be achieved. Wind River has implemented a lightweight MDM system that can be used to enhance control of the Android device, consisting of both server and client components. If you have an existing MDM system, the client portion is easily adaptable to connect to your in-house or third-party MDM solution.

Authentication and identification are key security capabilities with a broad set of features and overlapping functionality. One aspect of authentication and identification protects the resources on the device by allowing access only to known users with physical access to the device; users who cannot demonstrate that they are valid users must not be allowed access to the resources of the device. Another aspect protects the resources on the device by allowing access only to known remote systems; a device must not perform MDM actions unless it can be assured that the MDM server is the one it claims to be. A third aspect of authentication and identification protects the resources on a remote server or system from a compromised device; the device must authenticate to the remote server that it is the one it claims to be and that the user has the proper credentials to access the remote system’s resources.

To better support system security, measurement and attestation should be added to the secure boot process at startup to take a measurement of code and state and provide evidence of authenticity. These actions are repeated periodically during device operation, and results are reported back to the enterprise management system.
WIND RIVER ANDROID AND SECURITY EXPERIENCE

- Founding member of the Open Handset Alliance (OHA)
- Original Google commercialization partner
- 100+ Android projects since 2007
- Contributor to the U.S. National Security Agency’s SE Android project
- FIPS 140-2 certified cryptography
- Common Criteria certification
- Wurldtech’s Achilles certification

WIND RIVER SECURE ANDROID DEPLOYMENT

Adding advanced security capability to Android devices while still maintaining conformance to the Android development model introduces increased complexities for testing, validation, and certification of these devices.

Wind River offers a complete automated test environment, Wind River Test Management for Android, to prove compliance with Google’s Android Compatibility Test Suite (CTS), measure performance, and ensure the stability of devices running Android. Test Management for Android incorporates existing tests and test frameworks, and includes compliance test suites that can all be extended to support certification and validation processes.

Certification and validation of secure devices is assured and expedited by comprehensive tool suites managed by expert security resources. Wind River Professional Services can support medium- to high-assurance certification efforts for secure Android platforms, as well as auditing and forensic activities and requirements.

WIND RIVER SECURE MOBILITY VISION

The challenge of securing the Android commercial capability and mobile platform requires end-to-end system threat assessment and incorporation of embedded device strategies to effectively thwart cyberattacks and maintain secure communications. Wind River takes a holistic approach that includes threat and risk assessment services; technology solutions that counter security threats yet still deliver the benefits of commercial mobile platforms; and testing and verification frameworks that enable secure devices to be quickly verified, approved, and deployed.