Protecting the Internet of Things with Arxan Application Protection for IBM Solutions

Comprehensive data and application protection for connected Internet of Things devices

Connected devices bring new risks

The evolution of connected devices as nodes on the Internet of Things (IoT) brings limitless possibilities. By 2017, the Internet of Things will surpass the PC, tablet and phone market combined, and by 2018 the Wearables, Connected Car and TV markets will equal the tablet market.1

With this connectivity, however comes several security and privacy risks. According to Scott Crawford, Research Director at 451 Research, “the application’s removal from the enterprise datacenter poses a new set of risks for organizations that may already be struggling with application protection. The challenge will only become greater with the explosion of the Internet of Things.”2 The increase in new risks at the application layer can compromise a wide range of critical device systems, the integrity of valuable or private user information, or premium content and payment processing channels. Arxan Application Protection for IBM Solutions is a proven solution for software security of connected devices in the Internet of Things ecosystem. Arxan’s security controls (Guards) protect the critical information contained within the software library, as well as the end application to defend against reverse-engineering and tampering attacks.

Even flawless programming is susceptible to attacks

Even if an application contains no programming flaws, it is susceptible to physical attacks at the binary level, simply because binary code, no matter how unreadable by human eyes, is reversible and modifiable by many reverse-engineering and hacking tools. For example, there are tools available today to easily revert apps back to high-level source code in just a matter of minutes. Releasing unprotected applications, in some sense, is similar to giving away source code and leaving the application’s integrity exposed to compromise.

Highlights

• Provides software security for connected devices in the Internet of Things ecosystem
• Defends applications against reverse-engineering and tampering attacks
• Secures keys with White box cryptography solution protecting information and proving device identity
Proven Arxan and IBM IoT Protection

Arxan protects applications running on the Internet of Things in a number of ways. We protect:

• Mobile apps that control IoT devices
• IoT firmware / embedded applications
• Applications on open IoT platforms

A protected application reduces your risk of:

• Improper or unsafe operation
• Exposure to unknown vulnerabilities
• Privacy breaches and confidential data theft
• Unauthorized access and fraud
• Brand and trust damage
• Intellectual property theft

Use Case Examples

Hackers seek to exploit unprotected Internet of Things applications in a variety of ways:

Connected Cars: The evolution of the connected car as a node on the Internet of Things (IoT) brings multiple security and privacy risks. Arxan has been used to protect hacker exploits on connected cars through infotainment systems, third-party applications and libraries, and service and testing tools.

Successful exploits can result in:

• Compromise to critical vehicle systems
• Theft of private vehicle and user information
• Unauthorized access to premium content and payment processing channels

Connected Wearable Devices (SDK Protection): Wearable devices utilize the API (Application Program Interface) for integration into their products. Mobile apps communicate through the API to collect real-time biometric data and other forms of data. Arxan has been used to protect the SDK by a wearable health software provider, and on a wide range of platforms to mitigate security risks to wearable devices, including preventing runtime analysis and making static analysis very difficult; encrypting sensitive data while on disk and decrypting it at runtime; preventing interception or modification of sensitive real-time biometric data flowing through SDK; protecting the application from modification or unauthorized changes, and preventing IP theft, cloning, and reverse engineering of the SDK and assets flowing through it.

Medical and Healthcare Devices: Arxan provides solutions that are being used to mitigate the risks to healthcare and medical device providers, such as device tampering, intellectual property (IP) theft, preventing patient data exposure, protecting staff and management applications, and protecting security components. A major medical device manufacturer applied Arxan to protect its Pacemaker Controller and Remote Home Monitoring devices from being tampered with.

Connected Homes: Smart Home Appliances, Smart Locks and Smart Home Automation Systems are at risk from hacking exploits that can expose sensitive data or access privileges.

In the case of Smart Home Appliances, Arxan has been used to prevent hackers from bypassing authentication controls to gain access to appliances, prevent hackers from bypassing local encryption to gain access to sensitive data stored within mobile apps, and also protect the mobile app from reverse engineering and disclosing information from backend systems.

In the case of Smart Locks, Arxan has been used to prevent the mobile app by mitigating the threat of unauthorized door unlocking, preventing the application from sending the electronic key to unauthorized users, safeguarding the electronic key/certificate stored on the device with state-of-the-art cryptographic key protection technology, mitigating eavesdropping threats so the communication between the phone and the lock is completely secure, and preventing communication with the server for nefarious activities or to obtain server data.

Smart Home Automation Systems deliver video, audio, lighting, climate, and security controls into a single mobile interface, allowing connectivity with virtually any smartphone, tablet or computer. This wide range of functionality also exposes a wide range of hacking vulnerabilities. Arxan has been used to prevent reverse-engineering of code that initiates sessions which load/decrypt/play music, prevents hackers from performing runtime analysis of code that decrypts music and starts a session, prevents hackers from attaining decryption of a key at runtime or performing static analysis of a key, prevents hackers from modifying the code that retrieves, processes, or streams music content, and prevents music piracy without a material impact on performance or speed.

Industrial Internet: Arxan has been employed by a leader in wireless vehicle detection systems that use wireless road sensors to detect vehicle presence and movement, providing accurate, dependable, real-time data for region-wide roadway optimization. The valuable assets that Arxan protects include intellectual property (IP) and hardware-binding, and Arxan safeguards these assets by mitigating the threat of bypassing security controls, preventing device cloning, and protecting proprietary code.

Arxan protects over $200+ billion in market value of assets in a wide range of IoT companies:

• A telecommunications equipment manufacturer with $127+ billion in market value
• A Fortune 100 global electronics company with $25+ billion in market value
• A medical equipment and device manufacturer with $61+ billion in market value
• A leading provider of automation and control solutions with $402+ million in market value
• A wearable health software provider with $10+ million in market value
How Do We Do It?
To defend against these attacks, Arxan works at the binary and object-code level. Without changing source code or disrupting software development, Arxan provides tamper resistance quickly and easily by embedding a collection of interdependent protection routines, called Guards, directly into a program, and then by obfuscating or scrambling the result. The Guards, which appear to be normal code, enable the program to defend itself, to know if it’s been attacked, and even to heal itself if it is modified. This way hackers cannot make unauthorized changes to program functionality to exploit performance parameters or insert malware.

Arxan’s approach is unique in that we:
• Offer the highest level of security in the market, given our approach that involves establishing a multi-layer, interconnected Guard Network
• Provide a solution that is proven in the industry
• Provide an easy and scalable approach to implementation
  – Involves no changes to source-code
  – Is easy to integrate into legacy applications
  – Involves automated insertion of self-protecting code

Recommended by Industry Analysts
IoT protection solutions are acknowledged by security analysts and security organizations as an important aspect of application security:
• OWASP: “Insecure Software/Firmware” identified as an Internet of Things Top 10 Risk.  
• 451 Research: “Application hardening and run-time protection is a critical component in the strategy to secure enterprise software, embedded systems, mobile apps and the much-b bandied ‘Internet of Things.’”

Supported Platforms
Arxan offers cross-platform support to ease adoption and enable standardization. This includes a diverse set of programming languages (C, C++, Objective C/C++, .NET, Java, HTML5/Javascript, etc.) and the following platforms:
• Android
• Apple
• Windows
• BlackBerry
• Tizen
• Linux
• Intel
• PowerPC
• ARM

Arxan solutions have been tested by and integrate with the IBM Security Portfolio.

For more information:

1 Business Insider, BI Intelligence Estimates, July 2015
2 451 Research, April 2015
4 451 Research, April 2015