Cybersecurity in IoT: Challenges and emerging technologies

Summary

IoT will impact many highly diverse sectors and applications. Levels of security will need to be risk based, but there will be underlying common security concerns. A major problem is the fragmented IoT software development ecosystem, with no agreed approach to IoT security. ARM is aiming to address this through its mbed suite of products. Certain applications will need a hardware root of trust (e.g. TrustZone). We support FIDO as a password-less approach to identity authentication.

Introduction

ARM welcomes this opportunity to respond to the RFI on cybersecurity challenges. Our focus is on security in the IoT space. We have tried below to show how we are developing technology to help address the challenges.

We have not organised our response explicitly around your specific questions, but a number of those questions are addressed implicitly or explicitly in thetext.

ARM is a UK Headquartered company, part of the Softbank Group, with a strong global presence. Our core business has been the design of microprocessors and related activities. Our designs are best known for their pre-eminence in the cell phone and mobile sector, but they are also increasingly being taken up in many other sectors, including IoT. The energy efficiency of our designs has been a key factor in our success, which we expect to take into the IoT world. It is clear that many of our designs are already going into IoT products.

Our devices are also starting to be used in servers and data centres.

IoT

Many commentators predict that IoT will have a huge impact on many areas of life. These will include transport, e-health, infrastructure, predictive management of capital equipment, as well as the connected home. It holds out the prospect of enabling society to manage resources more efficiently and to deliver services more effectively. Estimates of the number of connected devices are high: Gartner estimates 20.6 billion by 2020.

Security will have a key part to play in protecting this network of connected things and the data they handle from unauthorised access.

.

Data *security* in an IoT world is to be distinguished from data *protection*: the former is about securing data in storage or in transit from interference or unauthorized view; the latter is about ensuring that those who receive your data in an authorized way, can only do with it what you are comfortable for them to do with it.

This paper is concerned with data security: an area where the emerging technology can help.

IoT Security comprises three broad aspects: (i) device security (ii) communications security (iii) provision of upgrades over the air. All three are essential.

Our goal should be to create an IoT world where security is built in at the design stage. We refer to this as security becoming a 'hygiene factor'. Progress is being made but we are not there yet.

At the same time, we need to recognise that IoT security will need to be risk and value based: not all devices will need to have the same level of security protections in place.

The level of security may have to be tailored to the specific application domain.

Of course, all devices connected to the Internet will have common security needs, at least from the point of view of communication security. But there are differences in terms of how much protection is needed for data (particularly keys) stored on those devices (particularly concerning the resilience regarding physical attacks). The problem with thinking that certain devices (such as light bulbs) need much less security protection than others is that a compromise of such devices can still lead to a lot of harm to others. Examples of such harm are distributed denial of service attacks.

So much will depend on what the devices are doing, where they are located, and what information they are handling. It is often said that in any complex product (like a car) it might be possible to use a less secure system (like the entertainment system) to manipulate other more important systems in the vehicle. The solution for this is to have proper ways of separating the systems, or gating the communication between those different systems.

Providing IoT security requires a certain amount of computing power in the devices at the edge. We believe that the computing capability of our key IoT relevant CPUs (the M3 and M4) provides sufficient memory and resources to produce effective security e.g. through the ability to encrypt data on the fly at a sufficient speed, or store the data in encrypted form in a protected area.

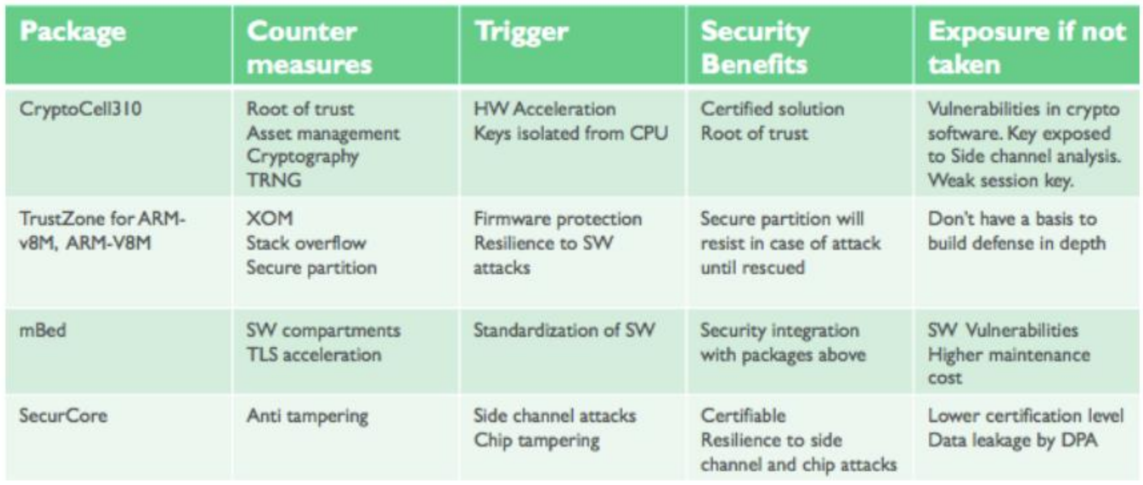
A major problem in the IoT world is the fragmented software ecosystem. There are many developers, and many alliances. Not all of them are transparent about the security they employ. This may derive from their view that it is safer not to disclose details of the security arrangements. This is not a view we share: we believe that overall IoT security would be enhanced by greater openness in this area. This would encourage challenges to software security systems, in, we hope, a constructive spirit of trying to improve them.

We need to create a common software framework across IoT.Of course there are questions about what this might entail: Should we all use only one implementation or should we use common standards but many implementations ? ARM is helping to address this through mbed and in the future will be able to put more functionality into Systems on Chips (see comments below on ARMv8-M).

Another aspect is the need to address the problem of the speed at which software becomes outdated. In the case of vehicles for example, the vehicle itself might have a lifespan of 12 years, whereas the software running it will have a life of probably only a couple of years at most, and the complexity of the software means it will probably have bugs in it which need to be fixed. This underlines the point that regular OTA upgrades are essential.

An Overview of ARM’s approach to IoT Security

ARM packages security technology into various building blocks: mbed OS, Trustzone, Cryptocell and SecureCore. These blocks cover both software and hardware elements. These are a foundation for IoT node security. The following table explains them :



Package	Counter measures	Trigger	Security Benefits	Exposure if not taken
CryptoCell310	Root of trust Asset management Cryptography TRNG	HW Acceleration Keys isolated from CPU	Certified solution Root of trust	Vulnerabilities in crypto software. Key exposed to Side channel analysis. Weak session key.
TrustZone for ARM-v8M, ARM-V8M	XOM Stack overflow Secure partition	Firmware protection Resilience to SW attacks	Secure partition will resist in case of attack until rescued	Don't have a basis to build defense in depth
mBed	SW compartments TLS acceleration	Standardization of SW	Security integration with packages above	SW Vulnerabilities Higher maintenance cost
SecurCore	Anti tampering	Side channel attacks Chip tampering	Certifiable Resilience to side channel and chip attacks	Lower certification level Data leakage by DPA

These security features are designed to work together to provide a comprehensive solution:

- The device boots with trusted software remaining in ROM
- Asset management coupled with strong cryptography ensures that the latest firmware is transferred and installed safely on the device
- XOM (Execute Only Memory) ensures software asset protection so that code simply cannot be copied.
- Stack overflow helps protect against software attacks.
- True random number generation ensures a strong session key is generated
- TrustZone for ARMv8-M facilitates software partitioning between secure and non secure helping to ensure that the firmware, private keys and secure identities are not exposed to external attacks.
- Firmware Over the Air (FOTA) allows software to be upgraded /restored after a known attack.
- Tamper resistant chips like ARM SecurCore offer resistance against attacks deriving from side channel analysis and chip tampering.

ARM’s mbed Platform

Although the IoT market will be made up of many vertical segments, most applications that can make use of Internet connected services have a common foundation. For example – smart cities, basic wearables and smart home devices require basic OS functionality like drivers, device security and provisioning support. Network connectivity may vary from application to application, but in general the IP networking, security, application layer and device management needs are all common.

The ARM mbed IoT Device Platform provides all the key ingredients to build secure and efficient IoT applications through ARM’s mbed OS, mbed Device Server and mbed Community Ecosystem.

The mbed Platform has two components: at the device level there is the mbed OS running on system-on-chips. This works as a standard OS, running the drivers, managing the hardware and communications, controlling the device.

The second component is on the server side, where there is software called mbed Device Connector (or mbed Cloud) that runs on any server whether powered by ARM or not. This helps the server manage the data coming from the devices. It can operate through a gateway which links to devices through short range communications.

The ARM mbed Device Connector lets developers connect IoT devices to the cloud without having to build the infrastructure, while providing the security, simplicity and capacity developers require to prove IoT applications at scale.

IoT needs complexity to be managed in order to scale up to billions of devices. mbed OS is designed to be a platform operating system, containing a core, security, and key IoT networking and communication technologies. mbed OS helps bring security by design into IoT by allowing developers to focus on application code, not underlying complexity.

ARM’s mbed OS

Operating systems have a key role to play. Currently we are seeing developers playing around with low level RTOS. This will not produce the security by design we are aiming at.

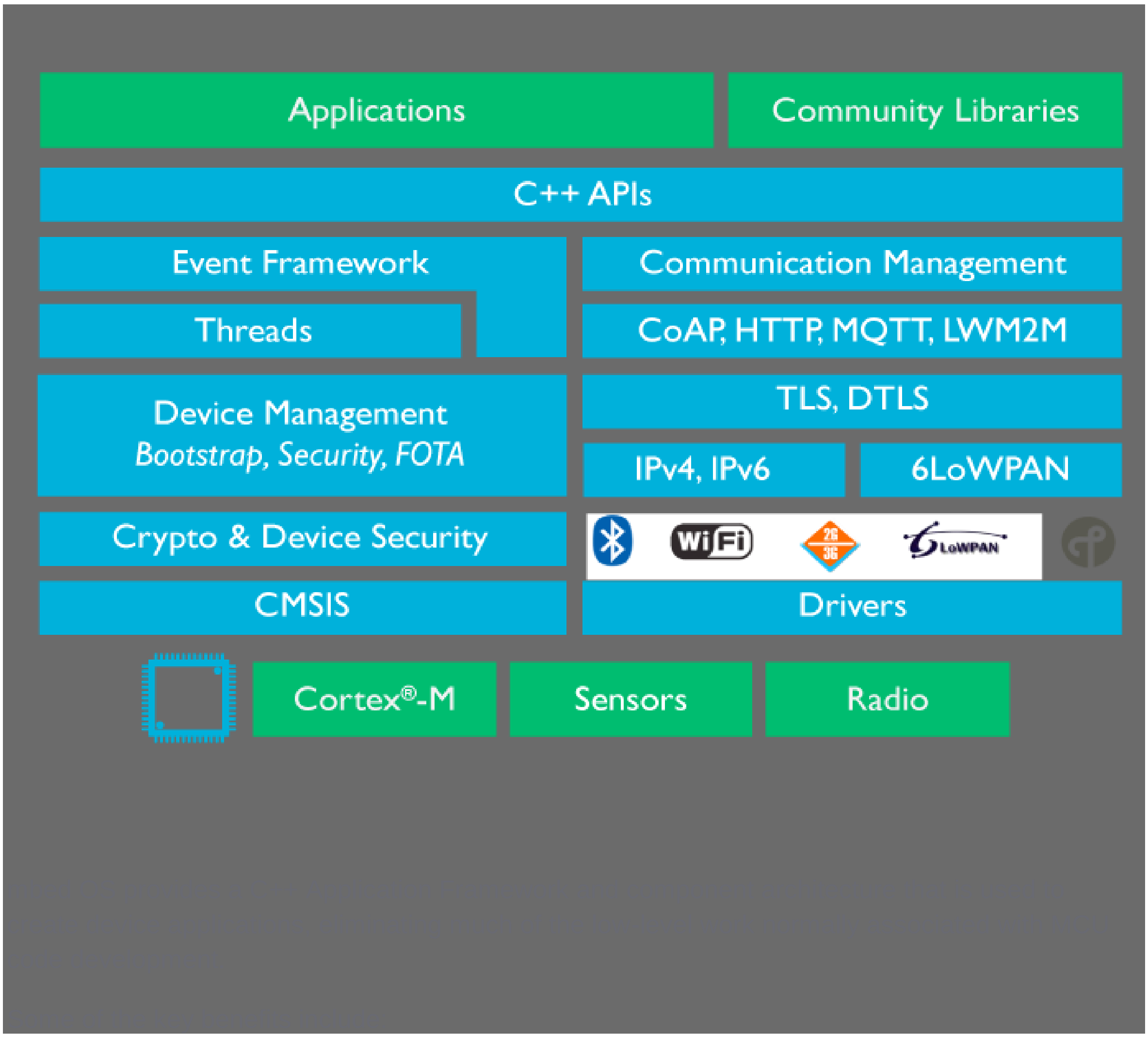
Our mbed OS is designed to address this, by providing an OS which will take care of the security management of a device (and other aspects like communications), leaving the developer free to build a device with security baked in.

mbed OS is a full stack OS. It addresses security in device hardware, software, communication and in the lifecycle of the device itself. It tries to solve many of the Internet of Things (IoT) security problems using standardized building blocks. Alongside robust communication stacks and safe firmware updates, mbed offers two security-specific building blocks: mbed TLS and mbed OS uVisor.

Hardware Enforced Security At the lowest level of mbed OS, is a supervisory kernel called uVisor to create isolated security domains which restrict access to memory and peripherals.

Communications Security mbed OS takes SSL and TLS, the standard protocols for securing communications on the internet, and allows developers to include them in mbed projects with a simple API.

ARM mbed TLS makes it easy for developers to include cryptographic and SSL/TLS capabilities in their embedded products, facilitating this functionality with a minimal code footprint. It offers an SSL library with an intuitive API and readable source code, and includes a comprehensive test suite.



TrustZone

ARM TrustZone Technology is a System on Chip and CPU system-wide approach to security that is used in billions of chips to protect valuable devices and services in a wide range of markets.

TrustZone security extensions allow a system to be physically partitioned in secure and non-secure components. This provides further isolation of assets and can be used to ensure that software operating within the normal operating system cannot directly access secure memory or secure peripherals.

The TrustZone based Trusted Execution Environment provides a ‘Trusted World’ where the security boundary is small enough to offer a route to verification and provable security. It is typically used for securing cryptographic keys, credentials, and other secure assets.

TrustZone works by providing the processor with an additional ‘secure state’ which allows secure application code and data to be isolated from normal operations, by only allowing execution of secure code or access to secure addresses. The dedicated secure operating system, the TEE works together with conventional operating systems such as Android or Linux to provide secure services. Interfaces for access to the TEE are being standardised by Global Platform.

ARMv8-M architecture extends TrustZone technology to Cortex-M class systems such as microcontrollers, enabling robust levels of protection at all points. TrustZone for ARMv8-M has the same high level features as TrustZone on applications processors but with the added benefit that switching between secure and non-secure worlds is done in hardware for faster transitions and greater power efficiency.

The ARM V8-M architecture reduces the complexity of developing secure embedded solutions for IoT.

A Role for Government?

The majority of the IoT market is not currently regulated. But some key areas where IoT has a role, like health, automotive, smart cities and infrastructure are prone to regulation for various reasons. One reason for regulation may be where the primary benefit is a public one, like the prospect of zero road deaths which connected transport might deliver. Another could be the risk of serious adverse consequence for a wide range of people if things go wrong. As an example a simple medical device like a glucometer could be the entry point to a hospital network and therefore a regulator may want to insist on stronger security solutions. The difficulty in this area of course is the risk that specific regulation quickly falls behind the development of the technology. It is to be expected that IoT security will in any event become a competitive differentiator in the market place.

A Note on Identity Authentication

Your RFI also requests views on identity authentication.

Many commentators recognise that Passwords are becoming increasingly inadequate in offering adequate security. Even one time passwords have problems: although they improve security they are not easy to use and not immune from vulnerabilities.

We are supporting the FIDO (Fast Identity Online) approach. In essence this requires the subject to authenticate themselves to their device in a variety of ways. The device then authenticates the user online using public key cryptography. If biometric data is used in the first stage, it never leaves the device.   No 'secrets' are kept on the server side, reducing the risk of linking services or accounts if security is compromised.

FIDO has been designed with the user experience primarily in mind, and aims to make authentication as easy as possible.

The FIDO Alliance is supported by a variety of companies and other organisations from different sectors.

Further Information on FIDO can be found at :
https://fidoalliance.org/resources/FIDO__Privacy_White_Paper_Jan_2016.pdf

We have also participated in relevant work at the IETF. See
https://datatracker.ietf.org/wg/oauth/charter/
https://datatracker.ietf.org/wg/ace/charter/

ARM August 2016