NTIA Consultation on Botnets etc

Introduction

ARM is a global leader in the design of micro-processors and associated products**.** There are currently some 100 billion ARM designed chips in circulation.

ARM also develops OSs (mbed OS, Keil RTX, and OP-TEE), Internet protocol stacks, IDEs, and offers a device management solution that includes a firmware update mechanism. Not only do we release our OS as open source (under an Apache 2 license) but also our security stacks (e.g., mbed TLS, mbed client).

There is much interest in the area of IoT Security. We have sought in this submission to give you an idea of the technology ARM has developed for improving the security of IoT and to explain one of the public policy approaches currently under consideration by the IoT Security Foundation, with which ARM has been involved.

Gaps and Impediments to closing them

There is at the moment no overarching direct, legal responsibility for the security and safety of connected devices. (Although there are measures which seek to address some of the problem eg on privacy (which includes security as a subset), measures against deceptive and unfair business practices, and special measures in some specific sectors (financial sector, healthcare, etc.)

One problem with security is that it adds a cost layer which, at present, it is not clear that the market will meet. This is compounded by the fact that the IoT Sector comprises so many diverse players.

It may be that some of these players have a strong interest in promoting security:

(i) For example, some network operators, faced with reputational and economic damage, may insist on security standards in order to get access to their networks. Some are already pushing their own solutions as a way to secure IoT and to reduce the impact of botnets. But it is not however at present clear that this will be effective and will further interoperability. Network operators may not be best placed to offer specific solutions and they have a mixed track record of solving internet security problems.

(ii) Insurance companies may refuse to insure large clients unless they comply with defined industry practices.

(iii) Some product manufacturers will introduce new, more secure, features which will be taken up as much for their usability as for their security value: for example the introduction of alternatives to passwords might find wide acceptance among consumers as an attractive, more useable, feature in its own right, as well as something which improves security.

The challenge is to encourage behaviours which elevate the importance of security while minimising the potential barriers such as lock in, substantial cost and effort of building in security processes and capabilities.

Against this background our view is the IoT Sector needs to build security into IoT.

ARM is aiming to drive this. If we want to make IoT devices more secure then we need to get OEMs to improve the security of their devices. ARM aims both to provide technical direction but also to encourage market pull for more secure devices.

Promoting a firmware update solution is in line with NTIA efforts (see https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security) and the only way to fix security problems. ARM has contributed its IoT firmware update design to the IETF, see https://tools.ietf.org/html/draft-moran-fud-architecture-00 and we make our OS and protocol stack available to developers (as open source).

Since we are aiming to make it easier for companies to develop secure IoT products we have released our standards-compliant device management implementation as open source code under an Apache 2 license (see mbed client [link below]). This device management solution is an implementation of the Open Mobile Alliance (OMA) LwM2M protocol, which among key provisioning also offers the possibility to convey firmware updates to IoT devices. A device management solution is suitable for those companies that prefer a complete security solution rather than a laundry list of best current practice recommendations. It is a kind-of one-stop-shop solution.

Key links for further information on our offerings:

- Mbed OS: https://github.com/ARMmbed/mbed-os
- Mbed Client: https://github.com/ARMmbed/mbed-client/
- Mbed TLS: https://github.com/ARMmbed/mbedtls

Secure By Default

Security is of course not a clear cut issue: one size will not fit all situations. Any effort at promoting security has to recognise this. It is also an evolving challenge, and will continue to evolve.

ARM believes that having a common language to talk about these issues is an important first step.

ARM is already taking inputs from across the industry and is bringing them together into an architecture specification.

ARM wants to build on industry collaboration on addressing these problems using recognised secure building blocks such as:

- Strong device level security isolation and compartmentalizing on even the most constrained devices . (See our recent launch of TrustZone for v8-M :http://www.arm.com/products/security-on-arm/trustzone).
- Simplifying development with device and server side cryptographic and SSL/TLS capabilities (+ device development with strong entropy)

- Building devices / endpoints capable of secure firmware updates over multiple network infrastructures and protocols
- Securing the manufacturing chain through best practices in trusted device identification, device on-boarding and service provisioning.

One option would be to look at the possibility of Industry and government collaboration on best practices around how secure firmware campaigns can practically be carried out. Such best practices would allow companies to reduce the costs of wasted campaigns, bricked devices, over-all costs of customer or consumer loss of confidence, and repair or crisis management for critical services.

In short: we believe that IoT security can be improved by improving security of the IoT devices themselves. This requires a solid firmware update mechanism to be implemented by OEMs. To relieve developers from re-implementing Internet protocols and security algorithms we recommend the use of off-the-shelf (freely available) IoT operating systems and protocol stacks. Finally, using state-of-the-art hardware security mechanisms IoT device security can be substantially improved.

Policy and the Role of Government

Various bodies are currently looking at how best to promote a higher standard of security among IoT players. The problem they are all trying to avoid is unnecessary regulation which risks freezing security at one moment in time, when in fact it is likely to be a fast evolving concept.

The IoT Security Foundation (IoTSF), with which ARM is involved, has developed a scheme which in essence provide a list of best practices in terms both of product design and operational practices in companies working on IoT devices.

The IoTSF Compliance Framework was published in December 2016 see https://iotsecurityfoundation.org/best-practice-guidelines/ .

This draws widely on best practise identified in a number of studies and other proposals. It aims to draw on industry best practice, and to integrate

ideas. It has the advantage of having been drawn up by a group including academics as well as industry professionals, and not dominated by any one company or group of companies. The IOTSF will be responsible for ensuring revisions to the Framework as issues arise or technologies evolve.

The IoTSF aim is to drive acceptance of the Framework through a mix of self-assessment and possible third party assessment.

The key elements of the scheme are:

- Companies should use the Foundation's recommended best practice as benchmarks in the development, manufacturing, test, and support processes;
- They should conduct internal self-assessments using the IoTSF Trust Framework throughout the product or service life cycle;
- They need to maintain the documentation and evidence gathering process throughout.

Through the self-assessment approach companies will be able to identify gaps they have in their processes and technical capability.

The goal is to establish a "Supply Chain of Trust" (SCOT).

The basic ideas behind this are as follows:

When a company in the supply chain develops and/or operates a product or service, they necessarily procure components from other suppliers.

- For example, a device maker may use an off-the-shelf OS running on an embedded processor. The device security may be seriously compromised by vulnerabilities in the software.
- Similarly, in implementing the device, its security may be compromised by poor practice by the maker, such as the use of default keys or leaving test interfaces open.
- Even if a product uses a secure OS and follows good practice in design and development, its security may be compromised after deployment as new exploits are discovered. Recovery from this requires good processes and designed-in security update procedures.

Thus a company procuring a component for use in its product/service ideally needs to apply rigorous security due-diligence to its suppliers.

In the above example this would apply to the OS supplier, and to any entity purchasing the whole product from its maker.

Supplier / customer relationships in the supply chain are *contractual*; either there is a bespoke contract in place or a set of standard terms and conditions of sale and purchase. These contracts commonly make stipulations about conformance to standards for performance, safety, and quality, and provide an enforcement mechanism. They could be enhanced to include security.

If a company in the IoT supply chain can enter into agreements with its suppliers and customers that include provisions relating to security; and/or can apply suitable due-diligence to its suppliers; it should become possible to ensure, as best we can, that the end product or service is and can be kept secure.

So the fundamental concept behind SCOT is to provide a framework that companies can use to embed security in their purchasing and supply arrangements.

These two aspects working together, if applied by each actor in a supply chain appropriately for the component being procured, enable a trusted supply chain to be built.

But this might be onerous for some companies, since the implication is that a procuring company has to apply the assessment process to each supplier, and the supplier has to be able to respond to the assessment. The latter might involve a supplier disclosing confidential commercial information, which he might not even have the right to do if it covers third-party relationships.

Hence the IoTSF is floating the additional idea of a certification process.

A company may submit its internal processes and/or their application to a specific product to assessment by a Trusted Third Party (T3P), such as an accreditation house, to obtain the **IoTSF Trustmark**. This can then be recognised by its customers that the supplier follows good practice; and recognised as such in contract documentation. Use of the Trustmark is subject to rules: the company must be an IoTSF member in good standing; there may be a recurring charge for its use; re-inspection may be possible; and the usage is subject to revocation in various circumstances.

Will a Voluntary Chain of Trust Scheme suffice?

Some have argued that alongside the idea of establishing a common set of security criteria, consideration should also be given to some sort of Trust Label. This, it is claimed, will make it easier for customers to decide if a product meets certain key standards.

The problem of course is what will such a label actually testify to? Should it be linked to compliance with a number of criteria as in the Framework above? Or should it be limited to compliance with a specific key criterion, such as for how long the product will be supported with upgrades?

Or maybe it could reflect both, but highlight the latter (length of support) as potentially the most crucial factor for some potential customers? These issues are being debated in various fora internationally.

It is probably worth starting by trying to drive voluntary take up of a scheme designed to promote stronger demand for secure IoT. Even where third party certification is not used, it may be that bodies such as the FTC in the US (or similar bodies elsewhere) would help tackle companies who falsely advertised compliance with such scheme.

Government working with others

It might help to outline the core elements of how the IoT SF sees its scheme as operating in the UK context alongside Government players:

- **UK IoT Security Principles** – this would be an overarching high-level UK framework for IoT security adoption across UK consumer sectors. This could be Government sponsored but not legally binding.
- **IoT Security Compliance Framework** – UK cross-sector developed and dynamically (at least annually) maintained detailed best practice/essential practice set (IOTSF Framework). Reviewed and contributed to by key Government Agencies.
- **Certification and Testing** – consistent approach supporting IoT Security Framework via self declaration (audited) and independent testing using existing test labs processes.
- **Sector IoT security use cases and application guidelines** – specific goal setting for specific industry sectors/retail sectors drawing from

IoT Security Compliance Framework in cooperation with representatives of key sectors.

- **International Recognition** – set of chapters and cross-recognition arrangements to have IoT Security Framework adopted internationally.
- **Standards Bodies** – Integration of more static and under-pinning elements of IoT Security Compliance Framework into emerging IoT security standards as either standalone or embedded in specific industry standards. These will operate at the (slowish) speed of standards processes, which might be too slow for the evolving IoT world, hence the importance of a more agile IoTSF style Framework.

ARM July 2017