“As cybercriminals are now targeting non-conventional electronic appliances such as battery chargers, mobile phones, smart meters and digital photo frames, companies need to pay even more attention to their security practices.”

Kevin Kwang,
ZDNet

Floodgate Security Framework (FSF) provides engineers developing embedded devices a comprehensive security solution allowing them to build secure, authenticated, trusted devices.

IT security practices require endpoints to be authenticated, trusted, secured and managed before they are allowed to operate on the corporate network. IT/OT convergence and the emergence of security standards in various industries requires embedded devices provide the same security capabilities as IT devices.

The Floodgate Security Framework provides:

- Management system integration for IT/OT convergence.
- Security capabilities to ensure the device is protected from attack.
- Building blocks for compliance with security standards including EDSA, ISA/IEC 62443 and NIST Cybersecurity guidelines.

Cyber Threats for Embedded Devices

Internet-based attacks are on the rise and an increasing number of these attacks are targeting embedded devices. Cyber-criminals, hacking bots, industrial or international espionage agents and even terrorist groups are now targeting industrial, military, automotive and medical devices as well as utility systems.

Reported attacks against industrial devices include:

- Automotive manufacturing plant shutdown resulting from a cyber-attack.
- Pipeline monitoring system that failed due to a DoS attack.
- Train system delays caused by hackers.
- Sewage spill caused by a control system hacked by an insider.
- Proliferation of malware targeting industrial automation systems including Stuxnet, Flame, Havex and BlackEnergy.

Copyright 2015 Icon Laboratories, Inc.
Floodgate Secure Boot Overview

Floodgate Secure Boot provides a critical security capability for embedded devices by ensuring that only validated code from the device OEM is allowed to run. This prevents attackers from replacing firmware with versions created to perform malicious operations.

Secure boot utilizes code signing ensuring the authenticity and integrity of firmware prior to execution. Floodgate Secure boot provides the APIs required for code signing, code validation and secure firmware updates.

Features

- Software APIs to enable secure boot from the initial power on to application execution.
- Hardware root of trust integration.
- Software based vTPM for legacy systems.
- Floodgate Agent integration for secure remote firmware updates.

Root of Trust/Chain of Trust

The concept of Root of Trust and Chain of Trust are fundamental to secure computing. The secure boot process is utilized to implement a chain of trust.

Root of Trust is provided by hardware services including cryptographic support, secure key storage, secure signature storage, and secure access to trusted functions. This allows the creation of a trusted module forming the basis, or root, for validating other components within the system. The first stage boot loader is part of the trusted platform module. From this root, the OS is validated, and from the OS, the applications are validated, creating a chain of trusted elements.

Hardware enabled root of trust ensures the boot loader is trusted and provides the services required for the boot loader to validate the application. The process is repeated at each step in the chain, creating a fully trusted system.
Floodgate Intrusion Detection overview

Floodgate IDS monitors system activity and configuration to detect unauthorized changes to the system. These changes are reported to a security management system. Floodgate IDS supports customizable responses to detected threats, including event logging, alert generation, shutting down the device, operating in “safe mode”, wiping data, and deleting firmware. Engineers integrating Floodgate IDS into their device can select the appropriate response based upon the severity of the threat and the specific requirements of their device.

Run-Time Integrity Validation (RTIV)

The Floodgate RTIV module monitors system files, static data and firmware for unauthorized modifications. Events are generated for any unauthorized modifications and sent to the Floodgate Agent for external reporting. User configurable responses are also supported including shutting down the device, disabling the device, wiping data or operating in a “safe mode”.

Application Guarding APIs

Floodgate Development tools generate Application Guarding APIs and a corresponding unique watermark for each task or application in the system. These APIs are inserted into each task to perform runtime cross-checking of each task’s watermark. This provides an additional level of protection against run-time changes to system executables.

Floodgate Firewall IDS support

The Floodgate Firewall logs security policy violation. These events are utilized by Floodgate IDS to help detect intrusions. Hackers attempting to penetrate an embedded device will probe for open ports and protocols and may send messages from blocked or unknown IP addresses. Floodgate IDS uses these events to help detect unauthorized attempts to access the device.

Secure Device Manifest

Floodgate IDS creates a unique device manifest for each embedded device. The device manifest includes:

- hash value for each firmware or application file
- watermark for each application
- hash value for static files/data
- device specific data (device name, MAC address, Unique ID, etc.)

The initial device manifest is generated at the factory when the device firmware and configuration information is loaded and cryptographically signed for security. The device manifest file is used for local RTIV validation. Integration with the Floodgate Agent allows regeneration of the device manifest after authorized changes to device configuration.

IDS is integrated with the Floodgate Agent, enabling remote audit of the device manifest from the McAfee ePO, Icon Labs Floodgate Management system or other Security Information and Event Management (SIEM) systems.
Floodgate Firewall Overview

Floodgate Firewall is a complete embedded firewall providing a critical layer of security for networked devices. Its unique design provides multiple types of filtering protecting against Internet-based threats:

- Static/rules-based filtering blocks packets based on configurable rules.
- Dynamic filtering/stateful packet inspection (SPI) blocks packets based on connection state.
- Protocol filtering blocks packets based on protocol specific criteria. It provides deep packet inspection (DPI) for industrial automation protocols, allowing control and validation of each individual field within the message, and filtering based on message type, message contents and message source.
- Threshold-based filtering blocks packets based on threshold crossings to protect against denial of service (DoS) attacks, broadcast storms and other packet flood conditions.

Features

- Easily configured filtering rules.
- Ethernet, IP/UDP/TCP/ICMP filtering.
- Protocol specific DPI for industrial automation protocols.
- Layer-based callbacks allow easy integration at any layer in the IP stack.
- Logging of blocked packets/policy violations.

Embedded Firewall Components

Received Packet From Network

SPI Filtering Engine

Log Event
Drop Packet

Block?

Static Filtering Engine

Log Event
Drop Packet

Block?

Threshold Filtering Engine

Log Event
Drop Packet

Block?

Protocol Filtering Engine

Log Event
Drop Packet

Block?

Normal Packet Processing

Firewall Callback Routines

3636 Westown Parkway
Suite 203
West Des Moines, IA 50266
Ph: 515-226-3443
Fax: 877-379-0504
Email: info@iconlabs.com

Copyright 2015 Icon Laboratories, Inc.
Floodgate Agent Overview

The Floodgate Agent enables embedded devices to integrate with security management systems, allowing them to operate as trusted, managed network elements. The Floodgate Agent is designed specifically to run on RTOS-based systems and provide integration with Icon Labs Floodgate Manager, the McAfee ePO management system, or other management systems.

The Floodgate Agent supports policy management, event reporting, remote firmware updates and situational awareness for RTOS based devices. This enables IT/OT convergence as OT devices can now operate as standard, managed IT assets.

Features

The Floodgate Agent is written in portable C code, allowing it to be easily ported to any embedded OS. The Floodgate Agent provides:

- Integration with the McAfee ePO & SIEM
- Integration with Icon Labs Floodgate Manager
- Extensible to allow support for other management systems
- Security policy management
- Event notification
- Event reporting API supports device and application specific events
- Audit log support
- Situational awareness
- Secure remote firmware updates
- Remote Key Management

Secure remote firmware updates

The Floodgate Agent is integrated with the Floodgate Secure Boot and IDS modules to enable secure remote firmware updates. The Floodgate Agent also supports TPM integration for key management and storage of validated firmware updates.

The Floodgate Agent secure firmware update module provides:

- Remote firmware download/storage
- Firmware validation
- Writing validated firmware and signatures to secure flash
- Device restart
- Notification of attempts to install unauthorized firmware

This process insures that only firmware from the device OEM can be installed on the device.
EDSA Certification Overview

ISASecure is a security compliance institute governing the Embedded Device Security Assurance (EDSA) standards and device certification program. EDSA has emerged as the primary security certification for Industrial Automation Devices. Other standards exist both within Industrial Automation and other vertical markets (NERC-CIP, NIST, FDA cybersecurity guidelines, etc.).

Regulator compliance building blocks

Security standards are tailored for the specific requirements of the vertical market they address, but they all share many common themes including:

- Identity management
- Mutual authentication/authorization
- Command audit log support
- Protection from cyberattacks, including protection at the endpoint
- Confidentiality/secure communication
- Availability/protection from DoS attacks
- Attack detection and reporting
- Attack mitigation
- Security policy management

Floodgate Security Framework provides key building blocks to help embedded devices achieve security compliance.

RTOS support

Traditional security solutions don’t meet the needs of IoT and embedded device developers. Floodgate Security Framework is specifically designed for embedded devices used in the Industrial Automation systems requiring EDSA certification. Floodgate Security Framework can support any embedded OS and has been ported to a wide range of RTOSes including VxWorks, Nucleus, INTEGRITY, embedded Linux, µC/OS-III, and RTXC.

EDSA Compliance Support

Floodgate Security Framework provides important building blocks for achieving EDSA compliance for embedded devices. FSF provides support for the following capabilities mandated by EDSA-311:

- App configuration protection
- OS configuration protection
- Executable code insertion protection
- Protection of static data
- Notification of attacks
- Detection of unauthorized changes
- Audit support
- Protocol fuzzing and replay attack protection
- Data flooding protection
- Denial of service protection
- Disabling of unused ports

www.iconlabs.com