Application Protection for IoT & Embedded Devices

Comprehensive protection for your most vulnerable assets

The Internet of Things (IoT) is rapidly driving the increase in number of digitally connected devices that are encroaching on every aspect of our lives, including our homes, offices, cars, cities and even our bodies. With the rise of smart phones, cheap sensors/bandwidth/processing, advent of IPv6, ubiquitous Wi-Fi coverage and big data, privacy and security concerns are now more real than ever.

More digitally connected devices mean more attack surface for hackers

IoT devices are an easy target for cybercriminals. Interfacing with the IoT devices are a multitude of 3rd party applications running on the personal mobile devices. A binary library provided by the OEM or a partner typically facilitates communication and sharing of the data resides on IoT devices. These binary libraries are vulnerable to reverse engineering and tampering attacks which can even be detrimental to personal safety.

- Prevent runtime attacks, including the modification of apps and insertion of malicious code
- Prevent unauthorized access to applications
- Prevent reverse engineering of your most critical assets
- Reduce the compromise of critical systems
- Reduce privacy breaches, brand and trust damage
- Guard against revenue loss, intellectual property theft and piracy

Embedded software apps are also vulnerable to code-based tampering and reverse-engineering. From telecommunications and medical devices to automation and digital media, embedded software is among the largest and fastest growing segments, reshaping everypart of the industry.

Risks	Description
Improper or Unsafe Operation	IoT applications/devices are susceptible to malicious code modifications, bypassing of controls and tampering with data integrity
Information Exposure or Loss	IoT applications/devices can reveal protect private information, keys, credentials
Intellectual Property (IP) Theft	Unprotected IoT applications and devices expose embedded proprietary algorithms than can easily be analyzed, stolen, or pirated
Exposure of Unknown Vulnerabilities	Patching of IoT devices is challenging. To prevent exposure to unknown vulnerabilities, it is recommended to make it generally more difficult for hackers to reverse-engineer, analyze, or exploit code
Protecting Security Components	• Many IoT providers have established common security modules that live inside their applications and provide security functionality, including authentication, policies that govern when and how the applications are used, etc. • Arxan protects the logic and libraries used to deliver homegrown and third-party security functionality

Arxan Code Protection to Mitigate the Risks

Arxan Application Protection for IoT & Embedded devices features automated, comprehensive, and customizable protections for software deployed on IoT & Embedded devices. Providing layered defense in depth to the code, it actively defends, detects and deters attempted application attacks, enabling durable and resilient security which makes apps tamper aware and tamper resistant.

DEFEND Against reverse engineering, tampering and any manner of theft

DETECT An attempted attack on the application code, or on another Guard

DETER Attacks with self-repair, custom responses, and alerts or by responding to runtime attacks with customizable actions

Arxan Cryptographic Key and Data Protection

With a robust implementation of white-box cryptography, Arxan's mathematical algorithm uses data and code obfuscation techniques to transform the cryptographic keys and related operations so keys cannot be discovered. The keys are never present either in either the static form orin runtime memory. Arxan protects:

- Static keys – Embedded in an application when it ships
- Dynamic keys – Generated on the fly at runtime
- Sensitive user-data

Arxan Code Protection and Arxan Cryptographic Key & Data Protection work in conjunction to provide a comprehensive Application Protection for IoT & Embedded Devices

Features and Benefits of Arxan Application Protection for IoT & Embedded Devices

- Tunable security for mobile platforms and theirapplications
- Layered network of protections, with no singlepoint of failure
- Self-healing in the event ofan attack by restoringprotections
- Requires no changes to source code
- RASP (Runtime Application Self-protection) measures
- Support for a broad range of emulators anddevices
- Support for the entire Google developmentplatform and other Android platforms
- Support within Xcode
- Support for the ARM processor
- Command line interface to integrate intobuild environment
- Probabilistic, randomized execution foradditional security
- Algorithmically Strong
- Simple APIs for easy integration