ETSI TR 103 309 V1.1.1 (2015-08)

CYBER;
Secure by Default - platform security technology

Reference
DTR/CYBER-0007

Keywords
cybersecurity, platforms, secure by default

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

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document 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 (http://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.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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.

Introduction

Often in order to make today's products and services secure, their usability has to be severely reduced. If an enterprise is to operate securely in a connected world, every product, system or service that is procured or deployed should be Secure by Default. It should actually be hard to make them insecure; technology should improve usability without compromising security.

Standards have been developed which describe how to provide the required features and mechanisms, however adoption of these into real systems is often slow.

A key reason for slow adoption is the lack of awareness outside the technical community of which security features exist and how they should be used. Effort is needed to build demand as well as supply.

1 Scope

The present document is intended to encourage development and adoption of 'secure by default' platform security technologies by showing how they can be used to effectively solve real business problems, and improve the usability of secure services. The intended audience is decision makers rather than engineering teams where they are deciding which features to include in a new platform, or which are required as part of a procurement activity. The present document focuses on a structure for describing identified business needs/issues for a particular set of users; detailing the characteristics needed of possible solutions, and finally identifying existing or emerging standards which provide those characteristics.

2 References

2.1 Normative 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 reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

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 necessary for the application of the present document.

Not applicable.

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 reference 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.

Not applicable.

3 Abbreviations

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

FIDO	Fast IDentity Online
IT	Information Technology

4 Secure by default approach

This clause describes the underlying philosophy behind 'secure by default'. The aim is to identify real business problems and suggest ways of solving them at root cause, rather than by applying patches or 'stop-gap' measures to address particular issues. The emphasis is therefore on security mechanisms embedded in core device functions; supplied literally 'by default' in products instead of being added afterwards via updates or complex configuration.

New features of this nature require fundamental changes to devices, hence development can take time. Promoting adoption may require that technical solutions be identified when they are still maturing; prototypes exist to verify the concept, however market support is required in order to justify investment in refining a product.

Finally it is clear that simply developing technical components is almost never sufficient to solve problems in the real world. Practical guidance is needed to ensure these components can be integrated appropriately into deployed systems. As well as identifying technologies, it is necessary to point out relevant good practice guidance where it exists.

5 Annex structure

5.1 Approach

This clause describes the framework that each annex needs to follow in relating business issues to the enabling technologies that address them.

5.2 Introduction

Describe a particular issue (problem or opportunity) at a high level. Aim to show why it is relevant to a particular market area.

5.3 Specific challenges

Break down the high level scope into discrete challenges which can be described in non-technical terms, but which could be addressed using technology.

5.4 Enabling technologies and good practice

Relate the above challenges to specific technologies which could provide solutions. While acknowledging that vendor proprietary solutions exist, it is not the aim of the present document to advertise them; rather to point out technical standards activities where they exist, and explain their relevance to the specific challenges.

Where it exists, explain where to find practical guidance on good practice for integrating the specified technologies into deployed systems.

It is outside the scope of the present document to discuss the fine details of particular technical standards. The aim is to provide sufficient information to explain their relevance and direct further enquiries if they are needed.

Annex A:
Personally owned IT

A.1 Introduction

It is inevitable that people will increasingly use personally owned IT in their jobs. Flexibility and ease of access to time-critical information are clear benefits, however the huge range of devices and user behaviours cause problems when it comes to managing risk.

Security-conscious enterprises need to design systems with this in mind; allow useful connectivity to a very wide range of devices, while at the same time understanding how and when to manage access to more sensitive resources.

Technology can help achieve this goal; the aim of this note is firstly to identify key challenges for risk owners in this area; secondly to encourage risk owners to investigate technical solutions. It is clearly not sufficient to rely on procedural controls and user education to manage risk.

It is necessary to initially identify resources that are very low risk, and can easily be made available with minimal controls (e.g. via a web service, with basic user authentication). The network architecture should isolate these from the more sensitive components, such that the former can be accessed wherever it is needed. Extra checks can subsequently be implemented to enforce access controls for the more protected parts of the system.

A.2 Specific Challenges

A.2.1 User ID - who wants access? How can their identity be verified?

Access should not be granted to an individual until the system is confident that they are the person they claim to be, and that they are appropriately authorized. The degree of confidence required is likely to be different for different types of access. The challenge is to establish confidence swiftly, with minimum inconvenience to the user.

A.2.2 Location - where is the access request coming from? Is that appropriate?

Some types of access may not be appropriate from certain locations (e.g. a public place, or outside certain areas of an office). Further, unexpected location information (e.g. from a country the requestor was known not to be visiting) might imply that an access request is not genuine. The challenge is to understand what location information is useful, and how trustworthy the information is likely to be.

A.2.3 Device ID - which devices are connecting to the network? Can this device be trusted to access that resource?

Strong, reliable device identification allows access control decisions to be made on a per-device basis, as well as per-user (e.g. some platforms may be able to access data not available to less protected hardware). Additionally such mechanisms can automate asset management processes and keep track of valuable devices. For example, log files would show when and where each device has been used, and by whom.

A.2.4 Device state - how is the device configured? Is the system (including apps) up to date?

In addition to knowing the identity of a device, one needs to be confident that it is appropriately configured; for example that data stored on a device will be encrypted, or that an application will be appropriately isolated from other unknown software. One should not trust a device unless they have confidence that recent patches have been promptly applied. The challenge is to ensure that when a device reports its state, the information is useful and trustworthy.

A.2.5 On-Device isolation - is sensitive data protected from malicious or insecure applications on a device?

The challenge is to achieve effective isolation without compromising usability.

A.3 Enabling technologies and good practice

A.3.1 Introduction

A number of vendors provide proprietary solutions to meet the above challenges. The goal of the present document is to encourage enterprises to seek out hardware-backed solutions built into commodity products, and to identify relevant standards where they exist.

In general the standards bodies provide advice on good practice in addition to the component specifications.

A.3.2 Trusted Platform Module

- https://www.trustedcomputinggroup.org/developers/trusted_platform_module/faq.
- Key storage provides device ID.
- Key storage plus anti-hammering protection provides for strong user ID without a need for complex passwords.
- Measurement and attestation provides reliable information on device state.

A.3.3 Secure Element

- https://www.globalplatform.org/mediaguideSE.asp.
- Key storage provides device ID.

A.3.4 Trusted Execution Environment

- https://www.globalplatform.org/mediaguidetee.asp.
- Provides isolation of critical software components for a variety of use cases, including user authentication.

A.3.5 FIDO alliance

- http://fidoalliance.org/about.
- Collection of specifications aimed at reducing reliance on passwords, and providing a framework for a variety of authentication mechanisms.

History

Document history		
V1.1.1	August 2015	Publication