Data Integrity and Confidentiality Resilient Operating System Environment for Multi-Level Security

REDWALL
TECHNOLOGIES LLC

Redwall Technologies, LLC
Beavercreek, Ohio
www.redwall.us

Contact:
John Rosenstengel
President & CEO
Redwall Technologies
john.rosenstengel@redwall.us

Topic Number: N172-105

SYSCOM: Marine Corps Systems Command (MCSC)
www.marcorsyscom.marines.mil

Program Sponsor:
PM Intelligence Systems

Other Potential Programs:
All major combatant commands; any program with a need to have classified or multi-level security on mobile devices

Current TRL: 8

Projected TRL: 9 / Q3 2024

Keywords: Cybersecurity, Mobile Communications, MLS, CSfC, Multirole, Rugged Handhelds

THE CHALLENGE

Commercial smartphones and tablet computers bring computing and connectivity to the battlefield, flightline, cockpit, point of maintenance, depot, telehealth, and other austere environments. However, these devices have inherent OS and application vulnerabilities that expose the DoD to significant risks and impose unpredictable OS update and patch costs. Redwall's NIAP-approved security solution addresses these deficiencies, while enabling a single device to securely operate on classified and unclassified networks. The ability to exchange, store, and utilize controlled and uncontrolled information on a single device reduces logistics costs and network security risks while increasing performance of both labor and systems. Redwall devices can be easily provisioned and reprovisioned to support any mission in any user role context.

THE INNOVATION

Behavioral analysis focuses on how a system should behave when not under attack or influence by an adversary and considers anything else a danger. This technique is effective against zero-day exploits. Even when the cause is completely unknown, the Redwall mobile solution will still stop the threat. Critical system resources are monitored for corruption and immediately (< 2 seconds) restored to known state, providing resilience and fight-through capabilities. Temporal and cryptographic isolation enable multilevel security on a single device.

THE NAVY BENEFIT

Multi-role, multi-mission, multi-level security on a single device (not including burner phones and BYOD)

- Inherent security that pre-empts zero-day exploits to the Android OS and by applications.
- Cyber-resilience with "fight-through-attack" capability to enable mission completion and countermeasures; rapid, policy-based device provisioning (via cloud or local network) to create custom, mission-specific device and application profiles.
- Deployed on military grade, rugged hardware from Motorola Solutions and Zebra Technologies to assure long term hardware support; Redwall's technology is built into devices with manufacturer support—always a trusted boot providing security that cannot be provided by any app.

THE FUTURE

As the core technology-allowing programs to permit SIPR, NIPR, and coalition classification levels on a single mobile device, Redwall's technology is being evaluated now with top commanders in live operations for Joint Operational Certification. Redwall is constantly working to add supported devices and new missions.

SBIR Pavilion

DEPARTMENT OF THE NAVY
SBIR
STTR
Small Business Innovation Research

2024 Navy Gold Coast | August 20 – 21, 2024