Security Foundation

Internet of Things Security Foundation

Make it safe to connect

ESTABLISHING PRINCIPLES FOR INTERNET OF THINGS SECURITY

SECURITY FIRST APPROACH

...designed in at the start

FIT FOR PURPOSE

...right sized for the application

RESILIENCE

...through operating life

Contents Table

- Does the data need to be private?
- Does the data need to be trusted?
- Is the safe and/or timely arrival of data important?
- Is it necessary to restrict access to or control of the device?
- Is it necessary to update the software on the device?
- Will ownership of the device need to be managed or transferred in a secure manner?
- Does the data need to be audited?

Foreword

By John Moor, Managing Director, IoT Security Foundation

Much has been said about the potential of IoT. So much so that it is has been featured at the peak of inflated expectations on Gartner's hype cycle for quite some time. As the hype inevitably subsides, the reality of delivering the benefits of IoT grows, and the initial excitement turns to concern. Challenges around security and privacy have moved beyond technical consideration and have now entered board room discussion - get them wrong and it could be the end of the business... really.

Whilst cyber security is well understood amongst computing professionals, the attraction of IoT is drawing interest from new comers from all quarters who are significantly less familiar with contemporary best practices or even the full implications of a breach. Your insecure product may not be the ultimate target but could provide the pivot point for an attack elsewhere in the system.

Cyber security is also a moveable feast - what is deemed secure today may not be tomorrow. We can expect more of the same to apply as IoT applications emerge and mature. There is already a growing number of new-to-security practitioners who are just starting to realise the scale of threat that adding connectivity to their product brings. Introducing security vulnerabilities into a network can create unintended consequences for anybody connected to it and therefore anybody looking to connect has a duty of care towards others. Whilst ultimate security will likely remain elusive, we have to do all we can to add depth in our defences and make it ever harder for adversaries to succeed in their nefarious endeavours.

On that front there is good news; the underlying principles that inform good security practices are well established and quite stable. With a necessary "start at the beginning and successively raise the bar" mentality, IoTSF has set about bringing a focus to matters of IoT security. We invited executive board member and mobile security expert, David Rogers, to edit a security principles blog for our website. We published that blog early in 2016 and have reproduced it here in a single document.

Whether you are a technology provider, a technology adopter or a technology user, we hope this stimulates thinking on how you can exercise care and extend a duty of care to others. We also hope that you'll engage with IoTSF, as a stakeholder or perhaps as a member, and help us achieve our mission of making it safe to connect.

I'd like to thank David Rogers for editing the blog and helping us create this publication. I'd also like to thank our founder members and the Executive Steering Board who are leading the way and working together to address security in the era of IoT.

Does the data need to be private?

Many IoT devices will require the collection, analysis and transmission of potentially sensitive data. It is essential that this data is adequately protected at all times, and that the user is aware what private data is being processed. Devices should:

- *Be designed with security, appropriate to the threat and device capability, in mind from the outset*
    - Security architectures for devices, networks and systems should be developed at the same time as the devices themselves, rather than retrofitted at a later date.
    - Consideration must be given to the intended use scenarios of the device and what security is appropriate.

- *Offer appropriate protection for all potential attack surfaces (e.g. device, network, server, cloud etc.)*

    - As well as the device itself, sensitive data may be exposed in other connected systems. Consider how the security of the data will be maintained throughout the whole network.

- *Inform users what private data is required in order for the device to function*

    - Users want to take advantage of the opportunities offered by IoT, but also want to ensure their privacy is protected. Device should be clear about what private data they are handling, and what the impact of denying this capability will be.

- *Allow users and security products to review sensitive data to verify the device is maintaining privacy*

    - As well as ensuring privacy is maintained, this will allow users/ devices to implement local security policies for handling sensitive data.

- *Ensure identifiers are removed or anonymised where necessary*

    - Exposure of sensitive personal identifiers may allow collection analysis of private data by unauthorised devices.

- *Manage encryption keys securely*

    - Consider the lifecycle of encryption keys, from provisioning through to decommissioning and/or revocation of the device.

Ultimately, the members of the IoT Security Foundation would like to see IoT devices which are designed with security in mind. By considering the answers to the questions above, developers can produce products - not just with better security but also with enhanced value, quality and usability. These products will then be able to form part of a safe, secure, scalable, manageable and transformative Internet of Things.

Does the data need to be trusted?

The issue of trust in IoT devices and systems

Data may need to be protected from tampering and modification in transit. This may be a malicious attacker, or simply poorly configured devices mishandling data. Appropriate security considerations may include:

- *Integrity of software is verified (e.g. secure boot)*
    - This helps to ensure that only known software is allowed to run on the device.
- *The device or system uses a hardware-rooted trust chain*
    - This allows the user to protect against sophisticated low-level software attacks and ensure that all software allowed to run on the device is appropriately authorised.
- *Authentication and integrity protection are applied to data*
    - Such protections allow users to be confident that received data is correct and from the claimed source.

- *Compromised or malfunctioning devices can be identified and revoked*

    - Erroneous data from such devices may affect other functionality of the system. Providing a way to identify these devices and then block, filter and revoke them in a secure fashion provides mitigation in this scenario.

- *Data is isolated from other systems or services where applicable*

    - IoT networks may handle many different types of data. To minimise the risk of data leakage, it should be clear which systems and services have access to which types of data.

- *System testing and calibration ensures data is handled correctly*

    - Ensuring that the system handles data as designed is crucial in providing security assurance.

- *Device metadata is trusted and verifiable*

    - Trusted metadata will allow users and devices to have confidence that the device is functioning as intended, and help to identify malfunctioning or compromised devices.

- *Re-using existing good security architectures rather than designing brand new ones*

    - While some security challenges for IoT are new and different, there are many which are similar to existing problems which have been studied for many years. Consider whether existing security architectures meet your needs.

Is the safe and/or timely arrival of data important?

Consider how the service would be impacted if data could be blocked or delayed. Points to consider include:

- *Data is accurately timestamped*
    - This allows users and devices to determine how current the data is and act accordingly.

- *Integrity of data in the device, server and other parts of the system is designed in from outset*
    - Considering any integrity requirements during the design phase will enable the system to meet such requirements without re-engineering at a later date.

- *Devices should provide failure handling and status monitoring to meet availability requirements*
    - When a device fails, it should fail into an appropriate configuration for its use.
      Users or managers should be able to monitor devices to determine their current status.

- Carriers and device managers can identify safety and timeliness needs in a secure, trusted fashion
    - Devices should securely communicate their requirements to allow networks to allocate resources accordingly and act appropriately when these are not being met.
- Any reliance on other systems or devices for availability is clearly detailed to the user
    - The user must be aware of what other systems their device has dependencies on in order to meet security requirements.
- Devices should identify themselves to a network using a secure identifier
    - This ensures that the network can allow efficient management and allocation of resources.
- Be clear what functionality the device is offering and its intended use. Make users aware of any restrictions or limitations
    - Some devices may appear similar, but have different assurance or reliability profiles. In order to avoid inappropriate deployments, users must be clear of what the device is intended to achieve.

Is it necessary to restrict access to or control of the device?

Prevention of unauthorised access or control is vital to secure devices. If an attacker gains control of the device they may be able to access sensitive data, or cause problems elsewhere in the network. To reduce this risk, developers should ensure:

- *Defences against hacking are dsesigned in from the outset*
    - Considering potential attacks during the design stage will ensure the device's security functionality is built on solid foundations and reduces the risk of serious security architecture issues emerging later in development.

- *Development processes incorporate secure coding standards, penetration testing etc.*
    - Practices such as these reduce the risks of unintentional vulnerabilities occurring in the product and help to identify and fix potential issues.

- *Service management occurs over an authenticated channel*
    - Only authorised entities should be able to manage IoT services.

Is it necessary to update the software on the device?

If a device is running out-of-date software, it may contain unpatched security vulnerabilities. Such vulnerabilities may allow exploitation of the device and its data by attackers.

Developers should ensure:

- *The vendor update and management process follows best security practice*
    - Security patches/updates should be applied in a timely fashion without impacting the functionality of the device.
- *Only authenticated sources are able to provide security updates or patches*
    - Allowing unauthenticated updates could allow attackers a way to run malicious code on the device.
- *Users and managers are easily able to see a device's patching update status*
    - This allows verification that devices are adherent to a specified security policy and ensures remedial action can be taken if required.

Will ownership of the device need to be managed or transferred in a secure manner?

Many IoT devices will change ownership at some point in their lifetime. To preserve the security of the device and data throughout its lifecycle, developers should:

- *Provide a secure method to transfer ownership of the device to another user*
    - This will allow both the old and new users to verify that the transfer of ownership has succeeded and that any sensitive data will be handled appropriately after handover.
- *Be clear which system components (devices, data, network etc.) are owned by the user*
    - Users or managers can clearly identify what their responsibilities are for ownership transfer. This will minimise the risk of security issues arising through misunderstandings of responsibilities.
- *Ensure that change of ownership does not impact security updates*
    - Critical security updates must continue to be supplied, regardless of who now owns the device

Does the data need to be audited?

IoT services may be required to meet a user audit, an enterprise audit or a regulatory audit requirement. Developers should consider providing:

- *Managed access to IoT data (for example at a local hub)*
    - If properly secured, this feature will build end-user trust and enable compliance with network policies (e.g. Intrusion Prevention Systems). This feature may also enable innovation via integration of IoT data sources.
- *Policy controls to disable unwanted features*
    - Failure to provide these may limit use in some enterprises, regions or markets.

IoT Security Foundation

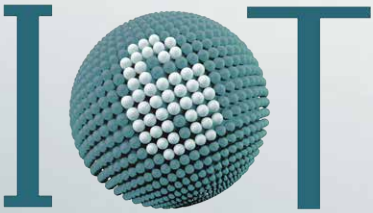
Our mission is to help secure the Internet of Things, in order to aid its adoption and maximise its benefits. To do this we will promote knowledge and clear best practice in appropriate security to those who specify, make and use IoT products and systems.

Want to be part of the IoTSF and help raise the quality of IoT security? Why not join us or make contact at iotsecurityfoundation.org

About the Editor

David is a mobile phone security expert who runs Copper Horse Solutions Ltd, a software and security company based in Windsor, UK. His company is currently focusing on security and privacy research for the Internet of Things and Smart Cities.

David also chairs the Device Security Group at the GSMA, teaches Mobile Systems Security at the University of Oxford and Cyber Security at York St John University. He has worked in the mobile industry for over 17 years in security and engineering roles. His book 'Mobile Security: A Guide for Users' was published in 2013.



Phone: +44(0)1506 401210
Email: contact@iotsecurityfoundation.org

www.iotsecurityfoundation.org