ICON LABS

Floodgate Secure Boot

Secure Boot Support for embedded devices

"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

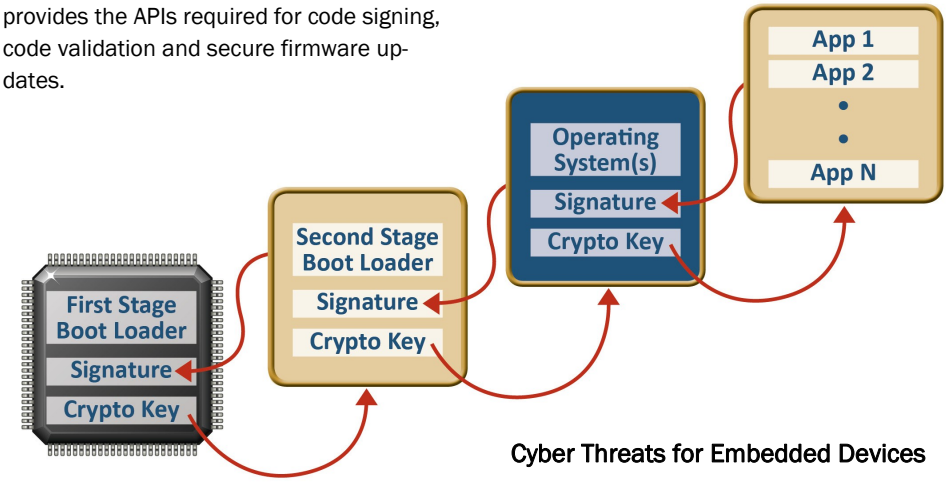
Overview

Floodgate Secure Boot provides a critical security feature 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.



Secure remote firmware updates

Floodgate Secure Boot is integrated with Floodgate Agent to provide secure remote firmware updates. New firmware loads are downloaded to the device using the Floodgate Agent. The agent saves the firmware and validates the new image using the secure boot APIs. Once validated, the agent writes the image, along with the new signature, to flash and reboots the device. This validation process provides checks of the firmware's:

- Authenticity—it is provided by the OEM.
- Integrity—it has not been modified.
- Alerting—if firmware validation fails, an alert can be sent by the Floodgate Agent.

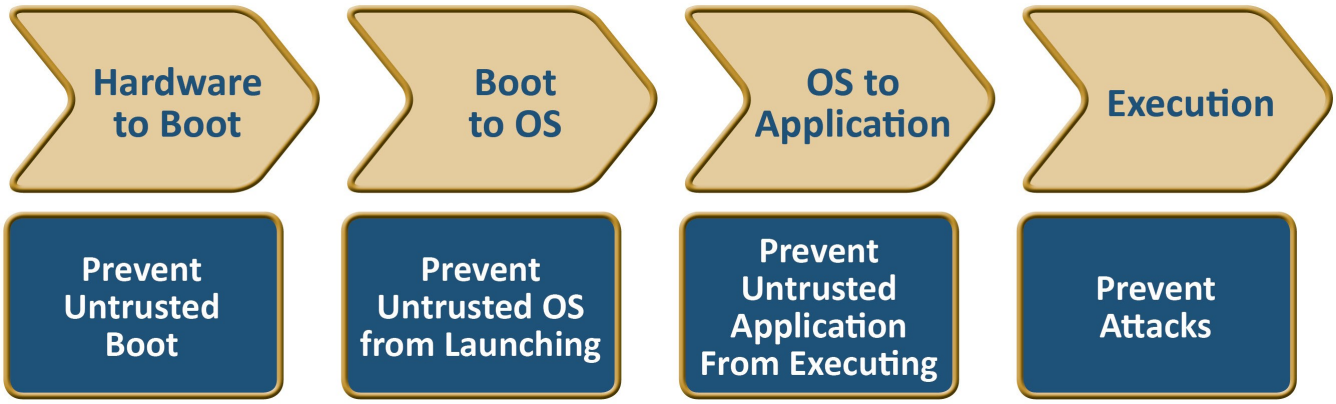
Cyber Threats for Embedded Devices

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

ICON LABS



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 that the boot loader is trusted and provides the services required for the boot loader to validate the application. This process is repeated at each step in the chain, creating a fully trusted system.

EDSA Compliance Support

Floodgate Secure Boot provides an important building block for achieving EDSA compliance for embedded devices. Secure Boot provides support for the following capabilities mandated by EDSA-311:

- App configuration protection
- OS configuration protection
- Executable code insertion protection
- Detection of unauthorized changes
- Audit support

Management System Integration

The Floodgate Secure Boot is integrated with the Floodgate Agent, enabling remote management from the McAfee ePO, Icon Labs Floodgate Management system or to other Security Information and Event Management (SIEM) systems. This integration provides:

- Centralized management of security policies.
- Situational Awareness and device status monitoring.
- Event management and log file analysis.

Intrusion Detection and Prevention

Hackers attempting to penetrate an embedded device often attempt to replace the device's firmware. Floodgate Secure Boot detects and blocks these attacks, and via the Floodgate Agent, reports them to a security management system for remediation.

Most cyberattacks remain undetected until it is too late. Early detection is critical to allow attacks to be contained, blocked and to prevent theft of confidential information, disruption of services or proliferation of the attack to other systems.

In UK supplied by
www.Phaedsys.com

PhaedruS SystemS

Phaedrus Systems
96 Brambling
Tamworth B77 5PG
Ph: 0808 1800 358

Email: info@phaedsys.com

Copyright 2015 Icon Laboratories, Inc.