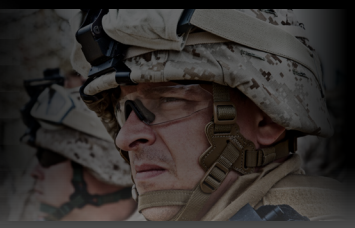
SECURE MOBILE TECHNOLOGY

- MULTIPLE POLICIES
- MULTIPLE MODES
- ONE DEVICE

REDWALL TECHNOLOGIES

RESTRICTED MODE

An encrypted voice and data app only for communicating with highly trusted parties



PRIVATE MODE

Banking and financial apps only, multi-factor authentication required

ENTERPRISE MODE

Install approved apps only from Play Store, no location services

PERSONAL MODE

Games, Twitter, Gmail, Facebook and other personal apps

Redwall Technology's mobile security product, featuring Redwall Mobile® (RwM) technology, brings together the security of a military-grade communications device with all the features and functionality of a modern smartphone in a single, inexpensive, high-assurance platform. RwM consists of modifications to the Linux kernel and Android operating system plus additional functionality to comply with the National Security Agency's (NSA) Enterprise Mobility Program. An optional RwM policy server can remotely monitor, update, and control the RwM devices. RwM provides a robust, trusted, and flexible Android platform, while still maintaining portability among multiple devices with minimal engineering.

The lowest level of security on Redwall devices is provided by a monitor that runs alongside the Linux kernel. This monitor performs checks on every system call, as well as in the scheduler. These checks complement each other, with the system call handler checking the integrity of the scheduler and the rest of the kernel, and the scheduler check helping to ensure the integrity of the system call handler. The monitor and critical portions of the kernel are protected by placing them in a separate memory domain with restricted access. Both the system call check and the scheduler check take steps to reinforce the security of this restricted memory domain. Levels above the kernel (such as core libraries, system files, and apps) are checked for potential security violations in a policy-specific manner.

Core RwM security includes:

- Security monitor in restricted memory domain
- Kernel Integrity checking
- File integrity checking
- Deny setuid
- Check interrupt vector and handler tables
- Prevent process privilege escalation
- Check syscall handler
- Check core scheduler call
- Remove Android Debug Bridge (ADB)
- Remove/restrict ability to load kernel modules
- Chain of trust from kernel to init to any executable in a privileged category
- In policy, deny ptrace
- In policy, deny execution from SD card
- Off-line check for super-privileged instructions
- Scramble Wi-Fi password
- Zeroize memory pages on free

REDWALL TECHNOLOGIES, LLC. 904.704.2127 | james.king@redwall.us

SECURE MOBILE TECHNOLOGY

REDWALL TECHNOLOGIES

In addition to the secure base, RwM allows a single device to operate in multiple modes, each of which has different security postures with different capabilities and levels of trust. The number of modes and the permissions within each mode are completely configurable. The switch between modes can be initiated by the user or via a policy server, or may be caused by an event on the device such as a security violation, or may even be based on the user's location. Cryptographic and temporal isolation ensure that there is no possibility of contamination across modes. It is as if the user is carrying separate devices.

Features of RwM modes include:

- Encrypt data partition for each mode with unique keys
- Modes are temporally separated
- Policy enforcement – syscall access control lists (ACLs), file ACLs, network ACLs,
- Violation actions – ignore, fail, kill process, reboot, log, remote log
- Differential Power Analysis (DPA) countermeasures during encryption
- Custom init GUI to support different authentication methods (before Android starts)
- Logical Volume Management (LVM)
- High-level ACLs (camera, Wi-Fi, bluetooth, NFC, app install, etc.),
- Shared partitions (telephony)
- Redwall keystore

The optional RwM provisioning and policy server provides the following functionality:

- Policy creation
- Device image creation
- Remote device monitoring
- Remote file and app management
- Remote device locking
- Remote logging

Redwall Mobile's patent pending n-persona technology effectively turns one smartphone, tablet of similar device into as many devices as desired, each with its own apps, data, settings and security code. Redwall Mobile is compatible with a wide variety of devices and technologies, which in and of itself sets it apart from narrower solutions. There are features, however, that even combinations of all available technologies cannot match without Redwall Mobile.

Behavioral vs. taxonomic analysis

Rather than looking for specific threats or porting specific parts of a system into a trusted container or cell, Redwall Mobile uses policies to define acceptable behavior, and treats any aberrations as a policy violation. And since Redwall Mobile handles violations with graduated responses based on the mode or persona, there is no need to lock down a device to the point where it becomes unusable. There are also no pattern definition files or threat definitions to maintain.

Policy-driven security model enforced from TEE in secure memory

Redwall Mobile creates a secure memory region wherein it executes a trusted monitor, called the trusted execution environment or TEE. Competing solutions must take over any trusted code, which adds cost when apps need to be ported to vendor-specific APIs, and grows the trusted computing base to rival the complexity of the untrusted base, making the division of little use. Redwall Mobile's TEE can monitor and enforce separation among different apps with zero changes to those apps.

Temporal isolation in addition to cryptographic and other methods

Sandboxing or virtualization cannot provide this level of isolation in theory, let alone in practice. Those solutions suffer from the shortcoming that trusted and untrusted data co-exist in memory, making them highly vulnerable. Dedicated devices like the Blackphone are even worse, requiring users to cary multiple devices for different roles or different levels of security. Redwall Mobile consolidates all the features of a locked-down secure device with an off-the-shelf device suitable for personal use, reducing cost and complexity, not to mention and weight burden and power usage.

Biomorphics

Redwall Mobile adds diversity between devices and processes while the device is running. This can reduce or more likely eliminate the ability of an attack to propagate from one device to another, as attackers must hit a moving target.

Device support

Redwall Mobile moves easily to new devices without the re-engineering efforts involved in porting virtualization or hypervisor solutions. And it does so with zero changes to existing apps or their frameworks, including both custom apps and Google Play Store apps.

REDWALL TECHNOLOGIES, LLC. 904.704.2127 | james.king@redwall.us