ETSI TR 103 303 V1.1.1 (2016-04)

TECHNICAL REPORT

CYBER;
Protection measures for ICT in the context of Critical Infrastructure

Reference

DTR/CYBER-0001

Keywords

Critical Infrastructure, Cyber Security

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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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

Copyright Notification

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 (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.

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.

1 Scope

The present document reviews the roles and subsequent measures for the protection of any infrastructure for which loss or damage in whole or in part will lead to significant negative impact on one or more of the economic activity of the stakeholders, the safety, security or health of the population, where such infrastructure is hereinafter referred to as Critical Infrastructure (CI). The resulting measures and processes for Critical Infrastructure Protection (CIP) where the CI in whole or in part is composed of ICT technologies using Cyber-Security mechanisms are defined and relevant mechanisms to be implemented are identified.

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

[i.1] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[i.2] Commission of the European Communities; COM(2006) 786 final; communication from the Commission on a European Programme for Critical Infrastructure Protection (Brussels, 12.12.2006).

[i.3] European Commission; SWD(2013) 318 final; Commission staff working document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure; Brussels, 28.8.2013.

[i.4] Public Safety Canada: "National Strategy for Critical Infrastructure".

NOTE: Available at http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf.

[i.5] Australian Government: "Critical Infrastructure Resilience Strategy", 2010.

NOTE: Available at http://www.tisn.gov.au/Documents/CriticalInfrastructureResilienceStrategyPlanAccessible.pdf.

[i.6] Japan Information Security Policy Council (ISPC): "Action Plan on Information Security Measures for Critical Infrastructure", 2005.

[i.7] ISO 27000 series: "Information technology -- Security techniques -- Information security management systems".

NOTE: ISO 27000 is a multipart standard. The reference is to the body of work prepared by ISO/IEC JTC1 SC27 in the domain of Information security management systems.

[i.8] ISO 15408-1: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".

[i.9] ETSI EG 202 387: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables".

[i.10] ETSI TR 103 309: "CYBER; Secure by Default - platform security technology".

[i.11] ETSI TR 103 305: "CYBER; Critical Security Controls for Effective Cyber Defence".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Critical Infrastructure (CI): infrastructure for which loss or damage in whole or in part will lead to significant negative impact on one or more of the economic activity of the stakeholders, the safety, security or health of the population

NOTE: Annex A of the present document presents a summary of existing definitions of CI that have informed the definition given above.

3.2 Abbreviations

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

AC	Access Control
CC	Common Criteria
CI	Critical Infrastructure
CIA	Confidentiality Integrity Availability
CIP	Critical Infrastructure Protection
CS	Critical Service
EAL	Evaluation Assurance Level
EU	European Union
ICT	Information Communications Technology
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
PKI	Public Key Infrastructure
RBAC	Role Based Access Control

4 Identification and notification of Critical Infrastructure

4.1 Definition of CI

In order to identify CI it is essential to have a clear definition of what constitutes a critical service. This should be based upon the impact of a deliberate or accidental disruption to the service over a realistic timeframe. Critical services should then be further classified according to defined scales of impact should disruption occur. Subsequently, the infrastructure, whether physical or logical, essential to the operation of the service should be identified and similarly classified by impact to form CI.

NOTE: Whilst it is possible for a critical service to have no critical infrastructure (e.g. in the case of highly distributed systems where any critical impact on the service would require systemic failure across several resources) such systems and services are not addressed in the present document.

The process of CI classification enables the prioritization of protection efforts and investment decisions across CI. In working towards a classification it may be helpful to group critical services into sectors and sub-sectors to manage engagement efforts with relevant operators.

EXAMPLE: In the energy sector, a critical sub-sector is electricity, with the transmission or distribution of electricity to the nation representing a critical service. ICT which underpin this service, such as Industrial Control Systems, can then be identified and classified according to the impact of an attack on the availability or integrity of the system.

4.2 Identification of CI

Once definitions and criteria have been established it is crucial to design and implement a process to create and maintain an up-to-date record of CI. Stakeholders should be identified and provided with adequate mandates and resources to carry out this function. CI should not be considered in isolation but as part of the wider critical service that it supports.

At a minimum, the information captured should include the possible impact of an attack on CI, the owner of the CI, the location (where relevant) and a record of any dependencies or interdependencies required for continued operation.

The key questions to ask when identifying CI are:

- Are the impacts of a successful attack on the CI understood (including those resulting from interdependencies)?
- Have those impacts been used to properly categorize the CI?
- Have any dependencies (including technical, procedural and commercial) relating to the CI been captured and analysed?
- Have any interdependencies relating to the CI been captured and subjected to further analysis?
- Can the owner of the CI and its location be quickly ascertained?
- How frequently will the categorization of this CI need to be reviewed?

EXAMPLE: The generation of electricity is often dependent upon water supplies to provide adequate cooling of equipment in power plants. Conversely, the supply of water is dependent on electricity. Failure to identify this interdependence may result in the misclassification of CI and the implementation of inadequate security.

The process of identifying and categorizing CI should be iterative. Following the identification of CI dependencies it might become clear that there is a risk of common mode or cascading failure. The process should also be subject to audit on a regular basis to ensure it remains effective.

4.3 Notification of CI

Organizations should be familiar with the definition(s) of CI in their sector(s) and the government body acting as a point of contact in this area. Any organization believing that they either meet the relevant definition of CI or will do so in the near future should notify the relevant government body.

NOTE: Given the national significance of CI it is presumed that a government appointed body has responsibility for CI.

The key questions to consider when notifying CI are:

- At what stage should an organization notify the relevant body?
- Are organizations aware of the criticality thresholds and notification requirements for CI?
- How will organizations be persuaded to notify the relevant body when they meet the threshold for CI?

5 Security domains for CI protection

5.1 Review of CIA paradigm and its applicability in CI Protection

5.1.1 Overview

The conventional paradigm for provision of security features is CIA – Confidentiality, Integrity, Availability. This paradigm is conventionally applied in well defined domains and is often combined with known triples of {*domain, attack, countermeasure*}, such that in the confidentiality branch the triple {*confidentiality, interception, encryption*} will often appear. The characteristics of the common description of attacks in the CIA paradigm are typically centred on single attack vectors with Alice and Bob representing the end points of the to-be-secured transaction, and Eve representing the adversary. The application of CIA to CI is not in question as an attack that causes an outage of some part of the infrastructure could be as simple as a masquerade attack giving privilege escalation sufficient to override normal run-time security. Thus CIA should be considered as an essential building block in protection of CI.

The succeeding clauses summarize the aims of each of the CIA elements and their role in CI protection.

5.1.2 Confidentiality

The role of confidentiality protection is to ensure that information shared by Alice and Bob is intelligible only to Alice and Bob, and Eve, even if she can access that information, should be unable to understand the information in like manner to Alice and Bob. In Critical Infrastructure Protection (CIP) there are many parts of the management of the infrastructure that will be required to remain confidential and this may include configuration information of assets and their interactions.

Confidentiality also has a close relationship to privacy (shared meaning in US-English) and to core concepts such as unobservability, anonymity, pseudonymity and unlinkability. For a generic system the more of the system that is exposed then the greater risk there is that an attacker can identify an attack path. However, making the entire system "secret" does not make it more secure as it may lead the operators of the system to a false sense of security, this model of "security by obscurity" has been discredited over a number of years and whilst making everything public is not to be recommended it is reasonable to assume that those intending to attack a system, even if external to the system, have knowledge of the operations and architecture of a system.

The method of providing confidentiality of data either in storage or in transit for ICT in CI assumes that access control capabilities have been implemented in the first instance. As in all cryptographically protected schemes the method of protection will depend on overall trust and the cardinality of the relationships being protected.

EXAMPLE: The cardinality of the secured relationship in symmetric encryption is 1:1 (e.g. GSM), whilst for asymmetric encryption the cardinality is 1:m or m:1 (e.g. e-commerce). Where m:n relationships need to be secured they often first need to be normalized to sets of 1:m/m:1 relationships.

5.1.3 Integrity

5.1.3.1 Overview of the role of integrity

The role of integrity protection is that if Eve modifies data that that modification is detectable by Alice (and Bob if the data is exchanged with Bob).

NOTE: Bob can, as an actor, be Alice in the future. In other words, Alice stores data for future retrieval, in such a case future-Alice (Bob) should be able to detect if the stored data has been modified in the period between storage and retrieval.

5.1.3.2 Supply chain integrity

Supply chain integrity is a special case of integrity and addresses the entire chain to the end user. In this instance the term integrity is closer to the meaning of the term used in written English and refers to the overall trustworthiness of the supply chain and not to the stability of the supply chain. In cases such as Just in Time manufacturing attacks on the supply chain may be seen in a number of ways, for example an attack on the logistics tracking and planning may result in delays in delivery of components. Whilst such attacks are not necessarily likely to change a "normal" attack to one where the impact is sufficient to escalate the attack to one impacting critical infrastructure it is reasonable to consider attacks against supply chain integrity as likely to impact economic activity and in some cases (e.g. supply of medical relief) to impact the health of a population.

In many cases the supply chain has roots in natural phenomena - distribution of clean drinking water requires rainfall to be captured in lakes, rivers and reservoirs. A localized drought may impact the ability of CI to work but it is difficult to force nature to re-supply, however if periodic drought is possible the CI should take that into consideration in ensuring that sources of supply to meet demand can be integrated to the architecture, in other words if part of the supply chain is damaged that the overall CS can be maintained by appropriate design of the supporting CI.

5.1.4 Availability

The Availability element of the CIA paradigm covers a wide range of aspects including access control, identification, authentication, reliability, resilience and monitoring (for the purpose of assuring availability).

Any system that is classified as CI, and the services it supports, will almost inevitably become subject to a higher degree of accountability to 3rd parties than non-CI systems. As CI exploits have significant negative impact on one or more of the economic activity of the stakeholders, the safety, security or health of the population, it is highly likely (certain) that government and their agencies will be concerned stakeholders. In consideration of the role of government to protect the economic activity of the nation or state, the safety, security and health of the population certain core requirements may have to be met for the provider of the CI. This may require that the provider/operator of the CI proves that the CI is adequately protected from unauthorized access.

Provisions for adequate CI protection may require to be independently verified. However, many of the existing schemes for such assurance are not scalable to very large and mutable systems. Of the existing standards based schemes in place the following may apply:

- ISO 27000 series [i.7]
  - The ISO 27000 series covers a wide range of security management, technical protection and controls capabilities. The set of controls identified in ISO 27001 for example cover a range of technology and organizational functions including access control, human resources, asset control, and incident management. These controls are mimicked in many national security assurance and evaluation programmes.
- ISO 15408-1 [i.8]
  - Commonly referred to as the Common Criteria (CC) in recognition of the willingness of signatories to recognize an evaluation made by one agency as valid for all signatories. The CC has been traditionally based on 2 types of evaluation product - a Protection Profile, and a Security Target with evaluation against a set of criteria and the depth of evaluation identified by discrete levels (e.g. Evaluation Assurance Level 5 (EAL5)). The evolution of CC towards a model of Community Protection Profiles (cPPs) is underway that drives CC towards a more standards like model. The bulk of existing CC evaluations are against components rather than systems.