ICON LABS

Floodgate Embedded IDS

Intrusion Detection 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 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 response to detected threats. Supported responses include 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.

Detecting Intrusions

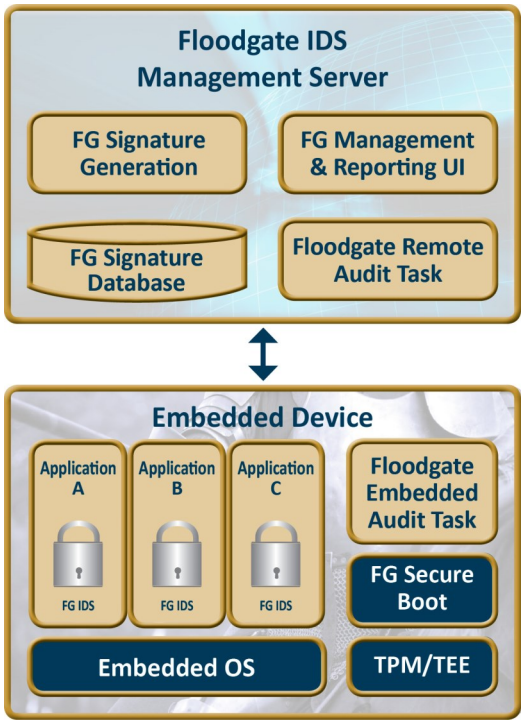
Hackers attempting to penetrate an embedded device using remote attacks will probe the device for open ports and weaknesses. Blocking all unused ports and protocols limits the attack surface potential hackers can exploit. Logging packets that violate configured filtering rules enables detection of unusual traffic patterns, traffic from unknown IP address or other suspicious behavior.

If an attacker successfully gains access to the device, they will frequently make changes to ensure they can access the device in the future. These changes may include modifying configuration files, creating new user accounts, modifying passwords and even modifying the firmware or applications running on the device itself.

Cyber Threats Mitigation

Most cyberattacks remain undetected until it is too late. Early detection is critical to contain, and block intrusions and to prevent theft of confidential information, disruption of services or proliferation of the attack to other systems.

By detecting and reporting attacks against the device, security staff can be alerted allowing them to mitigate and block the attack.



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

Run-Time Integrity Validation (RTIV)

The Floodgate RTIV module monitors system files, static data and firmware for unauthorized modifications. Events are generated for any anuthorized 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 unqiue watermark for each task or application in the system. These APIs are inserted into each task or application and perform runtime cross checking of each task's watermark. This provides an additional level of protection against run-time changes in system executables.

RTOS support

Floodgate IDS is specifically designed for use on embedded devices. Floodgate supports a wide range of RTOSes including embedded Linux, VxWorks, INTEGRITY, Nucleus, µC/OS-III and RTXC.

EDSA Compliance Support

Floodgate IDS provides an important building block for achieving EDSA compliance for embedded devices. Floodgate IDS 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

Harden the Device	Application Guarding APIs & watermarks Cryptographically signed device manifest protects firmware and static data files
Detect Intrusions	Device manifest validation Local and remote audits Boot time validation of firmware Run time validation of firmware & data Detection of firewall policy violations
Respond	Alert/logging Shut down Safe mode Disable the dev ice Wipe data/firmware Customized response

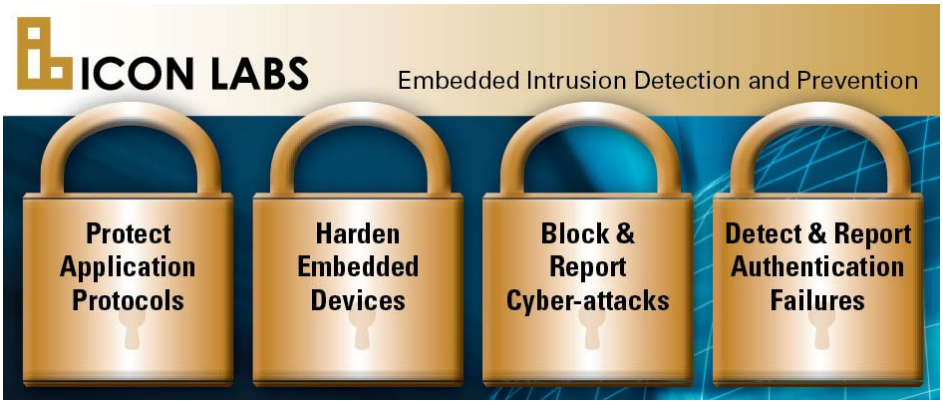
Secure Device Manifest/Remote Audit

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

- hash value for each firmware or application fie
- 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.

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