ETSI TR 103 534-1 V1.1.1 (2019-08)

SmartM2M;
Teaching material;
Part 1: Security

Reference

DTR/SmartM2M-103534-1

Keywords

cybersecurity, IoT, oneM2M

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Smart Machine-to-Machine communications (SmartM2M).

The present document is part 1 of a multi-part deliverable covering SmartM2M Training Material, as identified below:

Part 1: "Security";

Part 2: "Privacy".

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

1.1 Context for the present document

The design, development and deployment of - potentially large - IoT systems require to address a number of topics - such as privacy, interoperability or security - that are related and should be treated in a concerted manner. In this context, several Technical Reports have been developed that each address a specific facet of IoT systems.

In order to provide a global a coherent view of all the topics addressed, a common approach has been outlined across the the present document concerned with the objective to ensure that the requirements and specificities of the IoT systems are properly addressed and that the overall results are coherent and complementary.

The present document has been built with this common approach also applied in all of the other documents listed below:

ETSI TR 103 533 [i.1]

ETSI TR 103 534 [i.15]

NOTE: ETSI TR 103 534-1 is the present document

ETSI TR 103 535 [i.3]

ETSI TR 103 536 [i.4]

ETSI TR 103 537 [i.5]

ETSI TR 103 591 [i.19]

1.2 Scope of the present document

The present document presents teaching material to allow readers, identified by role, to gain knowledge of the fundamentals of IoT security.

The present document is structured as a set of annexes each containing the outline of training material. The more detailed training material, in the form of a set of PowerPoint slides is provided in archive tr_10353401v010101p0.zip as an electronic addition to the present document.

The annexes contain training material in the following areas:

- Threat, Vulnerability and Risk Analysis (TVRA) in IoT:
  - The role of TVRA is primarily to ensure that a system is designed and deployed with a thorough understanding of the environment in which it will be deployed, the purpose of the system, the components or assets of the system, the links between the deployment and its environment, and the technical/procedural/regulatory basis of the system. Having this core understanding alongside an analysis of the threats and threat agents that will seek to attack the system leads to an understanding of the risks to the system.
  - The material in this clause extends from material prepared for the ETSI TVRA Workshop (March 2009) and is based on the TVRA method published in ETSI TS 102 165-1 [i.2] with specific IoT use cases to drive the TVRA exercise.
- Secure configuration of IoT devices:
  - The vast majority of security failures occur as a result of poor configuration. For example reliance on default security attributes (the default password conundrum). The purpose of this module is to give guidance on how to securely configure IoT devices to minimise their attack surface.

- Cryptographic security basics as they apply in IoT:
  - Cryptography is the mathematical toolset that underpins the majority of countermeasures (i.e. authentication, encryption, integrity proof and verification). The purpose of this module is to give a simple grounding in the role and purpose, and the underlying mechanisms of cryptography. Amongst the topics to be covered are the following:
    - Role of cryptography in security
    - Historic roots of cryptography
    - Relationship identification to pre-select cryptographic architecture
    - Core cryptographic modes
  - The material provides examples based on AES as published in FIPS 197 [i.11] and the Diffie Hellman asymmetric key exchange protocol.
- Secure operation of IoT devices:
  - Closely related to secure configuration is secure operation and this module addresses the measures required to assure that a securely configured device can be operated securely.
- Applying best practices to IoT security:
  - The purpose of this module is to give specific training in how to apply the best practices identified in ETSI TR 103 533 [i.1] to real IoT systems.
- Programming guide for secure IoT:
  - The purpose of this module is to give guidance on secure or safe programming. By means of coding examples (in programming languages including Swift, C, C++, Java) the steps to minimise security flaws in programming of IoT devices.
- Guide to selecting a training provider:
  - A guide to the identification and selection of training providers and training programmes in IoT.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 103 533: "SmartM2M; Security; Standards Landscape and best practices".

[i.2] ETSI TS 102 165-1: "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.3] ETSI TR 103 535 (V1.1.1): "SmartM2M; Guidelines for using semantic interoperability in the industry".

[i.4] ETSI TR 103 536: "SmartM2M; Strategic / technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms".

[i.5] ETSI TR 103 537: "SmartM2M; Plugtests™ preparation on Semantic Interoperability".

[i.6] ETSI TR 103 591: "SmartM2M; Privacy study report; Standards Landscape and best practices".

[i.7] AIOTI: "High Level Architecture (HLA)", Release 4.0, June 2018.

[i.8] ENISA: "IoT Security Standards Gap Analysis", ISBN: 978-92-9204-275-2, DOI: 10.2824/713380.

[i.9] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[i.10] ETSI TS 103 645: "CYBER; Cyber Security for Consumer Internet of Things".

[i.11] National Institute of Standards and Technology (NIST) FIPS 197: "Federal Information Processing Standards Publication 197; Advanced Encryption Standard (AES)", November 26, 2001.

[i.12] GSMA IoT Security Guidelines and IoT Security Assessment.

NOTE: Available from https://www.gsma.com/iot/iot-security/iot-security-guidelines/

[i.13] ETSI TR 103 305-1: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

[i.14] ETSI TR 103 534: "SmartM2M; Teaching Material: Part 1 (Security) and Part 2 (Privacy)".

NOTE: ETSI TR 103 534-1 is the present document.

[i.15] ETSI EN 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AES	Advanced Encryption Standard
AIOTI	The Alliance for Internet of Things Innovation
API	Application Programming Interface
CASP	CompTIA Advanced Security Practitioner
CIA	Confidentiality, Integrity, Availability
CISSP	Certified Information Systems Security Professional
DB	DataBase

DBA	DataBase Administator
DBMS	DataBase Management System
DDoS	Distributed Denial of Service
DevOps	Development IT Operations
DevSecOps	Secure DevOps
DNS	Domain Name System
DoS	Denial of Service
e-CF	European e-Competence Framework
ENISA	European Union Agency for Network and Information Security
ERP	Enterprise Resource Planning
ESAPI	OWASP Enterprise Security API
ETSI	European Telecommunication Standards Institute
FIPS	Federal Information Processing Standard
GDPR	General Data Protection Regulation
GSMA	GSM Association
IaC	Infrastructure as Code
ICT	Information and Communications Technology
IoT	Internet of Things
ISC^2	International Information System Security Certification Consortium
IT	Information Technology
ORM	Object Relational Mapper
OS	Operating System
OWASP	Open Web Application Security Project
RSA	Rivest Shamir Aldeman
SQL	Structured Query Language
SSCP	Systems Security Certified Practitioner
TOE	Target Of Evaluation
TR	Technical Report
TVRA	Threat, Vulnerability and Risk Analysis

4 What is Security?

4.1 Introduction and overview

The question "What is Security?" is very difficult to answer succinctly. In the context of ICT, security is often taken to refer to the prevention of various forms of attack on the system, or elements of the system. The purpose of the present document, as indicated in the Scope statement, is to provide material to allow readers, identified by role, to gain knowledge of the fundamentals of IoT security.

Whilst these concepts are expanded upon in the remainder of the present document the complexity of "security" as a topic to understand is highlighted by the many roles and process that "security" has to tackle:

- System protection role:
  - Core CIA roles - least knowledge model to assure system operation.
  - Analytic role - data required to forecast, resolve, recover.
- Anti-adversary role:
  - Identify who gains from system breaches.
- Risk management role:
- Regulatory compliance role:
  - Assurance of technical provisions for GDPR, for the Cyber-Security directive, for law enforcement, for support of the eIDAS regulation and so forth.

A reasonable level of understanding of each of these roles, and the technologies and processes that enable them, is the ultimate goal of the present document.

4.2 Teaching goals

The bulk of the material in the present document is aimed at tutor led teaching and there is a presumption of prior knowledge to apply the material to the actual audience. Thus there are hints given at points in the material for the tutor/teacher to drive classroom exercises. Such exercises are not definitive in that there is no implied certificate or other statement of learning from the material but are intended to allow the tutor to assess the success of students in assimilating the material offered.

NOTE: In the case of tutor lead classwork the tutor is expected to expand upon the base material that is provided in the present document and its attachments as required by the students.

4.3 Learning goals

Whilst not specifically designed for self-tutoring when used in such a context, as for teaching goals, the present document has some specific learning goals when acting as the basis of self-taught material. Specific learning goals are indicated at the start of each clause in order to guide the reader as to the new knowledge that will be gained after completion of the material in each clause.

5 Security in the context of IoT

5.1 A global approach to IoT Systems

5.1.1 Major characteristics of IoT systems

IoT systems are often seen as an extension to existing systems needed because of the (potentially massive) addition of networked devices. However, this approach does not take stock of a set of essential characteristics of IoT systems that push for an alternative approach where the IoT system is at the centre of attention of those who want to make them happen. This advocates for an "IoT-centric" view.

Most of the above-mentioned essential characteristics may be found in other ICT-based systems. However, the main difference with IoT systems is that they all have to be dealt with simultaneously. The most essential ones are:

- **Stakeholders.** There is a large variety of potential stakeholders with a wide range of roles that shape the way each of them can be considered in the IoT system. Moreover, none of them can be ignored.
- **Privacy.** In the case of IoT systems that deal with critical data in critical applications (e.g. e-Health, Intelligent Transport, Food, Industrial systems), privacy becomes a make or break property.
- **Interoperability.** There are very strong interoperability requirements because of the need to provide seamless interoperability across many different systems, sub-systems, devices, etc.
- **Security.** As an essential enabling property for Trust, security is a key feature of all IoT systems and needs to be dealt with in a global manner. One key challenge is that it is involving a variety of users in a variety of use cases.
- **Technologies.** By nature, all IoT systems have to integrate potentially very diverse technologies, very often for the same purpose (with a risk of overlap). The balance between proprietary and standardised solutions has to be carefully managed, with a lot of potential implications on the choice of the supporting platforms.
- **Deployment.** A key aspect of IoT systems is that they emerge at the very same time where Cloud Computing and Edge Computing have become mainstream technologies. All IoT systems have to deal with the need to support both Cloud-based and Edge-based deployments with the associated challenges of management of data, etc.
- **Legacy.** Many IoT systems have to deal with legacy (e.g. existing connectivity, back-end ERP systems). The challenge is to deal with these requirements without compromising the "IoT centric" approach.

5.1.2 The need for an "IoT-centric" view

5.1.2.1 Introduction

In support of an "IoT-centric "approach, some elements have been used in the present document in order to:

- Support the analysis of the requirements, use cases and technology choices (in particular related to interoperability).
- Ensure that the target audience can benefit from recommendations adapted to their needs.

5.1.2.2 Roles

A drawback of many current approaches to system development is a focus on the technical solutions, which may lead to suboptimal or even ineffective systems. In the case of IoT systems, a very large variety of potential stakeholders are involved, each coming with specific - and potentially conflicting - requirements and expectations. Their elicitation requires that the precise definition of roles that can be related to in the analysis of the requirements, of the use cases, etc.

Examples of such roles to be characterised and analysed are: System Designer, System Developer, System Deployer, End-user, Device Manufacturer. Some of these roles are specifically addressed in the present document.

5.1.2.3 Reference Architecture(s)

In order to better achieve interoperability, many elements (e.g. vocabularies, definitions, models) have to be defined, agreed and shared by the IoT stakeholders. This can ensure a common understanding across them of the concepts used for the IoT system definition. They also are a preamble to standardisation. Moreover, the need to be able to deal with a great variety of IoT systems architectures, it is also necessary to adopt Reference Architectures, in particular Functional Architectures. The AIOTI High-Level Architecture (see [i.7]) is the reference for the present document.

5.1.2.4 Guidelines

The very large span of requirements, Use Cases and roles within an IoT system make it difficult to provide prototypical solutions applicable to all of the various issues addressed. The approach taken in the present document is to outline some solutions but also to provide guidelines on how they can be used depending on the target audience. Such guidelines are associated to the relevant roles and provide support for the decision-making.

6 Overview of IoT security challenge

6.1 The challenge

The core challenge in IoT, particularly embedded IoT where devices are often of an "enable and forget" form, is to recognise that as an IoT device has processing and communication capacity, that often can be programmed post-shipment, that it is a vector to attack any of the user, the system or something in the wider connected network. This entails understanding of the management of risk through management of impact (if something happens) and management of likelihood (of something happening). These aspects, impact and likelihood of an attack, have been at the core of security engineering since its inception. The set of things that engineers are able to do to minimise risk are considerable and part of the challenge in IoT is to provide a minimum set of technical capabilities that maximise the security of the system. However even with the appropriate technology in place it is still necessary to have the non-technology aspects correctly implemented and this means distribution chains, physical security measures, personnel measures and so forth.

The primary security provisioning strategies of redesign or hardening are consistent with the goal of security design to ensure a low likelihood of an unwanted incident arising. As the likelihood of an unwanted incident is dependent upon the presence of weakness in an asset and also the presence of both threats and threat agents that exploit the weakness it is the purpose of security systems to remove, or mask, the weaknesses of an asset.