IOT SECURITY CHALLENGES AND TESTING

Stefan Kuipers (Stefan.Kuipers@nxp.com)
Marc Vauclair (Marc.Vauclair@nxp.com)
NXP/CTO/Security Concepts Team

OCTOBER 2020

SECURE CONNECTIONS FOR A SMARTER WORLD

IOT SECURITY INTRODUCTION

- Digital transformation has significantly accelerated in many industries
- This goes along with the generation & collection of tremendous amount of data, and billions of new connections controlling critical world states
- NXP shares here how this threatens national security, mission critical infrastructures, citizens safety & privacy
- NXP will formulate recommendations on key ingredients to mitigate risks and establish trust in devices manufactured by a myriad of global players in a highly competitive IoT market
- NXP is at the root of the supply chain of electronic devices and therefore can contribute strongly to anchor roots of Trust in IoT devices

BASIC IOT SECURITY ISSUES

Device manufacturers focus on functionality

- Manufacturers typically unaware of security challenges
- Most devices not enabled to get security updates

Others than buyers and users are often victim

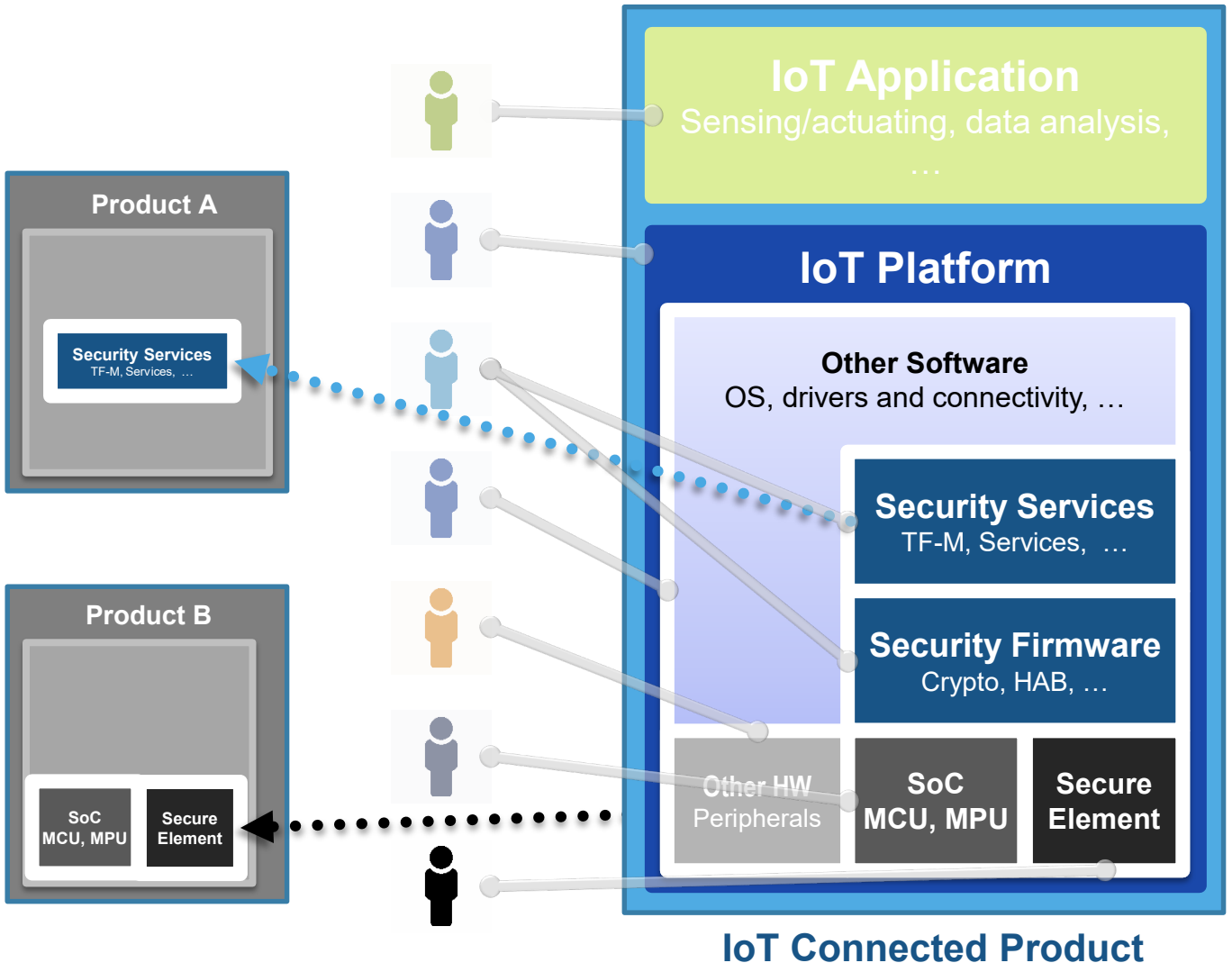
- Little incentive for producers to improve products
- Little incentive for buyers to pay for security that benefits others

Software is never bug free

- Software support throughout product lifetime is limited
- Physical attacks used to enable scalable software attacks*

*scalable attack = one person can hack many IoT devices remotely

PRODUCT COMPLEXITY



- Connected products composed of **many parts**…

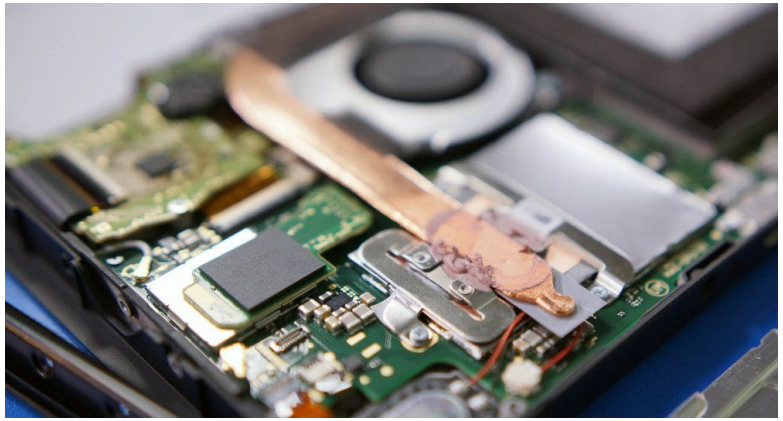
...potentially **reused** in several products

…potentially developed by **different actors**

THE THREAT

Logical attacks

Make use of software errors in the IoT device



Physical attacks

Make use of physical vulnerabilities in the IoT device

Are logical attacks always remote?
Are physical attacks always local?

Not Necessarily

And further: remote attacks often start with local physical attacks to find and exploit weaknesses

ATTACK TYPES: THE THREAT IS NOT ALWAYS REMOTE

LOGICAL
By sending malicious messages, the software will misbehave.

PHYSICAL
Making use of physical properties or deficiencies in the device.

LOCAL
Adversary must be in the proximity of the device.

REMOTE
Adversary can be anywhere.

CRITICAL SECURITY ASSETS

Integrity and Authenticity

Sensor Data – systems potentially make decisions based on this data

Control Commands – systems act on this data

Updates – resiliency of a system is its ability to be patched and updated securely

Confidentiality

Privacy of user actions and data

Protection of knowledge on critical infrastructure

Protection of critical Intellectual Property

Availability (Denial of Service)

Prevent loss of critical services (keeping the lights on)

Reliability of services

Examples of Basic Attack Protection

Boot Code protection (can only run authorized software)

Disable maintenance and debug modes

Protect and Restrict Usage of the cryptographic keys (access control)

ATTACKS ARE OFTEN TRACED TO A GLOBAL, VULNERABLE SUPPLY CHAIN

Design

Un-evaluated designs (security wise)

Manufacture

Programming of illegitimate SW

Exposure of secrets

Distribute & Integrate

Injection of counterfeits

Device supply chain

Commission

Connection to compromised Clouds

Operate

Injection of compromised SW updates

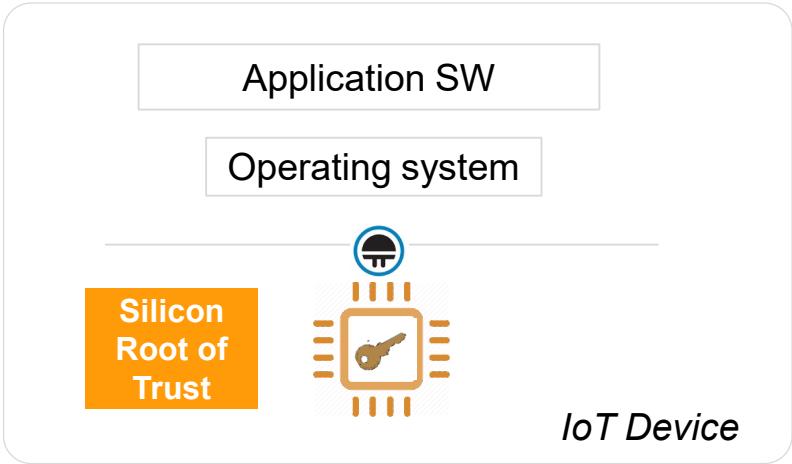
In the field

IT IS KEY TO BUILD TRUST AT HW LEVEL, AT EARLIEST STAGE OF SUPPLY CHAIN

Silicon Supply chain

Untrusted Device Supply Chain

HW Security foundation



- ✓ Tamper resistant, hardware security enclave
- ✓ Secured injection of proof of origin
- ✓ Secure injection of connection identities for cloud services
- ✓ Secure injection of keys such that only legitimate software can be executed

CHALLENGES

Security Integration can be highly complicated

- Typical IoT manufactures have little or no experience
- Security must be end-to-end and planned into design, manufacturing, delivery, operations, decommissioning

Security comes at an additional cost

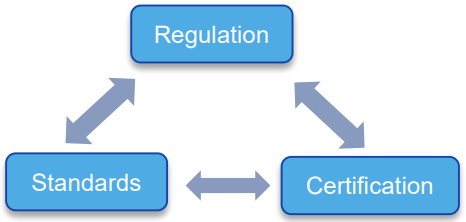
- Real security has a cost (R&D, silicon, testing, manufacturing, key management, SW maintenance, etc.)
- Typically vendors, competing with other global players, go for the bare minimum at the time of manufacturing

Return on Investment (ROI) difficult to assess

- Difficult to explain value of security to OEMs and Consumers
- Risk factors for consumer devices are however significant
- Compromising a single device can impact many more users than the initial victim
- Regulation is an opportunity to enhance security for all stakeholders and put competitors at par

SECURITY TESTING - CONSUMERS AND MARKET NEED SECURITY CERTIFICATION

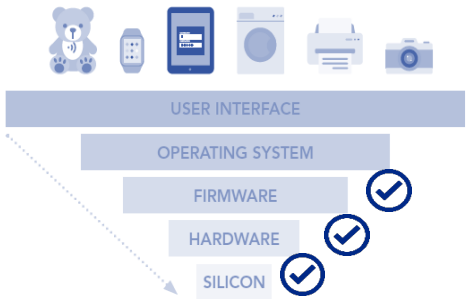
Consumers, industry, governments and infrastructure owners (e.g. utilities) need a ‘security rating’ and certification of what they buy to make conscious and educated decisions



S.734 - Internet of Things Cybersecurity Improvement Act of 2019

The certification of IoT devices and systems must rely on technical standards to explain what to do, and be enforced by regulations to be applied

Certification provides oversight of standards being met



Standardized, certified security subsystems will significantly reduce the cost and complexity of integration, while preventing basic mistakes in implementation. Recent initiatives aim at addressing this (e.g. SESIP). The certification must cover security maintenance over device lifetime

SESIP = Security Evaluation Standard for IoT Platforms

SECURITY EVALUATION STANDARD FOR IOT PLATFORMS

- A security **certification framework** similar to Common Criteria
  - Certification scope and evaluation depth not fixed
  - Allows **flexibility** on security claims
  - Uses **Protection Profiles** as security references

- Tailored to address **IoT components** up to full platforms
  - HW, drivers, connectivity libraries, Root of Trust, operating systems

- Offers 5 pre-defined assurance levels SESIP1-5

SECURITY ASSURANCE DEFINED

Assurance levels

Self-assessment
Utilizing public tools to discover publicized potential vulnerabilities

Black-Grey box penetration testing
Adding vulnerability analysis and penetration testing

White-box vulnerability analysis and penetration testing
Adding source code review

Reuse of SOG-IS CC evaluation
More evidences and higher attack potential

Reuse of SOG-IS CC evaluation
More evidences and higher attack potential

SUMMARY AND RECOMMENDATIONS

Increasing security value through stronger implementation certifications will lead to more secure products and a better protected critical infrastructure.

NXP ready to support with subject matter expertise and advice to congressional approaches for real world IoT security solutions

INCREASE THE LEVEL OF SECURITY IN IOT DEVICES

Make mandatory in standards:

- data protection
- device integrity
- updatability and resilience

Anchor root-of-trust in Hardware

EAL1,2 and FIPS not sufficient

MAKE CERTIFICATION RELEVANT FOR DEVICE VENDORS

Reduce the burden to integrate already certified components

Make certification and its value understandable

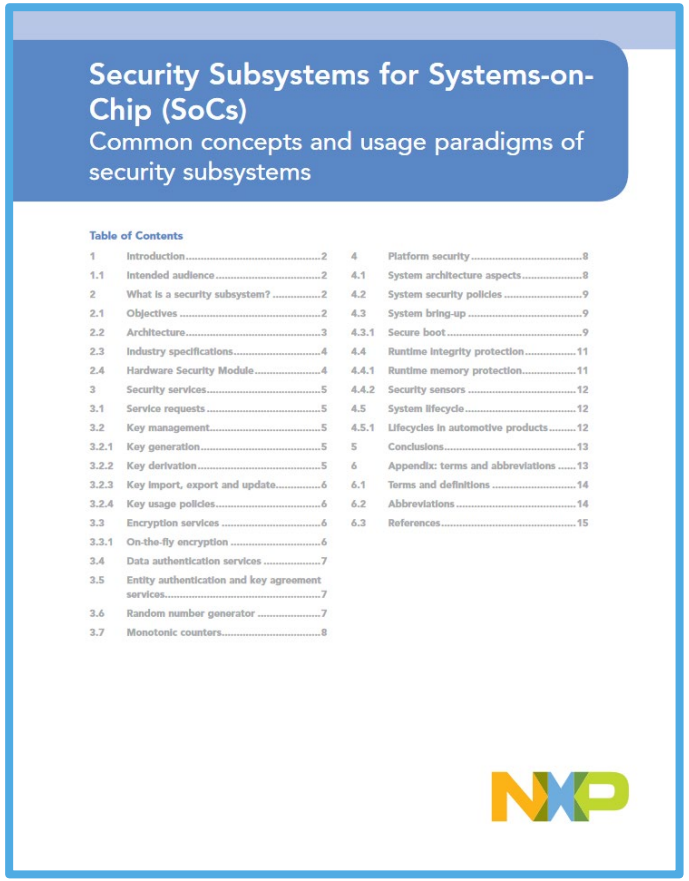
ESTABLISH CONSUMER'S TRUST IN IOT

Consumers need to gain trust in IoT products

Establish an IoT Trust mark to support the consumer's decision on security

FURTHER READINGS

https://www.nxp.com/docs/en/white-paper/NXP-FROM-IOT-TO-IOTRUST-WP.pdf

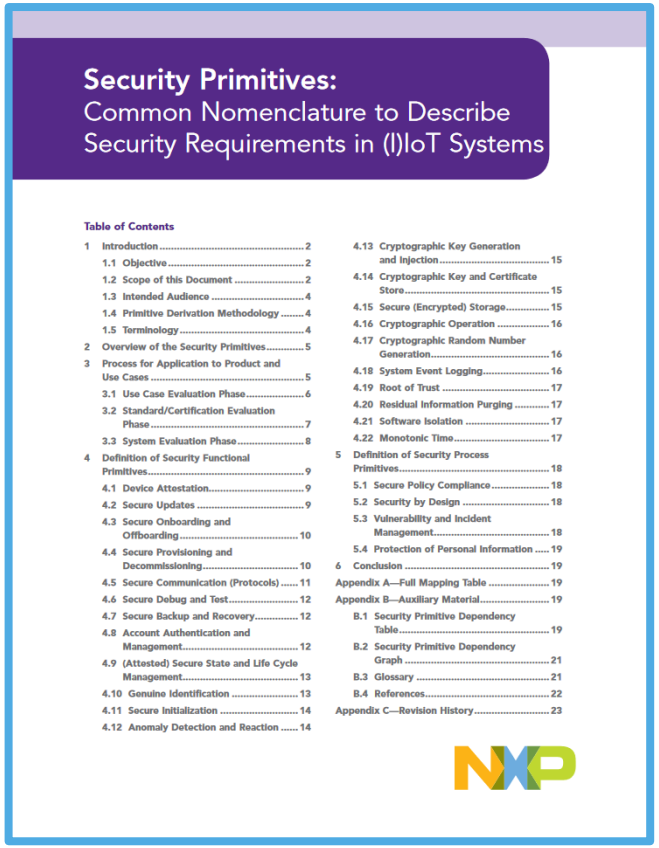


Security Subsystems for Systems-on-Chip (SoCs)
Common concepts and usage paradigms of security subsystems

Table of Contents

1 Introduction ... 2
1.1 Intended audience ... 2
2 What is a security subsystem? ... 2
2.1 Objectives ... 2
2.2 Architecture ... 3
2.3 Industry specifications ... 4
2.4 Hardware Security Module ... 4
3 Security services ... 5
3.1 Service requests ... 5
3.2 Key management ... 5
3.2.1 Key generation ... 5
3.2.2 Key derivation ... 5
3.2.3 Key import, export and update ... 6
3.2.4 Key usage policies ... 6
3.3 Encryption services ... 6
3.3.1 On-the-fly encryption ... 6
3.4 Data authentication services ... 7
3.5 Entity authentication and key agreement services ... 7
3.6 Random number generator ... 7
3.7 Monotonic counters ... 8
4 Platform security ... 8
4.1 System architecture aspects ... 8
4.2 System security policies ... 9
4.3 System bring-up ... 9
4.3.1 Secure boot ... 9
4.4 Runtime integrity protection ... 11
4.4.1 Runtime memory protection ... 11
4.4.2 Security sensors ... 12
4.5 System lifecycle ... 12
4.5.1 Lifecycles in automotive products ... 12
5 Conclusions ... 13
6 Appendix: terms and abbreviations ... 13
6.1 Terms and definitions ... 14
6.2 Abbreviations ... 14
6.3 References ... 15

https://www.nxp.com/docs/en/white-paper/Security-Subsystems-WP.pdf



Security Primitives:
Common Nomenclature to Describe Security Requirements in (I)IoT Systems

Table of Contents

1 Introduction ... 2
1.1 Objective ... 2
1.2 Scope of this Document ... 2
1.3 Intended Audience ... 4
1.4 Primitive Derivation Methodology ... 4
1.5 Terminology ... 4
2 Overview of the Security Primitives ... 5
3 Process for Application to Product and Use Cases ... 5
3.1 Use Case Evaluation Phase ... 6
3.2 Standard/Certification Evaluation Phase ... 7
3.3 System Evaluation Phase ... 8
4 Definition of Security Functional Primitives ... 9
4.1 Device Attestation ... 9
4.2 Secure Updates ... 9
4.3 Secure Onboarding and Offboarding ... 10
4.4 Secure Provisioning and Decommissioning ... 10
4.5 Secure Communication (Protocols) ... 11
4.6 Secure Debug and Test ... 12
4.7 Secure Backup and Recovery ... 12
4.8 Account Authentication and Management ... 12
4.9 (Attested) Secure State and Life Cycle Management ... 13
4.10 Genuine Identification ... 13
4.11 Secure Initialization ... 14
4.12 Anomaly Detection and Reaction ... 14
4.13 Cryptographic Key Generation and Injection ... 15
4.14 Cryptographic Key and Certificate Store ... 15
4.15 Secure (Encrypted) Storage ... 15
4.16 Cryptographic Operation ... 16
4.17 Cryptographic Random Number Generation ... 16
4.18 System Event Logging ... 16
4.19 Root of Trust ... 17
4.20 Residual Information Purging ... 17
4.21 Software Isolation ... 17
4.22 Monotonic Time ... 17
5 Definition of Security Process Primitives ... 18
5.1 Secure Policy Compliance ... 18
5.2 Security by Design ... 18
5.3 Vulnerability and Incident Management ... 18
5.4 Protection of Personal Information ... 19
6 Conclusion ... 19
Appendix A—Full Mapping Table ... 19
Appendix B—Auxiliary Material ... 19
B.1 Security Primitive Dependency Table ... 19
B.2 Security Primitive Dependency Graph ... 21
B.3 Glossary ... 21
B.4 References ... 22
Appendix C—Revision History ... 23

https://www.nxp.com/docs/en/white-paper/SEC_PRIMITIVES_WP.pdf

SECURE CONNECTIONS
FOR A SMARTER WORLD