STAR LAB

202.706.7027
www.starlab.io

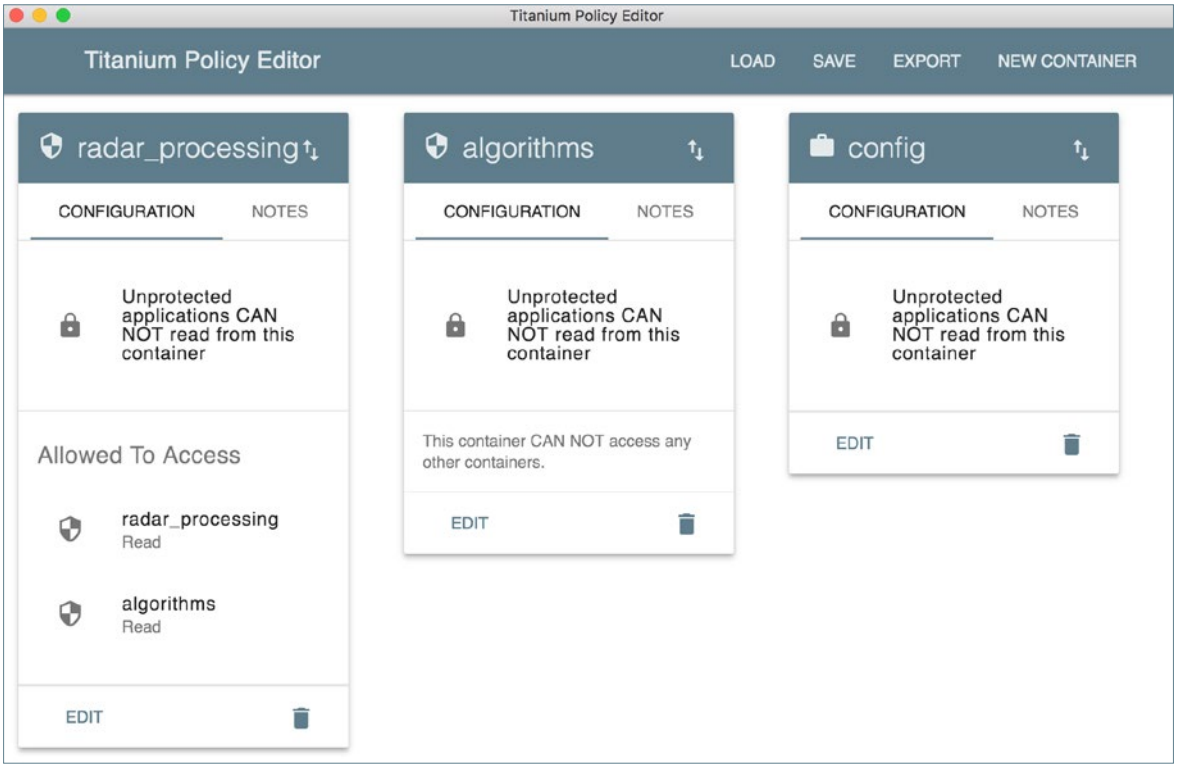
TITANIUM SECURITY SUITE

Bulletproof Security for Embedded Linux Systems

Got Root? Is your system still secure when an attacker gains root access? A common misconception is that network protections and user authentication controls are sufficient to ensure the confidentiality and integrity of sensitive applications and data. Attackers continue to prove otherwise.

Our threat model begins with an assumption that the attacker will eventually gain root (admin) access to your system. Given that reality, the Titanium Security Suite is specifically designed to protect critical software applications, system configurations, and data from unauthorized access, modification, reverse engineering, or theft by malicious insiders.

For operationally-deployed Linux systems, the Titanium Security Suite offers the most robust Linux security capabilities available on the market today.



TITANIUM FEATURES

ENCRYPTION AT REST

TITANIUM encrypts protected entities at rest, and prevents unauthorized access to them at runtime. During system operation, TITANIUM authenticates the protected entities, verifying that they have not been altered, and only decrypts files as they are needed. Decryption keys are themselves protected and stored out-of-band to the attacker.

MANDATORY ACCESS CONTROL

TITANIUM simplifies Mandatory Access Control policy creation, requiring policy to only be written for protected applications, libraries, scripts, and data files. TITANIUM defaults to denying access to protected entities. The MAC enforcement engine assumes that the attacker already has administrator-level access. Thus, TITANIUM mandatory access control policies are themselves encrypted and authenticated as part of the secure boot process.

IP AND DATA PROTECTION

TITANIUM ensure sensitive applications, data files, and configurations are cryptographically bound to particular deployment hardware. Thus, TITANIUM prevents an attacker from being able to copy and run applications on non-authentic or instrumented hardware. Further runtime protections include debug prevention, copy protection, unauthorized reading of memory, and protection against unauthenticated code loading into a protected application.

INTEGRITY AND ENFORCEMENT OF CONFIGURATION

TITANIUM verifies signatures and checksums on data and configuration files before they can be accessed by a protected application. TITANIUM also verifies file provenance parameters such as type, location, and filesystem accessibility before allowing a protected application access to data and

OS HARDENING AND ATTACK SURFACE REDUCTION

TITANIUM removes unnecessary OS functionality which could help an attacker analyze system configuration, execution flow, and protected applications. For example, TITANIUM-protected systems do not allow unsigned module loading or process debugging. Unlike SELinux or other security tools, TITANIUM-hardened configurations cannot be modified or bypassed in the field.

SYSTEM HARDWARE ACCESS CONTROL

TITANIUM controls and restricts direct access to system hardware resources, such as peripherals and storage devices. TITANIUM's hardware resource access control policies prevent malicious modifications of the system BIOS and firmware, and enable secure software updates.

Pricing data available upon request. Contact Star Lab to schedule a demonstration.

Technical Specifications:	
Core Functionality	FortiFS file system filter driver (encryption/decryption) Titanium Linux Security Module (LSM) Graphical and command-line packaging & deployment tools
Supported Micro-architectures	All 32 & 64-bit Intel, 32 & 64-bit ARM. Most modern PPC and MIPS processors
Kernel support	Linux kernel version 3.19 and newer
Encrypted File Format	AES-256-CBC, SHA-256 HMAC (auth), ECDSA p-384 (policy signing)
Distro Compatibility	Most Linux distros, incl. RedHat, CentOS, Ubuntu, RedHawk, Yocto-based, RT
Processor/Chipset Features	AES-NI (Intel), VE (ARM), TPM, UEFI
Performance Features	Extremely minimal startup and runtime performance impact
Security Features	Secure Boot, Software Encryption, Anti-debug, OS Hardening, Deprivileged root
Mandatory Access Control	Memory/Process Isolation, SECCOMP syscall gatekeeping, HW Device Protection

Star Lab Corporation
1221 Connecticut Ave NW
Washington, DC 20036

STAR LAB

https://starlab.io
202.706.7027
info@starlab.io