August 2015

Response to OTA draft
IoT Trust Framework

Stephen McCarney
Arxan Technologies

Arxan Technologies, 6903 Rockledge Drive, Suite 1250
Bethesda, MD 20817

Arxan applauds the efforts of OTA and its members in drafting a trust framework for IoT. Arxan provides the world's strongest application protection solutions for some of the most reputable companies, and our solutions are currently strengthening privacy and security of applications on more than 400 million devices. Arxan was recognized as the 2015 winner of the IT World Awards for Application Protection of the Internet of Things, and as a 2015 finalist for Best IoT Product by CSI. We share this brief introduction to Arxan not in the spirit of self-promotion, but merely to help highlight that we are on the front lines of application security in IoT, we understand very well the threats to consumer privacy and security, and we can offer valuable insight into the IoT trust framework.

We recognize that our response is reacting to a thoughtful output from a collective meeting of the minds at OTA. We hope that this response is only the beginning of more proactive engagement with OTA and the ITWG. We appreciate your consideration of two security measures – code hardening and key protection – which are critical IoT application protections that complement a preventive, holistic approach to security and privacy. We recommend that this **proposed minimum requirement be added after #11** in the current draft framework as such:

Proposed Minimum Requirements

11. Manufacturers must conduct penetration testing for devices, applications and services. The objective is to help identify and patch vulnerabilities. Ideally such testing should be independently verifiable.

12. Manufacturers must harden the code of IoT applications and protect the application's cryptographic keys to prevent reverse-engineering, code tampering, and cryptographic key discovery.

13. Manufacturers must have capabilities to remediate vulnerabilities in a prompt and reliable manner either through remote updates and / or through consumer notifications and instructions. Alternatives could be device replacement or manufacturer upgrade, product recall or onsite service for connected home devices. It is recognized some embedded devices' current design may not have this capability and it is recommended such update / upgradability capabilities be clarified to the consumer in advance of purchase.

What Are Application Hardening and Key Protection, and Why Are These Measures Essential for the IoT Trust Framework?

Application Code Hardening

In the current IoT Trust Framework draft, #11 focuses on pen testing – and rightfully so. However, even if an application contains no programming flaws, it remains vulnerable at the binary level, because binary code -- no matter how unreadable to human eyes -- is easily reversible and modifiable by many reverse-engineering and hacking tools. There are tools available today to easily revert apps back to high-level source code in just a matter of minutes. Therefore in many situations, releasing improperly protected applications is equivalent to giving away source code. Application code hardening prevents reverse-engineering and tampering by embedding a collection of guards directly into the binary

code before applications are released. This can be done without changing source code or disrupting software development. The guards, which appear as normal code, enable the application to defend itself, to know if it is attacked, and even to heal itself if it is modified. This way hackers cannot make unauthorized changes to application functionality, to exploit performance, or to insert malware.

Key Protection (White-Box Cryptography)
Access to digital content, data, and information systems is commonly protected by encryption, a first line of defense. Encryption is a prevalent security component in the draft IoT Trust Framework. However, encryption has a single point of failure – the instance at which the decryption key is used. Keys are the critical component for securing systems, communication and applications, and therefore must be protected at all times. Without proper key protection, signature patterns and cryptographic routines can be used by an attacker to easily navigate to where the keys will (typically) be constructed in memory. Subsequently, fatal exploits can be easily executed.

White-box cryptography (WBC) provides a secure implementation of cryptographic algorithms in an execution environment, such as on a desktop computer or a mobile device, which is fully observable and modifiable by an attacker. White-box cryptography is intended for any security system that employs cryptographic algorithms and keys, and that is executed in an open and untrusted environment. This protection combines a mathematical algorithm with data and code obfuscation techniques to transform the key and related operations so keys cannot be discovered. The keys are never present either in the static form or in runtime memory (mitigating memory scraping).

What both application code protection and key protection mean for the consumer is that the IoT applications they are using can be trusted to perform as they should and they can be trusted to protect the privacy of their sensitive data.

Real Examples of How Application Code Hardening and Key Protection are Used in IoT

Some of the world's leading IoT manufacturers are using code hardening and key protection to strengthen security and protect privacy. Here are just two examples where companies are using these security measures in the connected home arena:

Use Case #1

- Users control home appliances with a mobile phone app remotely via a cloud server
- Security and privacy concerns include:
    - Hackers can bypass authentication controls to control appliances
    - Hackers can bypass local encryption to gain access to sensitive data stored within the mobile app
    - Hackers can reverse-engineer the app to expose information for backend systems
- These security and privacy concerns are mitigated with the use of application hardening – the insertion of self-protection guards into the binary

Use Case #2

- Electronic locks for the home allow users to lock/unlock doors from an Android or iOS mobile app
- Security and privacy concerns include:
    - Hacking the application to make it unlock a door even if the user is not logged into the app
    - Getting the electronic key/certificates stored on the device
    - Hacking the application to send keys to outside users
    - Snooping of the Bluetooth communication between the phone (device) and the lock
    - Hacking the app and making the app maliciously communicate with the server to obtain server data
- These security and privacy concerns are mitigated with the use of application code hardening and white box key protection security measures

More Information and Contact Details

Thank you for your sincere consideration of this recommendation. More information about Arxan and our involvement in connected homes, wearables, and other IoT industries and can accessed here. We are also happy to connect in person (based in the DC metro area) or by phone: 301-968-4295.

Cheers,

Stephen McCarney
Arxan Technologies
smccarney@arxan.com
301-968-4295
www.arxan.com