ETSI TS 102 165-1 V5.2.5 (2022-01)

CYBER;
Methods and protocols;
Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)

Reference
RTS/CYBER-0073

Keywords
authentication, confidentiality, 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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Cyber Security (CYBER).

The present document is part 1 of a multi-part deliverable covering methods and protocols for security standardization, as identified below:

Part 1: "Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)";

Part 2: "Protocol Framework Definition; Security Counter Measures".

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 defines a method primarily for use by ETSI standards developers in undertaking an analysis of the threats, risks and vulnerabilities of an Information and Communications Technology (ICT) system.

NOTE: The method described has been tailored to apply to pre-production but can be applied to production devices with due attention given to possibility that the application of countermeasures may be unachievable for a re-design strategy.

The method described in the present document builds from the Common Criteria for security assurance and evaluation defined in ISO/IEC 15408 [i.27], [i.28], [i.29] and specifically targets the means to build a Threat Vulnerability and Risk Analysis (TVRA) to allow its reference by an ETSI specification developed using the guidelines given in ETSI EG 202 387 [i.1] and ETSI ES 202 382 [i.24]. The TVRA forms part of the documentation set for the Target Of Evaluation as specified in ETSI ES 202 382 [i.24] with its intended audience being a developer of standards based Protection Profiles.

The use of the method described in the present document for application outside the "Design for Assurance" paradigm described in ETSI EG 202 387 [i.1] is supported but some of the examples and stages of evaluation may not be appropriate.

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 https://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.

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 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.2] ETSI TR 187 011: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Application of ISO-15408-2 requirements to ETSI standards - guide, method and application with examples".

[i.3] ETSI TR 187 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN-SEC); Threat, Vulnerability and Risk Analysis".

[i.4] ETSI TR 102 055: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); ENUM scenarios for user and infrastructure ENUM".

[i.5] Void.

[i.6] Void.

[i.7] ETSI TS 102 051: "ENUM Administration in Europe".

[i.8] Void.

[i.9] ETSI ETR 332 (1996): "Security Techniques Advisory Group (STAG); Security requirements capture".

[i.10] CESG: "HMG IA Standard Numbers 1 & 2 - Supplement - Technical Risk Assessment and Risk Treatment", Issue No: 1.0, April 2012.

[i.11] CC Users Forum (September 2014): "Collaborative Protection Profiles: The Benefits of an Evolved Common Criteria Implementation".

NOTE: Available from http://spo.cfx.mybluehost.me/wp-content/uploads/2020/10/cPP_White_Paper.pdf.

[i.12] ISO/IEC 27002:2005: "Information technology -- Security techniques -- Code of practice for information security management".

[i.13] ISO/IEC 27001:2005: "Information Technology - Security Techniques - Information Security Management Systems - Requirements".

[i.14] ptc/04-10-02: "Object Management Group. UML 2.0 Superstructure Specification", edition, 2004.

[i.15] IETF RFC 3761: "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)".

[i.16] Void.

[i.17] Void.

[i.18] Void.

[i.19] Void.

[i.20] Void.

[i.21] ISO 31000:2009: "Risk management - Principles and guidelines".

NOTE: The above reference supersedes the reference to AS/NZS 4360: "Standards Australian, Risk Management" in earlier editions of the present document.

[i.22] ISO/IEC 18028:2005 (Parts 4 and 5): "Information technology -- Security techniques -- IT network security".

NOTE: ISO/IEC 18028 is a multi-part publication and the reference above is used to refer to the series.

[i.23] Void.

[i.24] ETSI ES 202 382: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Protection Profiles".

[i.25] Void.

[i.26] ETSI TS 187 001: "Network Technologies (NTECH); NGN SECurity (SEC); Requirements".

[i.27] ISO/IEC 15408-1: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".

[i.28] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".

[i.29] ISO/IEC 15408-3: "Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements".

[i.30] ISO/IEC 15408: "Information technology - Security techniques - Evaluation criteria for IT security".

NOTE: When referring to all parts of ISO/IEC 15408 the reference above is used.

[i.31] ISO/IEC 17799: "Information technology -- Security techniques -- Code of practice for information security management".

[i.32] Common Methodology for Information Technology Security Evaluation: "Evaluation methodology", July 2009 Version 3.1 Revision 3 Final.

NOTE: Available at https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R3.pdf.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI EG 202 387 [i.1], ISO/IEC 17799 [i.31], ISO/IEC 18028 [i.22] and the following apply:

asset: anything that has value to the organization, its business operations and its continuity

authentication: ensuring that the identity of a subject or resource is the one claimed

availability: property of being accessible and usable on demand by an authorized entity ISO/IEC 18028 [i.22]

confidentiality: ensuring that information is accessible only to those authorized to have access

cyber herd immunity: a form of immunity to attack wherein a critical mass of vulnerable assets are protected against a certain type of attack such that it becomes unprofitable for attackers to attempt to discover unprotected assets to attack

impact: result of an information security incident, caused by a threat, which affects assets

integrity: safeguarding the accuracy and completeness of information and processing methods

mitigation: limitation of the negative consequences of a particular event

nonce: arbitrary number that is generated for security purposes (such as an initialization vector) that is used only one time in any security session

NOTE: Although random and pseudo-random numbers theoretically produce unique numbers, there is the possibility that the same number can be generated more than once.

non-repudiation: ability to prove an action or event has taken place, so that this event or action cannot be repudiated later

residual risk: risk remaining after risk treatment

risk: potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization

threat: potential cause of an incident that may result in harm to a system or organization

NOTE 1: A threat consists of an asset, a threat agent and an adverse action of that threat agent on that asset (clause 6.2 of Common Criteria part 1 - ISO/IEC 15408-1 [i.27]).

NOTE 2: A **threat** is enacted by a **threat agent**, and may lead to an **unwanted incident** breaking certain pre-defined security objectives.

threat agent: entity that can adversely act on an asset

unwanted incident: incident such as loss of confidentiality, integrity and/or availability

NOTE: See ISO 31000 [i.21].

user: person or process using the system in order to gain access to some system resident or system accessible service

vulnerability: weakness of an asset or group of assets that can be exploited by one or more threats

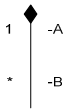
NOTE: A **vulnerability**, consistent with the definition given in ISO/IEC 18028 [i.22], is modelled as the combination of a **weakness** that can be exploited by one or more **threats**.

3.2 Symbols

For the purposes of the present document, the symbols given in OMG UML2 [i.14] and the following apply:

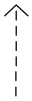
Generalization/Specialization: UML concept showing relationship between entities A and B where the two entities exhibit the property that A (top of arrow) is the general case whereas B is the specific case

EXAMPLE: A countermeasure is a specialized asset.



Composition: UML concept showing relationship between entities A and B where A "is composed of" B

EXAMPLE: Vulnerability "is composed of" a threat and a weakness.



Dependency: UML concept showing relationship between entities A and B where B is dependent upon A

EXAMPLE: Security requirements "depend on" security objectives.

Aggregation: UML concept showing relationship between entities A and B where A "is an aggregate of" B

EXAMPLE: System "is an aggregate of" assets.

3.3 Abbreviations

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

ACK	ACKnkowlegement
ANSI	American National Standards Institute
ARP	Address Resolution Protocol
CAT	CATegory (of Change Request)

CC Common Criteria
CIA Confidentiality Integrity Availability
CIAAA Confidentiality, Integrity, Availability, Authenticity and Accountability
CM Configuration Management
cPP collaborative Protection Profile
CPU Core Processor Unit
DDDS Dynamic Delegation Discovery System
DDoS Distributed Denial of Service
DNS Domaine Name Service
DNSSEC DNS SECurity
DoS Denial of Service
DOS/DoS Denial of Service
EAL Evaluation Assurance Level
ENUM Electronic NUMbering
ERD Entity Relationship Diagram
FAU Functional class AUdit

NOTE: From ISO/IEC 15408-2 [i.28].

FCO Functional class Communication

NOTE: From ISO/IEC 15408-2 [i.28].

FCS Functional class Cryptographic Support

NOTE: From ISO/IEC 15408-2 [i.28].

FDP Functional class user Data Protection

NOTE: From ISO/IEC 15408-2 [i.28].

FIA Functional class Identification and Authentication

NOTE: From ISO/IEC 15408-2 [i.28].

FMT Functional class Security Management

NOTE: From ISO/IEC 15408-2 [i.28].

FPR Functional class Privacy

NOTE: From ISO/IEC 15408-2 [i.28].

FPT Functional class Protection of the TSF

NOTE: From ISO/IEC 15408-2 [i.28].

FRU Functional class Resource Utilization

NOTE: From ISO/IEC 15408-2 [i.28].

FTA Functional class TOE Access

NOTE: From ISO/IEC 15408-2 [i.28].

FTP Functional class Trusted Path/Channels

NOTE: From ISO/IEC 15408-2 [i.28].

HTTP Hyper Text Transmission Protocol
ICMP Internet Control Message Protocol
IMS IP Multimedia Subsystem
IoT Internet of Things
IP Internet Protocol
ISBN International Standard Book Number
ISO International Organization for Standardization

IT	Information Technology
LAN	Local Area Network
MS	Mobile Station
NAPTR	Naming Authority PoinTeR
NASS	Network Attachment Sub-System
NGN	Next Generation Network
NTP	Network Time Protocol
OSI	Open System Interconnection
PP	Protection Profile
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure SHell
ST	Security Targets
SYN	(TCP) SYN(chronize)
TCP	Transport Control Protocol
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TOE	Target Of Evaluation
TSF	TOE Security Function
TSP	TOE Security Policy
TTP	Trusted Third Party
TVRA	Threat Vulnerability and Risk Analysis
UDP	User Datagram Protocol
UML	Unified Modelling Language
URI	Uniform Resource Identifiers

4 Introduction

4.1 Role of TVRA

It is recognized that without an understanding of the system, the threats to the system and a systematic countermeasure cost-benefit analysis that appropriate selection of countermeasures cannot be made. Within ETSI a Threat Vulnerability and Risk Analysis (TVRA) is used to identify risk to the system based upon the product of the likelihood of an attack, and the impact that such an attack will have on the system. The TVRA method described in the present document is primarily aimed at use within the standards domain to give justification for the development of standards based security solutions. In addition the TVRA may be used as the source of parts of a Protection Profile (PP), see ETSI ES 202 382 [i.24]. Large parts of the descriptive text of a PP may in turn be derived from the TVRA:

- security objectives;
- security requirements;
- rationale.

The method described in the present document provides a means of documenting the rationale for designing security countermeasures in a system by application of a systematic method, and by using part of the method to visualize the relationship of objectives, requirements, system design and system vulnerabilities.

The method systematically addresses those aspects of ICT systems covered by standardization and quantifies their assets, vulnerabilities and threats. The primary focus of the TVRA is on the assets of a system and it is required to ensure that they can perform their primary function when subjected to malicious attack. The output of the TVRA is a quantified measure of the risks to the assets and a set of detailed security requirements that will minimize that risk.

For the purposes of analysis all assets are considered to have weaknesses.

The depth of the TVRA changes as the system design becomes more detailed. A TVRA working from the system objectives will identify at a very coarse level the required security functionality to ensure that the objectives can be met without damage to the system. The structure of activities in development of a TVRA is shown in figure 1. The process is shown as recursive wherein in any change to any aspect of the system or its environment requires the process to be restarted.

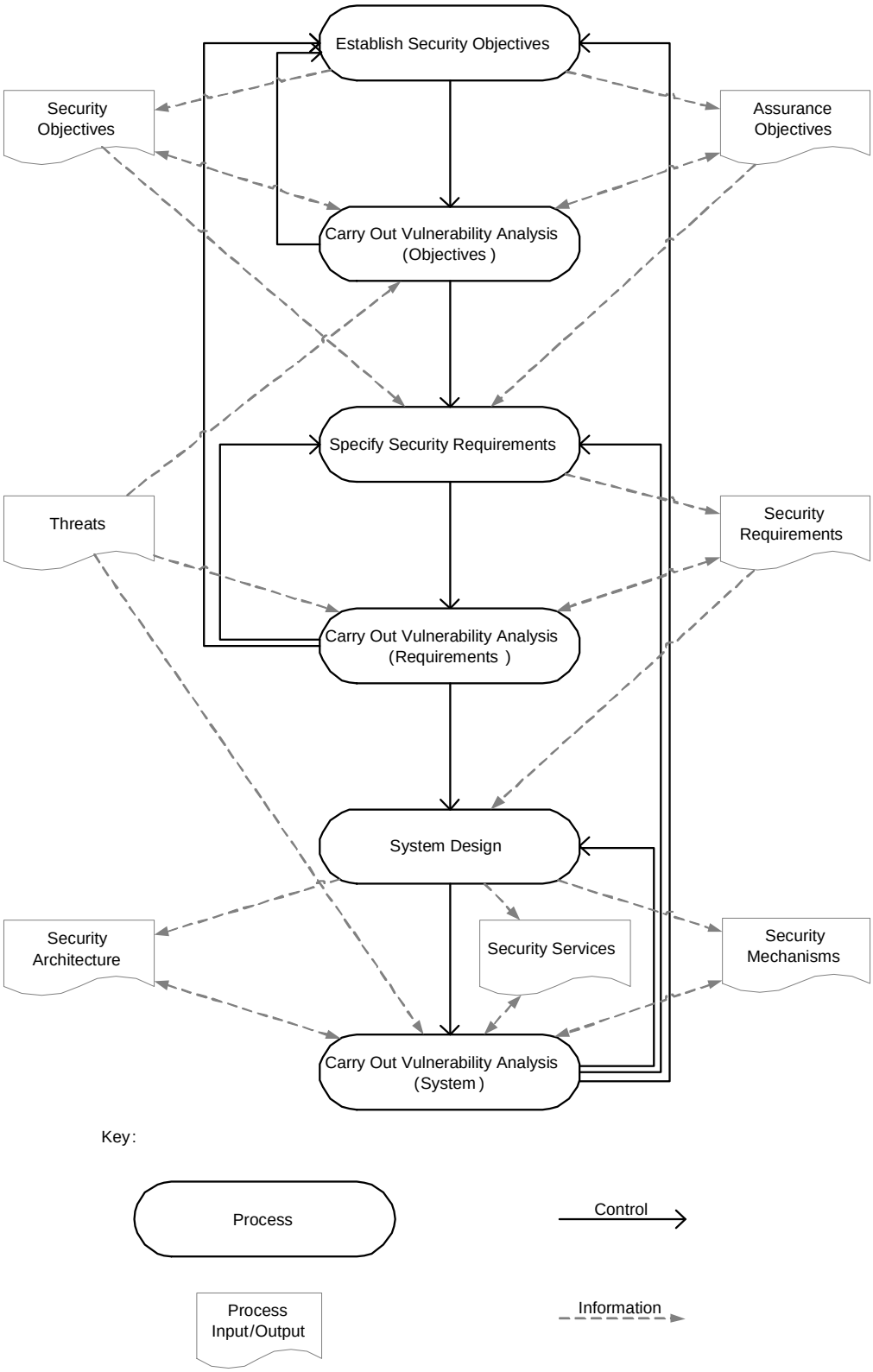


Figure 1: Structure of security analysis and development in standards documents

The purpose of the TVRA is to determine how open to attack the system, or components of the system are. A measure of openness of the system to attack is "attack potential" which combines factors of expertise, availability and resources to give a metric for attack evaluation and this is explored further in clause 6.6.

An alternative view of the nature of TVRA is given in figure 2 showing that any change either internal (say by application of countermeasures) or external to the system requires that the TVRA process is redone.

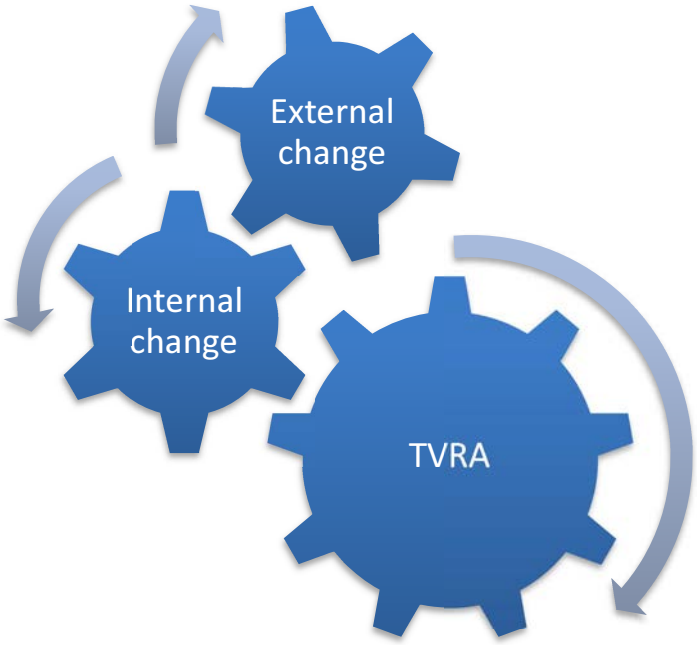


Figure 2: Cyclical nature of TVRA wherein any change requires reapplication of TVRA

4.2 Generic TVRA relationships

One of the keys to a successful TVRA, and also of a successful system design, is the ability to show the relationship of objectives and requirements to the system design. Figure 3 shows the dependencies between system objectives, system requirements and system design highlighting the interplay of security objectives and requirements.

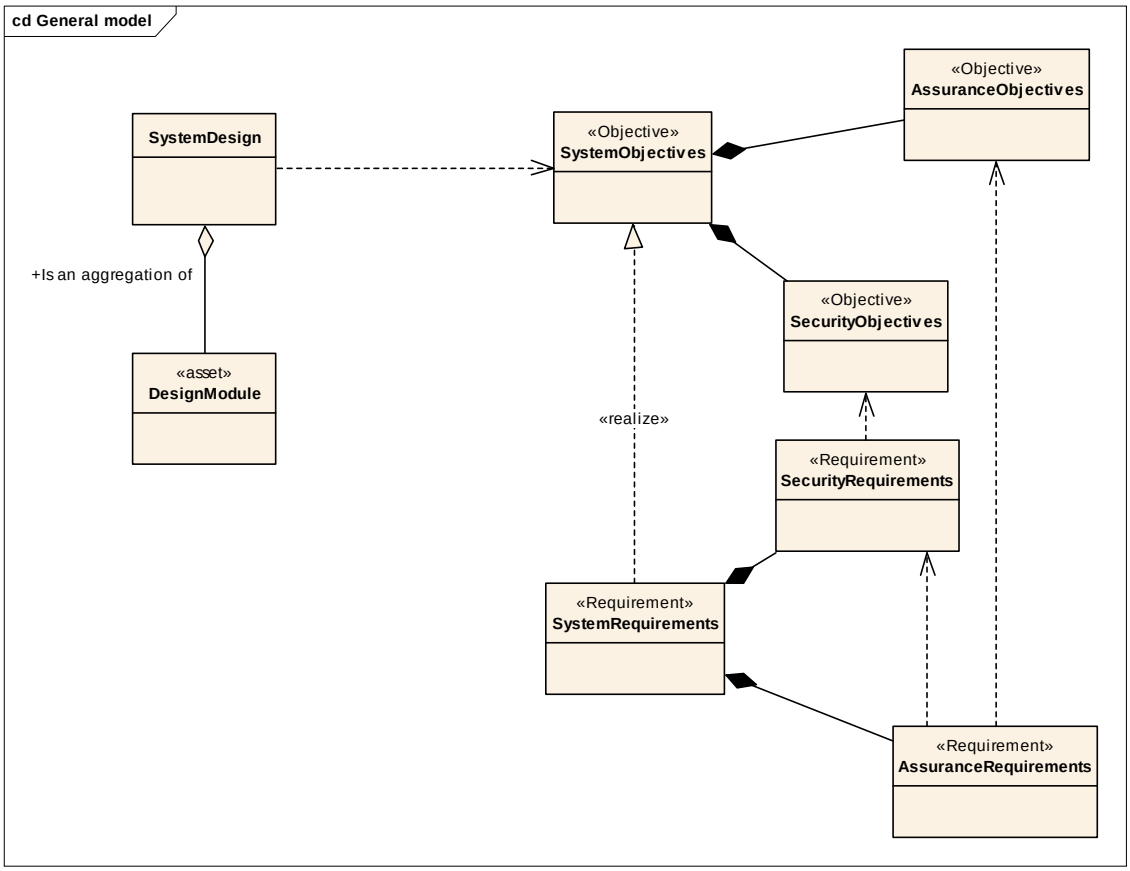


Figure 3: Relationship between system design, objectives and requirements

For most systems the development of system requirements goes far beyond just security and one concern for TVRA is to ensure that the system design is itself robust and therefore has fully documented requirements across all its aspects.

A TVRA requires that both the system being examined (with its catalogued objectives and requirements) and the assets of the system and how it fits to its environment are clearly identified. In the context of TVRA the key relationship is that between a vulnerability and an asset and this is a weighted relationship with the weighting being defined as the risk to the asset due to the associated vulnerability. A pictorial view of the asset-threat-weakness-vulnerability-countermeasure relationship to system design is given in figure 4.

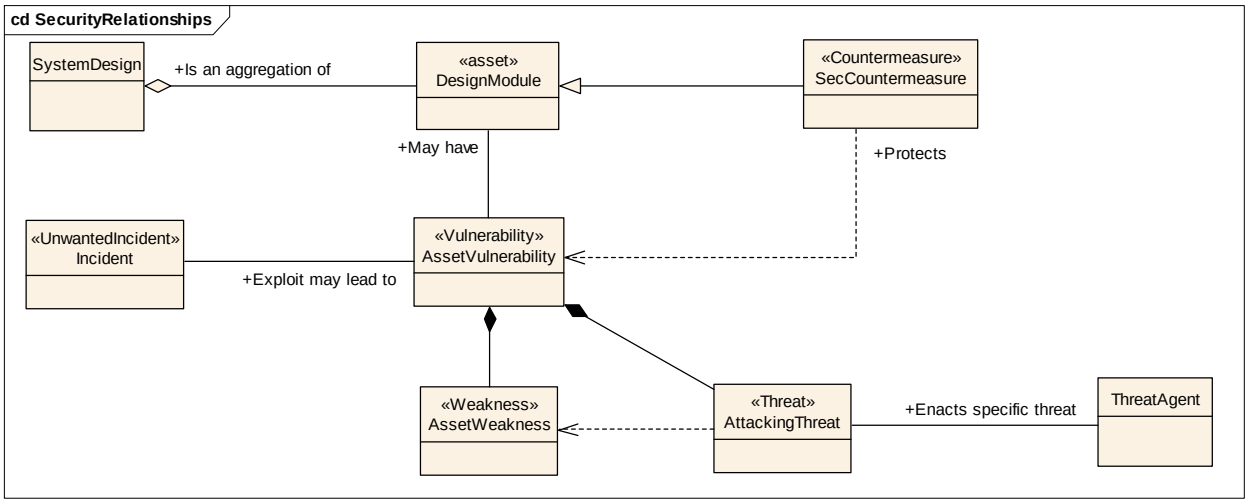


Figure 4: Generic security TVRA model

One of the purposes of security design is to minimize the probability of any instance of the class "unwanted incident" being instantiated. It should be noted that whilst some countermeasures may themselves become system assets, and as such have their own vulnerabilities, many instances of countermeasures will be considered as policies, system guidelines and, if captured early enough, system redesign.

The data types pertaining to the model in figure 4 are given in figure 5. Essentially threats can be classified as one of 5 types:

- Interception.
- Manipulation.
- Denial of service.
- Repudiation of sending, and
- Repudiation of receiving.

NOTE: A more general case may be repudiation of involvement in an action, for communication this can be stated as repudiation of sending or receiving, but may be any other action such as editing or deleting a file (where such actions themselves are considered under manipulation threats).

Similarly security objectives can be classified as one of 5 types (commonly referred to as "CIA" types):

- Confidentiality.
- Integrity.
- Availability.
- Authenticity.
- Accountability.

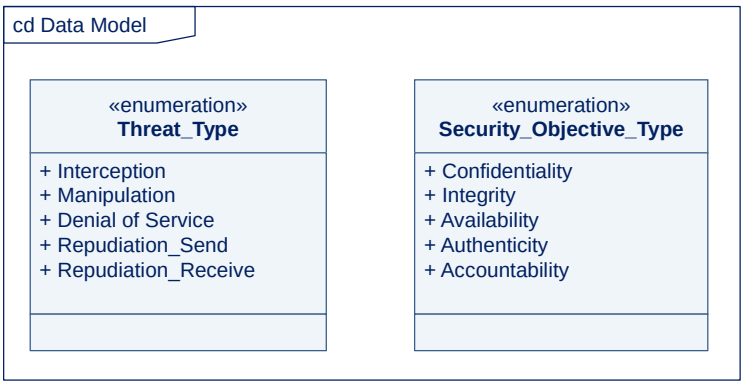


Figure 5: Data types pertaining to security relationship model

4.3 Countermeasure strategies

4.3.0 Overview of strategies

The goal of security design is 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. An essential non-technical component of security strategies is the management of the system and its human components. The non-technical measures are outlined in ISO/IEC 27001 [i.13] and in ISO/IEC 27002 [i.12].

The following strategies are considered within the present document:

- Asset redesign.
- Asset hardening.

4.3.1 Asset redesign

The assumption made prior to analysis is that all assets have weaknesses and the job of the analyst is to identify those weaknesses. Where weaknesses are found and have a large number of associated threats and threat agents there may be a possibility to redesign the asset in such a way as to remove the inherent weaknesses. The viability of this strategy depends on a number of factors including the maturity of the asset design and the relative cost of redesign versus the cost of weakness masking through asset hardening.

4.3.2 Asset hardening

An asset may have some weaknesses that cannot be removed but which may be masked or made inaccessible by the addition of additional features or capabilities to the vulnerable asset or other assets in the system such that the combination of assets in the system presents a lower likelihood of attack, and hence a lower risk to the system.

NOTE: As assets are added to the system the complexity of the system increases and the number of assets and inter-asset relationships to be protected is also increased. This may lead to a point where the resultant system cannot be adequately protected as the system complexity introduced as protection outweighs the set of assets defined for basic system functionality.

4.4 Relationship with Common Criteria evaluation

The primary purpose of an ETSI TVRA is to support and rationalize security standardization, and to support and rationalize system design decisions, where the overall objective of the standard is to minimize risk of exploitation and attack of a compliant system when deployed. In order to consider this fully the TVRA method described in the present document addresses the impact of an attack on the system whereas ISO/IEC 15408 [i.30] primarily addresses the resistance to attack of the system. In this view the TVRA method complements ISO/IEC 15408 [i.30]. A particular objective of the TVRA method is to prepare the justifications for security decisions and that may as a result be referenced in a PP for the security feature.

The structure of the assurance class for vulnerability analysis described in ISO/IEC 15408 [i.30] is slightly different from the structure recommended for a TVRA in the present document, however the two approaches are considered complementary.

Within a final common criteria evaluation [i.30] the vulnerability analysis assurance family assumes that the system design is complete whereas the purpose of the vulnerability analysis exercise in ETSI is to be able to identify vulnerabilities that require the provision of countermeasures, and then to assess the vulnerabilities that exist in the system with the countermeasures applied. The final documented TVRA may be used in the context of common criteria evaluation [i.30] to satisfy those aspects of evaluation found in sections (a), (b) and (c) of a protection profile (see ETSI ES 202 382 [i.24], clauses 5.1.2 through to clauses 5.1.7).

Figure 6 (taken from ETSI EG 202 387 [i.1]) shows a simplified view of the relationships between the components of Common Criteria Protection Profiles (PP), Security Targets (ST) and Targets Of Evaluation (TOE). The standardization process fits primarily in the "Consumer side" of the figure.

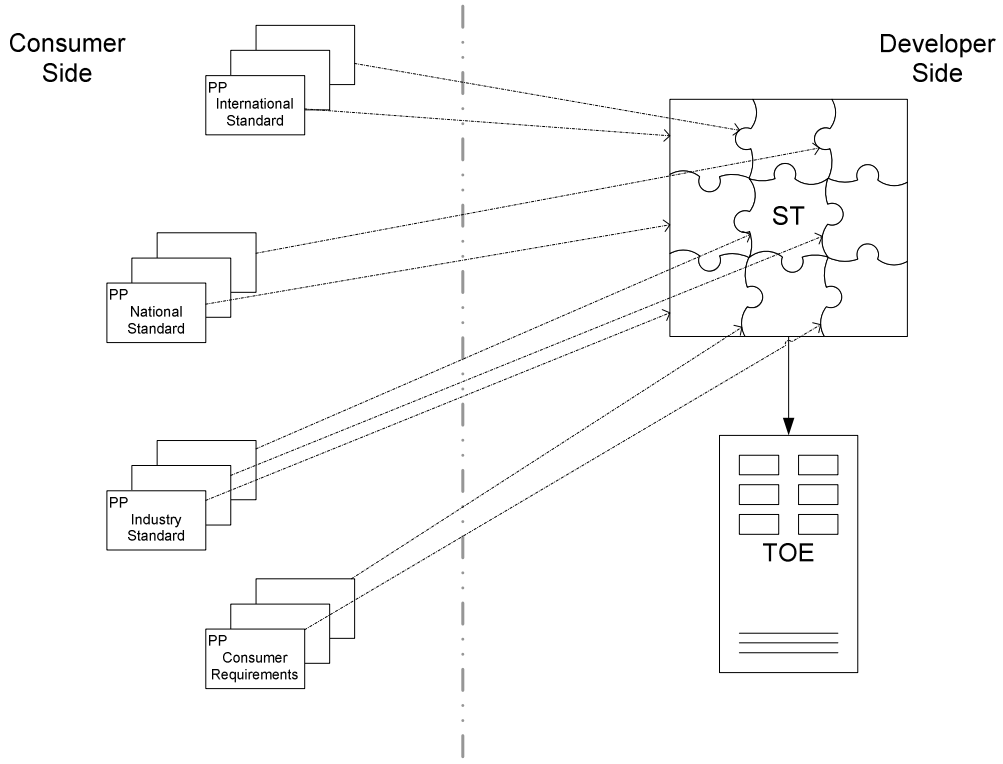


Figure 6: Relationship between PPs, STs and TOEs

The approach outlined in the present document that identifies a close relationship between a PP and a technical standard is also considered in the development of collaborative Protection Profiles (cPPs) within the Common Criteria groups that propose the cPP as the basis for interoperability between products conforming to the cPP [i.11] in like manner to the purpose of standards to assure interoperability.

5 TVRA method

5.1 Overview

5.1.0 Introduction

The TVRA method involves a systematic identification of the unwanted incidents to be prevented in the system, and for the system itself, identifying the assets it is composed of and their associated weaknesses, the threats and the threat agents that will attack the system, before determining the risk to the system by modelling the likelihood and impact of attacks on the system's vulnerabilities.

The TVRA method derives from the model shown in figure 4. The TVRA models a system consisting of assets. An asset may be physical, human or logical. **Assets** in the model may have **Weaknesses** that may be attacked by **Threats**. A **Threat** is enacted by a **Threat Agent**, and may lead to an **Unwanted Incident** breaking certain pre-defined security objectives. A **Vulnerability**, consistent with the definition given in ISO/IEC 18028 [i.22], is modelled as the combination of a **Weakness** that can be exploited by one or more **Threats**. When applied, **Countermeasures** protect against **Threats** to **Vulnerabilities** and reduce the **Risk**.

The TVRA method process consists of the following steps:

1) Identification of the Target Of Evaluation (TOE) resulting in a high level description of the main assets of the TOE and the TOE environment and a specification of the goal, purpose and scope of the TVRA.

2) Identification of the objectives resulting in a high level statement of the security aims and issues to be resolved.

3) Identification of the functional security requirements, derived from the objectives from step 2.

4) Inventory of the assets as refinements of the high level asset descriptions from step 1 and additional assets as a result of steps 2 and 3.

5) Identification and classification of the vulnerabilities in the system, the threats that can exploit them, and the unwanted incidents that may result.

6) Quantifying the occurrence likelihood and impact of the threats.

7) Establishment of the risks.

8) Identification of countermeasures framework (conceptual) resulting in a list of alternative security services and capabilities needed to reduce the risk.

9) Countermeasure cost-benefit analysis (including security requirements cost-benefit analysis depending on the scope and purpose of the TVRA) to identify the best fit security services and capabilities amongst alternatives from step 8.

10) Specification of detailed requirements for the security services and capabilities from step 9.

Each step in the method has guidance attached to lead the analyst. In particular for steps 6 and 9, which involves detailed calculations of the likelihood and impact values and cost and benefit of alternative countermeasures, the use of repeatable metrics is essential to the repeatability of the analysis over time. The metrics used in step 5 are developed from the guidance given in ETSI ETR 332 [i.9] and ISO/IEC 15408 [i.30]. One characteristic of the method is to include an evaluation of whether an attack exploiting a vulnerability can be automated thereby offering an additional metric to be used in assessing risk. The product of occurrence likelihood and impact values from step 5 gives a measure of the risk to the asset. A countermeasure will reduce the likelihood of the threat being successful and/or reduces its impact. Step 8 identifies alternative countermeasures to protect the system and its assets against threats. The costs and benefits of each countermeasure are evaluated in step 9 in order to identify those that are the most effective at removing threats at an acceptable cost.

The application of countermeasures adds assets to the system and may create new vulnerabilities, indicating that the TVRA will need to be undertaken again, and the method should be repeated until all the risks have been reduced to an acceptable level. Furthermore, by allowing the analysis to be rerun when attack likelihood changes, the risk to the system may be re-evaluated as knowledge of new or revised attacks becomes available.

A database should be used to store the decomposition of the system into its core elements (assets), threats, threat agents, weaknesses, vulnerabilities and countermeasures such that the analysis can be repeated whenever the design or the environment changes.

NOTE 1: The database is to be compiled by the analyst/designer. A sample database structure is provided in annex E.

NOTE 2: The database structure provided in annex E is referred to as the eTVRA and is intended as an interactive tool to support the TVRA method.

The method systematically addresses those aspects of telecommunications systems covered by standardization and quantifies their assets, vulnerabilities and threats. The primary focus of the TVRA is on the assets of a system and is required to ensure that they can perform their primary function when subjected to malicious attack. The output of the TVRA is a quantified measure of the risks to the assets and a set of detailed security requirements that will minimize that risk.

For the purposes of analysis all assets are considered to have weaknesses.

The TVRA method identifies the assets of a system, the weaknesses of each asset and the potential threats associated with these weaknesses. Publishing the details of a particular weakness is likely to increase the risk to the system, particularly where a means of exploiting the weakness is also published unless countermeasures are implemented promptly.

NOTE 3: The term threat agent is used in the present document to refer to a specific means to enact a threat in order to exploit a weakness.

It should be noted that in some cases the determination of a countermeasure to a particular threat will not automatically lead to its deployment. Step 9 of the TVRA method provides a means to analyse the costs and benefits of deploying each countermeasure.

5.1.1 Target of Evaluation description

5.1.1.0 Introduction

ISO/IEC 15408-1 [i.27] requires that a brief but clear description of the Target Of Evaluation (TOE) is given in order to make the security aspects of the TOE clear. A similar approach is adopted in the TVRA method and the scope of the TVRA should be considered in the same way that a TOE is considered in ISO/IEC 15408-1 [i.27] and in the PP pro forma defined in ETSI ES 202 382 [i.24]. It is recognized that an attack on any asset may affect not only the asset but also the system in which the asset exists (the environment).

5.1.1.1 Security environment

The security environment describes the security aspects of the environment in which the asset is intended to be used. It shall include:

- Security assumptions:
  - the intended use of the implementation;
  - the physical, user and connection aspects of the environment in which an implementation will operate.
- Assets:
  - the assets with which the asset under analysis will interact with;
  - the nature of the asset's interaction with other assets.
- Threats and threat agents:
  - all threats against which specific protection is required within either the implementation of a standard or its expected environment;
  - the threat agents that will be used to enact the identified threats.
- Organizational security policies:
  - any security policies or rules with which an implementation of a standard shall comply.

The description of the security environment shall be tabulated following the format illustrated in the example.

EXAMPLE:

A Security Environment		
a.1 Assumptions		
TVRA-id	**Summary text**	**Citation**
a.1.1	ENUM is used to resolve a given telephone number (E.164 identity) to a known IP address	IETF RFC 3761 [i.15] ETSI TS 102 051 [i.7] ETSI TR 102 055 [i.4]
a.1.2	ENUM runs over DNS	
..	..	..
a.2 Assets		
a.2.1	DNS records in Leaf server	
a.2.2	NAPTR record in Leaf server	
..	..	..
a.3 Threats		
a.3.1	Confidentiality (DNS records are intended to be public)	
a.3.2	Integrity (DNS records are intended to be accurate)	
..	..	..
a.4 Threat agents		
a.4.2	overload of communication	
a.4.3		
..	..	..
a.5 Security policies (OPTIONAL)		
a.5.1		
a.5.2		

5.1.1.2 Security objectives

A TVRA shall contain a definition of the security objectives of both the asset and its environment. These objectives are expected to cover the assumptions, threats and policies described in the asset security environment (see clause 5.1.1.1). They should be expressed in broad terms rather than in detail and should be segregated into two distinct groups, thus:

- Security objectives for the asset:
  - it should be clear which aspects of the identified threats and policies are addressed by each objective;
  - if the base security standard specifies a protocol, it is likely that the asset security objectives will be specified in the Stage 1 (or equivalent) specification.
- Security objectives for the environment:
  - it should be clear which aspects of the identified threats and policies are expected to be addressed by the environment because they are not covered (either wholly or in part) by the asset security objectives;
  - communications standards rarely specify requirements for the environment so it is unlikely that the security objectives for the environment will be stated explicitly in the base security standard or any associated document.

EXAMPLE:

B Security Objectives		
b.1 Security objectives for the asset		
b.1.1	The asset should ensure that only registered users may access the system	
b.1.2		
..	..	..
b.2 Security objectives for the environment		

5.1.1.3 Security requirements

5.1.1.3.1 The relationship between security objectives and security requirements

The distinction between security objectives and security requirements is an important one to make. An objective is the expression of what a security system should be able to do in very broad terms whereas a requirement is a more detailed specification of how an objective is achieved. As an example, the following statement is a security objective for an asset.

EXAMPLE 1: The asset should ensure that only registered users may access the system.

One of the security requirements associated with this objective could be:

EXAMPLE 2: A user shall be successfully identified and authenticated to the asset by means of a user name and password before all other interactions between the asset and that user.

NOTE: It would not be unusual for a single objective to be realized by the implementation of more than one requirement nor for a single requirement to partially implement more than one objective.

5.1.1.3.2 Security requirements statements

Security requirements should be identified for both the asset and, where applicable, its environment. The asset security requirements should be classified into the following groups:

- Asset security functional requirements:
  - an identification of each of the security-related functional requirements specified in the base security standard and an indication of where in the standard the detailed requirement can be found;
  - where possible, an indication of which of the functional components defined in ISO/IEC 15408-2 [i.28] the requirement represents.
- Asset security assurance requirements:
  - an indication of the Evaluation Assurance Level (EAL) that an implementation of the base security standard could be expected to meet. As there are likely to be many implementations in a number of different application areas, the EAL requirement could be expressed as a range (e.g. EAL3 - EAL5);
  - where possible, an identification of any specific assurance components from ISO/IEC 15408-3 [i.29] which will apply to an implementation;
  - where necessary, a specification of any essential assurance requirements which are not included in ISO/IEC 15408-3 [i.29].

The specification of security requirements for the environment is optional and should only be included in the analysis if security objectives for the environment are identified earlier in the analysis (see clause 5.1.1.2). If requirements for the environment are included, they should be presented in the same way as functional requirements for the asset.

EXAMPLE:

C Security Requirements			
c.1 asset security requirements			
c.1.1 asset security functional requirements			
c.1.1.1	NGN R1 IMS authentication shall support early deployment scenarios (with support for legacy equipment's).	FIA_UAU.3	ETSI TS 187 001 [i.26] clause 4.2, ISO/IEC 15408-2 [i.28] clause 11.4.2
c.1.1.1	In non-early deployment scenarios, IMS authentication shall be independent from access authentication.	FIA_UAU.3	ETSI TS 187 001 [i.26] clause 4.2, ISO/IEC 15408-2 [i.28] clause 11.4.2
..	..	..	..
c.1.2 asset security assurance requirements			
c.1.2.1			
..	..		..
c.2 Environment security requirements (OPTIONAL)			
c.2.1			

5.1.1.3.3 Interaction with ISO/IEC 15408

In the preceding clause it is recommended that where possible assurance and functional components from ISO/IEC 15408-2 [i.28] and ISO/IEC 15408-3 [i.29] should be identified. The guidance to the application of Common Criteria in ETSI deliverables, ETSI EG 202 387 [i.1], should be used as source material in this case. A summary of the relevant content of ETSI EG 202 387 [i.1] follows.

ISO/IEC 15408-2 [i.28] identifies a set of functional components which cover the major elements of any security product or process and these are defined in the following classes (ISO/IEC 15408-2 [i.28] component name in brackets):

- Security audit (FAU).
- Communication (FCO).
- Cryptographic support (FCS).
- User data protection (FDP).
- Identification and authentication (FIA).
- Security management (FMT).
- Privacy (FPR).
- Protection of the Target of Evaluation Security Functions (FPT).
- Resource utilization (FRU).
- Target of Evaluation access (FTA).
- Trusted path/channels (FTP).

The components can be used in the development of requirements at both an abstract level and at the detail development level.

The developer needs to be aware of the functional components and to report their use.

EXAMPLE: A countermeasure to prevent masquerade may require that the identity is presented and validated, then authenticated, prior to system access. To implement this countermeasure will require a design that includes components "User identification before action" and "User authentication before action" (FIA_UID.2 and FIA_UAU.2 respectively in ISO/IEC-15408-2 [i.28]).

Table 1: Evaluation service level summary as specified in ISO/IEC 15408-3 [i.29]

Assurance Class	Assurance Family	Assurance Component by Evaluation Assurance Level (EAL)						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	Security architecture (ADV_ARC)		1	1	1	1	1	1
	Functional specification (ADV_FSP)	1	2	3	4	5	5	6
	Implementation representation (ADV_IMP)				1	1	2	2
	TSF internals (ADV_INT)					2	3	3
	Security policy modelling (ADV_SPM)						1	1
	TOE design (ADV_TDS)		1	2	3	4	5	6
Guidance documents	Operational user guidance (AGD_OPE)	1	1	1	1	1	1	1
	Preparative procedures (AGD_PRE	1	1	1	1	1	1	1
Life-cycle support	CM capabilities (ALC_CMC)	1	2	3	4	4	5	5
	CM scope (ALC_CMS)	1	2	3	4	5	5	5
	Delivery (ALC_DEL)		1	1	1	1	1	1
	Development security (ALC_DVS)			1	1	1	2	2
	Flaw remediation (ALC_FLR)							
	Life-cycle definition (ALC_LCD)			1	1	1	1	2
	Tools and techniques (ALC_TAT)				1	2	3	3
Security Target evaluation	Conformance claims (ASE_CCL)	1	1	1	1	1	1	1
	Extended components definition (ASE_ECD)	1	1	1	1	1	1	1
	ST introduction (ASE_INT)	1	1	1	1	1	1	1
	Security objectives (ASE_OBJ)	1	2	2	2	2	2	2
	Security requirements (ASE_REQ)	1	2	2	2	2	2	2
	Security problem definition (ASE_SPD)		1	1	1	1	1	1
	TOE summary specification (ASE_TSS)	1	1	1	1	1	1	1
Tests	Coverage (ATE_COV)		1	2	2	2	3	3
	Depth (ATE_DPT)			1	1	3	3	4
	Functional tests (ATE_FUN)		1	1	1	1	2	2
	Independent testing (ATE_IND)	1	2	2	2	2	2	3
Vulnerability assessment	Vulnerability analysis (AVA_VAN)	1	2	2	3	4	5	5

ETSI TR 187 011 [i.2] provides guidelines and method on how to apply ISO/IEC 15408-2 [i.28] requirements to ETSI standards. ETSI TR 187 002 [i.3] provides examples of security functional requirements.

NOTE: The EAL model is being updated in the development of cPPs as outlined in [i.11] and in due course, as noted in [i.11], evaluation is to be made against the content of the cPP.

5.1.2 Threats and threat agents

Threats to a telecommunications system are fairly restricted and fall into a small set of easily identified operations. The means to enact these threats are conversely many and varied and it is the "agent of threat" that will take most time to identify and that is the source of the risk to the system.

Threats in ICT belong to one of the following groups (showing subclasses of each threat) as outlined in clause 4.2 and shown in a tree in figure 7:

- Interception:
  - Eavesdropping:
    - A breach of confidentiality by unauthorized monitoring of communication.
- Manipulation:
  - Masquerade ("spoofing"):
    - The pretence of an entity to be a different entity. This may be a basis for other threats like unauthorized access or forgery.

- Loss or corruption of information:
  - The integrity of data (transferred) is compromised by unauthorized deletion, insertion, modification, reordering, replay or delay.
- Unauthorized access:
  - An entity accesses data in violation to the security policy in force.
- Forgery:
  - An entity fabricates information and claims that such information was received from another entity or sent to another entity.

- Repudiation:
  - An entity involved in an exchange subsequently denies the fact.
- Denial of service:
  - An entity fails to perform its function or prevents other entities from performing their functions.

NOTE: Denial of Service may be considered as a specialism of Manipulation but is shown as a discrete threat group as it may combine elements of all groups and further is sufficiently prevalent to require such separation.

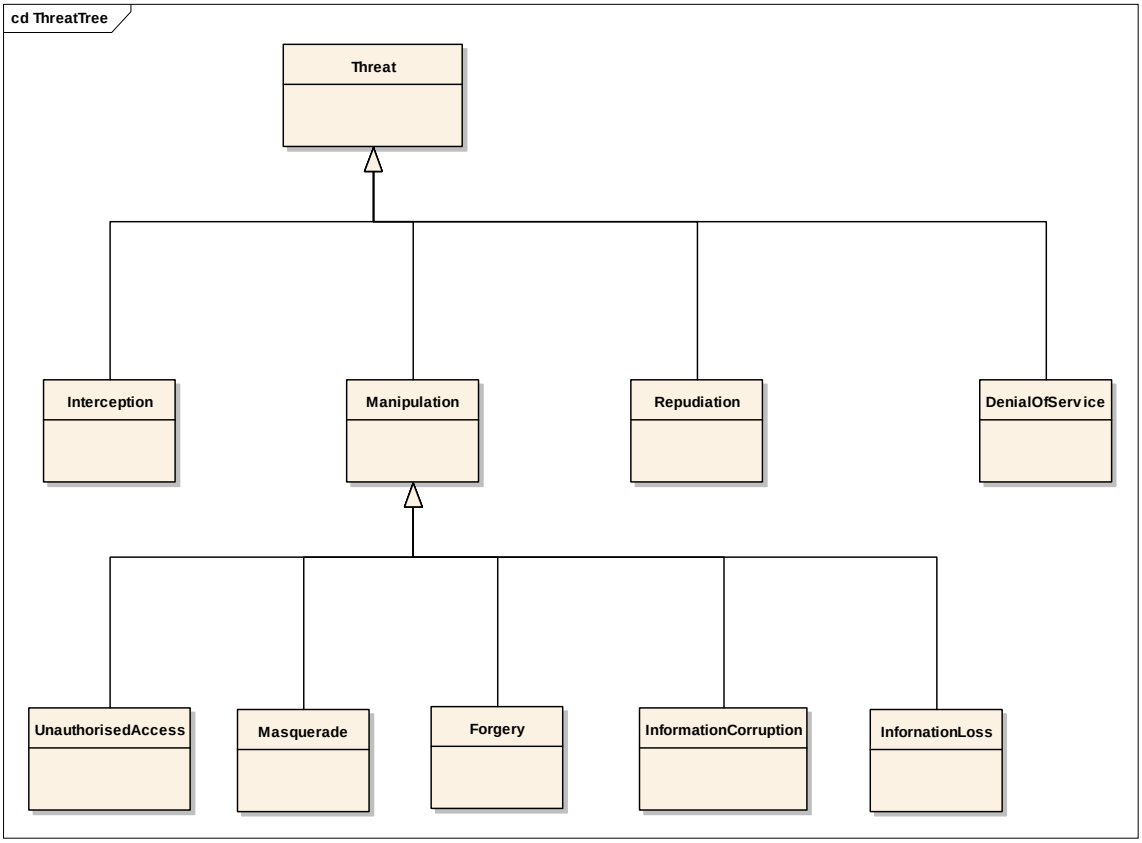


Figure 7: Threat tree

Table 1A shows how the principle CIAAA security objective classifications are vulnerable to specific types of threat.

Table 1A: Threats to security objective types

Threat	Objective type				
	Confidentiality	Integrity	Availability	Authenticity	Accountability
Interception (eavesdropping)	X				
Unauthorized access	X	X		X	X
Masquerade	X	X		X	X
Forgery		X	X	X	X
Loss or corruption of information		X	X		
Repudiation		X		X	X
Denial of service			X		

5.2 Actors and roles

For the purpose of security standardization, only technical security countermeasures are considered, which means that relevant actors to consider are *users*. A user is defined as a person or process using the system in order to gain access to some system resident or system accessible service. Users can further be categorized dependent on whether they belong to the organization running the services (internal users) or whether they access the services as external users.

Each time a user accesses a service, the user will take on a role. In some cases there will be a one-to-one relationship between a user and a role, i.e. the user will always stay in the same role. In other cases there will be a one-to-many relationship between a specific user and the possible roles the user can play. This latter case is the normal telecommunications and ICT case in which the same user may act as a call initiator, call receiver, registrant, etc.

The following gives a high level classification of the most common roles:

- network operators (*private or public*);
- service providers (Bearer Service Providers or Value Added Service Providers);
- service subscribers/service customers;
- service end users;
- equipment/software vendors.

Some security measures may require actors to enforce the role of a Trusted Third Party (TTP). An important security issue is how these actors should be allowed to interact with each other in the context of the service or function they are using.

5.3 Rationale

To comply with ISO/IEC 15408-1 [i.27] a PP should provide a rationale, for both the security objectives and the security requirements. It should explain in detail how the security objectives and the security requirements address the threats identified in the asset's security environment. Thus one of the purposes of the TVRA is to provide this rationale and it may, therefore, be referred to in the PP as the source of the rationale. The association of objectives, requirement, threats and assets within a TVRA provides the rationale for the selection of the security architecture and the countermeasures described by the PP.

6 Method process

6.1 Overview

The TVRA method systematically identifies the assets, and the relationships between assets (where the relationship may be considered as an intangible asset), and then for each asset, establishes the weaknesses this asset may have, assesses how practical it is to attack this weakness and assesses the resulting risk.

For each step in this method a number of metrics are defined to assist the user of the method.

6.2 Step 1: Identification of Target Of Evaluation (TOE)

A successful TVRA depends on a clear definition of the scope, purpose and goal of the analysis. A comprehensive description of the Target Of Evaluation (TOE) and its environment should be produced. A TOE should be considered to represent a "system under standardization". At this early stage it is essential that the boundary between the system (the target of standardization) and its environment is defined. Without this definition, it is likely that at least some of the security objectives (step 2) specified will be impossible to meet. There are no strict rules on how to determine what is in the system and what is in its environment but, as a guide, in communication systems it is likely that the boundary will pass through interfaces rather than entities and that human users will exist within the environment rather than the system. It is also likely that the system will comprise a number of easily identifiable assets which may be decomposed into multiple assets themselves at a later stage in the development process. The TOE description should include a high level description of the main assets of the TOE and its environment. The simple example in figure 8 shows graphically the boundary between a system and its environment.

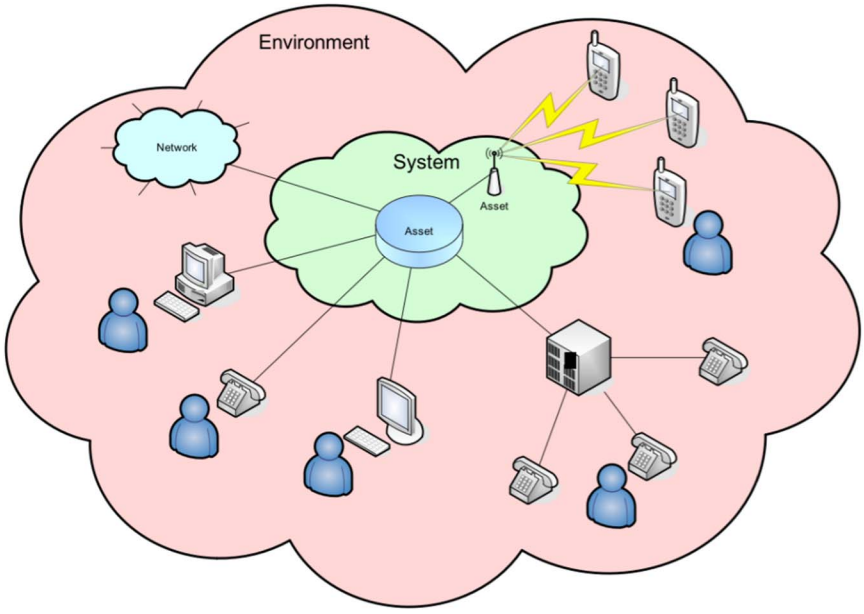


Figure 8: Example of a security system with its environment

The scope defines the boundary of the analysis and may be used to support the identification of the TOE and the TOE environment. It is essential to the analysis that the scope description is specific and unambiguous and that it clearly identifies the assets of both TOE and TOE environment.

The purpose and goal of the analysis is to help to direct the TVRA activities and may be used to verify the quality of the analysis output.

The use of UML use case diagrams, class diagrams, deployment diagrams, object diagrams and behavioural diagrams to model the TOE and the TOE environment may later be used to identify the assets and may assist in other analysis activities. If such methods are used the diagrams should be part of the TOE description and analysis documentation.

The abstraction level required of the TOE and TOE environment depends on the purpose of the analysis and the information available. The TOE description may include an outline and details of the architecture, relevant applications, reference points, information flows and possible attack interfaces. Attack interfaces are specific assets (such as reference points) in the TOE environment or the interfaces between the TOE and the TOE environment that a threat agent can use to launch an attack against one or more weaknesses in the assets. Attack interfaces may also be procedural (exploiting a weakness in a security procedure).

ISO/IEC 15408-1 [i.27] provides guidelines on producing TOE and TOE environment descriptions. ETSI TR 187 002 [i.3] provides examples of TOE descriptions.

6.3 Step 2: Identification of objectives

Security objectives identify the broad aims of a standard or system in terms of the protection to be given to users and information within the framework of the CIAAA attributes. Without such objectives it is difficult to develop a coherent set of security requirements and, therefore, complete a meaningful TVRA exercise. Security objectives should be specific to the target system and clearly specify the CIAAA attributes affected. ETSI TR 187 011 [i.2] provides guidelines on how to write security objectives and ETSI TR 187 002 [i.3] provides examples of security objectives. The following gives a demonstration of security objectives identification and specification for the CIAAA attribute availability.

Within the context of standardization there are a number of objectives for security that are intended to ensure availability of the network and customer confidence. These objectives break down to the following technical security issues for most telecommunications services:

- charging fraud;
- protection of privacy; and
- ensuring availability of the offered services.

The goals for ICT services should therefore aim to reduce these risks by reducing the ability to mount attacks that prevent the achievement of these objectives.

The following technical objectives for ICT services security hold:

- Prevention of masquerade:
  - being able to determine that a user claiming to be Alice is always Alice, Bob is always Bob, and Bob cannot pretend to be Alice;
  - applies to both masquerade of the user and of the system or service.
- Ensure availability of the ICT services:
  - the service is accessible and usable on demand by an authorized entity.

NOTE: In general, a user expects to be able to place a call, and complete the call without being cut off in the middle.

- Maintain privacy of communication:
  - where the parties to a call communicate across public networks mechanisms should exist to prevent eavesdropping;
  - the only delivery points for communication have to be the legitimate parties to the call.

6.4 Step 3: Identification of functional security requirements

The system requirements are dependent on the system objectives identified in step 1 and have two specialisms shown in figure 8a identifying security and assurance requirement specialisms.

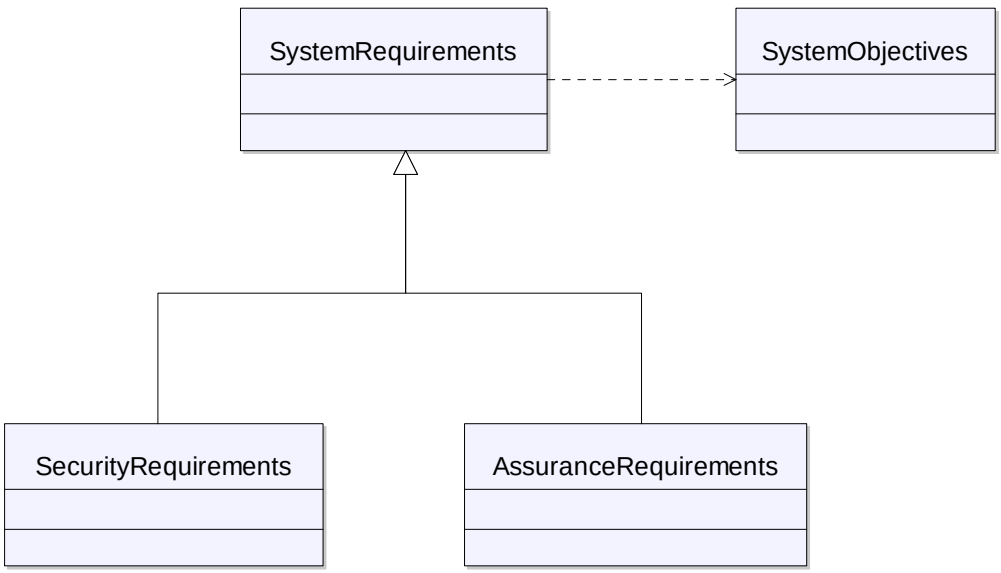


Figure 8a: Dependency relationship between requirements and objectives

When building systems the use of ISO/IEC 15408-2 [i.28] functional capabilities offer a means to unambiguously state requirements. ETSI TR 187 011 [i.2] provides guidelines and method on how to apply ISO/IEC 15408-2 [i.28] requirements to ETSI standards. ETSI TR 187 002 [i.3] provides examples of security functional requirements.

6.5 Step 4: Systematic inventory of the assets

It is important to document the nature of any asset of the system and the complexity of the technology used in the construction of the asset and any information relating to the technology used in the asset that is available in the public domain. Between them these three aspects determine in large part the level of understanding of the asset.

The life expectancy of the asset is used in consideration of the time taken to develop and run an attack (develop a threat agent for a specific attack type). This may be affected by aspects such as the frequency with which a key or password is updated, and the duration in which the asset is expected to be in operational use.

NOTE 1: If an asset is protected by a key or password and the attack is based on key or password guessing then the frequency of key or password update can be a countermeasure.

Three kinds of **assets** are defined:

- physical assets:
  - equipment;
- human assets; and
- logical assets:
  - the information stored in and handled by the physical assets.

An asset is at **risk** when a weakness exists and a **viable threat** is present. The seriousness of the **vulnerability** depends on the **value** of the **asset** and the **likelihood** of the **weakness** to be exploited by the threat.

Systematic inventory of the assets requires a thorough evaluation of the system at hand. A first round of this evaluation should be performed by addressing typical scenarios appropriate to the system under discussion:

- Take a typical scenario.
- Analyse the physical assets by following the scenario.
- Analyse the human assets involved in the scenario.
- Analyse which logical assets exist in each of the physical assets.
- Analyse which logical assets are handled by the human assets.
- Consider other scenarios which may highlight different assets and repeat the process until no further assets are found.

When the system under discussion has multiple aspects, repeat this process for all aspects of the system until no more assets are found.

The use of UML use case diagrams, class diagrams and object diagrams may assist in the analysis of the system to identify the assets. If such methods are used the diagrams should be used in the analysis documentation.

The eTVRA database may be used to store the decomposition of the assets and their relationships from the TOE and the database definition (see annex E) contains a number of tables to store the definition of the asset and its relationship to other assets and to the system it is a member of.

In order to catalogue an asset the following attributes and relationships shall be identified:

- The system in which the asset resides.

NOTE 2: An asset can exist in more than one system and a system can contain many assets (a many-to-many relationship).

- The asset parent-child-sibling relationships if any exist.

NOTE 3: An asset can be a parent to one or more other assets and such relationships are captured. Similarly an asset can be a peer (sibling) to another asset and such relationships are captured.

It is the impact on the system from a successful attack on a specific asset that is particularly important when analysing a TOE. Table 2 identifies the three levels of impact used to evaluate assets in step 4 of the TVRA process.

If a system is composed of multiple assets, which should be considered as the default, any non-redundant system will fail if one system component fails, however a redundant system may only fail if multiple assets are subject to attack. Thus whilst the bulk of the TVRA method addresses the impact and attacks on a single asset due consideration should be made for the cumulative impact of attacks on multiple assets of the system, or for the cumulative impact of repeated attacks on a single asset.

Table 2: Asset impact

Impact	Explanation	Value
Low	The concerned party is not harmed very strongly; the possible damage is low.	1
Medium	The threat addresses the interests of providers/subscribers and cannot be neglected.	2
High	A basis of business is threatened and severe damage might occur in this context.	3

System decomposition, wherein a system, the TOE, is decomposed to its constituent assets such that each asset shall be subject to analysis, this requires that a TOE boundary is established for each asset within the boundary of the containing system. In most cases the boundary of an asset, if modelled as an abstract class with an exposed interface and accessible data, is identifiable as the expected entities that can access the exposed interfaces.

6.6 Step 5: Systematic identification of vulnerabilities and threat level

6.6.0 Overview

In order to identify potential vulnerabilities in a TOE and its environment it is first necessary to determine where its weaknesses exist, what, if any, viable threats could exploit those weaknesses and what harm could be caused by an attack on each weakness. It is only a weakness for which such a threat exists that can be considered to be a vulnerability within the system.

6.6.1 Identification of weakness

A weakness within a system offers a potential point of attack for a threat agent. However, viable attacks will not necessarily be possible against all weaknesses. It is only those where an attack could realistically be mounted that can be considered to be vulnerabilities.

6.6.2 Identification of a vulnerability

Possible attack interfaces need to be identified and all possible attacks need to be elaborated. This is in addition to those already identified in step 1 and involves a further analysis of such.

6.6.3 Identification of attack method

6.6.3.0 Introduction

The difficulty of mounting a successful attack is determined by a number of factors that are defined and described in detail in the remainder of this clause.

6.6.3.1 Assessment of the practicality

6.6.3.1.0 Core assessment

An evaluator shall determine the attack potential associated with each of the vulnerabilities identified and shall consider the effect of the vulnerability becoming publicly known. That is, an attacker would not have to repeat the analysis to identify the vulnerability, but would only have to perform the exploitation. In some instances knowledge of the vulnerability would not immediately facilitate exploitation because considerable further analysis would be required to permit the development of an attack method.

In direct attacks against probabilistic or permutational mechanisms, the issue of exploitation will normally be the most important, since potential vulnerabilities in these mechanisms will often be self-evident, however this may not always be the case. With cryptographic mechanisms, for example, knowledge of subtle potential vulnerabilities may considerably affect the effectiveness of a brute force attack. Knowledge that users of a system tend to choose first names as passwords will have a similar effect. For vulnerability testing above AVA_VAN.1 (see ISO/IEC 15408-3 [i.29] and ETSI EG 202 387 [i.1] for further consideration of the Common Criteria Vulnerability Analysis Assurance class), the initial identification of potential vulnerabilities will become a much more important consideration, since the existence of difficult to uncover potential vulnerabilities may be promulgated, often rendering exploitation trivial.

The factors defined here are derived from those defined in clause B.4 of the Common Criteria Evaluation methodology [i.32] using the **weighted summation method** to calculate the overall attack potential.

The following factors shall be evaluated during analysis to determine the weight of the attack potential required to exploit a vulnerability:

- System knowledge.
- Time.

- Expertise.
- Opportunity.
- Equipment.

6.6.3.1.1 Knowledge factor

The knowledge factor is derived from that defined in clause B.4 of the Common Criteria Evaluation methodology [i.32] using the weighted summation method to calculate the overall attack potential.

Knowledge of the asset refers to specific expertise in relation to the asset. This is distinct from generic expertise, but not unrelated to it. Identified levels are as follows:

- Public information concerning the asset (e.g. as gained from the Internet).
- Restricted information concerning the asset (e.g. knowledge that is controlled within the developer organization and shared with other organizations under a non-disclosure agreement).
- **Sensitive** information about the asset (e.g. knowledge that is shared between discreet teams within the developer organization, access to which is constrained only to members of the specified teams).
- **Critical** information about the asset (e.g. knowledge that is known by only a few individuals, access to which is very tightly controlled on a strict need to know basis and individual undertaking).

The knowledge of the asset may graduate according to design abstraction, although this can only be done on an asset by asset basis. Some asset designs may be public sources (or heavily based on public sources) and therefore even the design representation would be classified as public or at most restricted, while the implementation representation for other assets is very closely controlled as it would give an attacker information that would aid an attack and is therefore considered to be sensitive or even critical.

NOTE: Open source software is an example of asset design or implementation that is wholly in the public domain, however the level of risk represented by open source is tempered by the level of vulnerability it exhibits. There is some evidence that open source software is open to greater scrutiny to resolve errors but it is stressed that the weighting here is only intended to be on the asset itself.

Care should be taken here to ensure the highest level of knowledge of the asset required during identification, development and running of the potential vulnerability is identified.

6.6.3.1.2 Time factor

The role of time in evaluating the likelihood of an attack requires evaluation of the total amount of time taken by an attacker to identify that a particular, potential, weakness may exist, then to develop an attack method (threat agent) and to sustain effort required to mount the attack. When considering this factor, the worst case scenario should be used to estimate the amount of time required.

EXAMPLE: The time taken to identify a potential vulnerability can be the time taken to locate the potential vulnerability from information that is publicly available or can be the time required to analyse the design information to identify a potential vulnerability.

In addition to this time taken for identification, consideration of the time required to develop an attack method (which may also be publicly available) and to successfully mount the attack on the asset to exploit the vulnerability shall be included in this factor.

The following definitions apply (values escalate):

- within minutes:
  - an attack can be identified or exploited in less than an hour;
- within hours:
  - an attack can succeed in less than a day;

- within days:
  - an attack can succeed in less than a week;
- within weeks:
  - an attack can succeed in less than a month;
- within months:
  - a successful attack requires in excess of a month.

6.6.3.1.3 Expertise factor

Specialist expertise refers to the level of generic knowledge of the underlying principles, product type or attack methods (e.g. Internet protocols, Unix operating systems, buffer overflows). The levels of expertise to be applied within this factor are defined as below:

- **Laymen** are not knowledgeable compared to experts or proficient persons, with no particular expertise.
- **Proficient** persons are knowledgeable in that they are familiar with the security behaviour of the product or system type.
- **Experts** are familiar with the underlying algorithms, protocols, hardware, structures, security behaviour, principles and concepts of security employed, techniques and tools for the definition of new attacks, cryptography, classical attacks for the product type, attack methods, etc. implemented in the product or system type.

When describing the expertise required, the total number of experts required shall be included; the number of people for each type of expertise required and access to the expertise (dissemination) shall be considered when describing the expertise required. Therefore, if expertise in both techniques for types of attack applicable to the asset and underlying algorithms and protocols is required, then the highest level of Multiple Specialist Expertise characterization should be assumed.

6.6.3.1.4 Opportunity factor

Opportunity is also an important consideration, and has a relationship to the Elapsed Time factor. Identification or exploitation of a vulnerability may require considerable amounts of access to an asset that may increase the likelihood of detection. Some attack methods may require considerable effort off-line, and only brief access to the asset to exploit. Access may also need to be continuous, or over a number of sessions.

For some assets the window of opportunity may equate to the number of samples of the asset that the attacker can obtain. This is particularly relevant where attempts to penetrate the system (asset) and undermine the TSP may result in the destruction of the asset preventing use of that asset sample for further testing, e.g. hardware devices. Often in these cases distribution of the asset is controlled and so the attacker will apply effort to obtain further samples of the asset.

For the purposes of this clause unnecessary/unlimited access means that the attack does not need any kind of opportunity to be realized; easy means that access is required for less than a day or that the number of asset samples required to perform the attack is less than ten; moderate means that access is required for less than a month or that the number of asset samples required to perform the attack is less than fifty; difficult means that access is required for at least a month or that the number of asset samples required to perform the attack is less than one hundred; none means that the opportunity window is not sufficient to perform the attack (the length for which the asset to be exploited is available or is sensitive is less than the opportunity length needed to perform the attack -for example, if the asset key is changed each week and the attack needs two weeks).

The actual number of samples of an asset should not be considered fixed but rather should be considered against what would be a normal supply amount.

EXAMPLE: If a normal residential consumer attempts to hold more than a reasonable number of samples for residential use it may be characterized as the precursor to an attack.

Consideration of this factor may result in a determining that it is not possible to complete the exploit, due to requirements for time availability that are greater than the opportunity time.

6.6.3.1.5 Equipment factor

The equipment factor addresses the IT hardware/software or other equipment required to identify or exploit a vulnerability:

- **Standard** equipment is readily available to the attacker, either for the identification of a vulnerability or for an attack. This equipment may be a part of the asset itself (e.g. a debugger in an operating system), or can be readily obtained (e.g. Internet downloads, protocol analyser or simple attack scripts).
- **Specialized** equipment is not readily available to the attacker, but could be acquired without undue effort. This could include purchase of moderate amounts of equipment (e.g. power analysis tools, use of hundreds of PCs linked across the Internet would fall into this category), or development of more extensive attack scripts or programs.
- **Bespoke** equipment is not readily available to the public as it may need to be specially produced (e.g. very sophisticated software), or because the equipment is so specialized that its distribution is controlled, possibly even restricted. Alternatively, the equipment may be very expensive in relation to standard and specialized classifications.
- **Multiple bespoke** equipment extends the definition of bespoke equipment to address where multiple instances of equipment are used by the attacker, e.g. addressing the recruitment of multiple devices in establishing a botnet.

Specialist expertise and knowledge of the asset are concerned with the information required for persons to be able to attack an asset. There is an implicit relationship between an attacker's expertise (where the attacker may be one or more persons with complementary areas of knowledge) and the ability to effectively make use of equipment in an attack. The weaker the attacker's expertise, the lower the potential to use equipment (IT hardware/software or other equipment). Likewise, the greater the expertise, the greater the potential for equipment to be used in the attack. Although implicit, this relationship between expertise and the use of equipment does not always apply, for instance, when environmental measures prevent an expert attacker's use of equipment, or when, through the efforts of others, attack tools requiring little expertise to be effectively used are created and freely distributed (e.g. via the Internet).

6.6.3.1.6 Intensity factor

The intensity of an attack may be a factor in determining risk to the system or asset under attack. Table 3 identifies three possible levels of attack intensity and assigns values to each for use in the subsequent threat analysis.

Table 3: Attack intensity levels

Attack intensity	Value
Single instance of attack	0
Moderate level of multiple instances	1
Heavy level of multiple instances	2

The intensity of an attack may be modified by use of:

- distributed threat agents (many sources of attack);
- reducing the time interval between attacks; or
- by combining these two.

In the simplest case a threat agent is assumed to operate at one place for one instance of an attack in any one time period (where even if the attack is repeated the interval between attacks is greater than the asset recovery time such that the attacks can be considered as discrete). For many attacks where manual processes need to be executed at a particular location (such as intercepting a physical line) this is an adequate point of view. In many practical implementations or deployments, including those considered in standards development, consideration only of the discrete attack may be insufficient for risk analysis. Assets are often automated and accessible via networks, and as threat agents are also assets, then so may the attacks be automated and network accessible.

6.6.4 Identification of threat agents

A *threat agent* is an entity that can adversely act on assets. There exist different types of threat agents. The objective and the extent to which a threat agent is motivated and capable to successfully mount an attack on an asset differs per threat agent.

NOTE: Capability and motivation are treated separately in the application of the method but are then combined to determine the risk of a threat being enacted.

An evaluator shall identify threat agents that potentially want to launch an attack, and determine the threat level represented by each of these threat agents. The threat level is a value attributed to the combination of the capability and motivation of a threat agent to attack an asset. Capability is a characteristic of a threat agent that defines the level of technical sophistication of the threat. Motivation is a measure of how much a threat agent desires to attack and compromise an asset or group of assets. See annex B for more information.

It may be beneficial for the analysis to distinguish between the threat source and the threat actor. A *threat source* is a person or organization that desires to breach security and ultimately will benefit from a compromise in some way (e.g. nation state, criminal organization, activist) [i.10]. A *Threat Actor* is a person, or group of persons, who actually performs the attack (e.g. hackers, script kiddy, insider (e.g. employee), physical intruders) [i.10]. A threat source can recruit, influence or coerce a threat actor to mount an attack on their behalf. In the simplest case the *threat source* and the *threat agent* are the same entity and are treated as synonyms in the remainder of the present document.

In considering the role of motivation as it influences threat level, table 4 categorizes motivation levels. Table 5 presents a measure of the capability of the attacker. The motivation level and capability level are mapped to identify the threat level (see table 6).

Table 4: Motivation levels

Motivation levels	Description
Very low (indifferent)	The system is considered to have limited to no value to the threat agent, thus the threat agent is very unlikely to attempt any attack on the system.
Low (curious)	The system is considered to have minimal value to the threat agent. Threat agents may attempt to attack the system out of curiosity or opportunistic motivation. Non system deterrents may be sufficient to deter the threat agent from initiating the attack (e.g. due to potential ramifications if the agent can be linked to the attack).
Medium (interested)	The system is considered to have moderate value to the threat agent. The threat agent will attempt to attack the system on a frequent basis. It is also considered unlikely that the threat agent can be deterred from initiating the attack by the existence of non-system deterrents.
High (committed)	The system is considered to have significant value to the threat agent. The threat agent will attempt to attack the system on a persistent and frequent basis. It is considered highly unlikely that the threat agent can be deterred from initiating the attack by the existence of non-system deterrents.
Very high (focused)	Threat agent has a primary aim to attack the system.
NOTE: A non-system deterrent may include the criminalisation under law of the attack and a sufficient judiciary penalty (e.g. interment, financial penalty), with adequate law enforcement resources to capture and prosecute the threat agent.	

The determination of motivation, as discussed in annex B, is not generally considered as deterministic. However where sufficient resources can be applied to determine the level of motivation tables 5 and 6 consider the combination of threat agent capability and threat agent motivation to map a value for threat level.

Table 5: Capability levels

Capability levels	Description
Very little	Threat agent has almost no capabilities or resources. Matches an attack potential of Basic.
Little	Threat agent has very modest capabilities and resources. Matches an attack potential of Enhanced-Basic.
Limited	Threat agent has modest capabilities and resources. Matches an attack potential of Moderate.
Significant	Threat agent is capable and has significant resources. Matches an attack potential of High.
Formidable	Threat agent is extremely capable and well-resourced. Matches an attack potential of Beyond High.

Table 6: Mapping of motivation with capability to identify threat level [i.10]

Motivation	Capability				
	Very little	**Little**	**Limited**	**Significant**	**Formidable**
Very low (indifferent)	Negligible	Negligible	Low	Low	Low
Low (curious)	Negligible	Negligible	Low	Low	Moderate
Medium (interested)	Negligible	Low	Moderate	Severe	Severe
High (committed)	Low	Low	Moderate	Severe	Critical
Very high (focused)	Low	Moderate	Severe	Critical	Critical

6.7 Step 6: Calculation of the likelihood of the attack and its impact

Each of the attack factors shall be summed (i.e. Time + Expertise + Knowledge + Opportunity + Equipment) to give an overall attack potential rating as shown in table 7. The attack potential value shall then be mapped to a vulnerability rating (table 8). The vulnerability rating is then combined with the threat level using table 9 to obtain the Occurrence likelihood. The computation template to support step 6 is given in annex G.

Table 7: Attack potential

Factor	Range	Value
Time (elapsed time)	≤ 1 day	0
	≤ 1 week	1
	≤ 2 weeks	2
	≤ 1 month	4
	≤ 2 months	7
	≤ 3 months	10
	≤ 4 months	13
	≤ 5 months	15
	≤ 6 months	17
	> 6 months (see note 1)	19
Expertise	Layman	0
	Proficient	3
	Expert	6
	Multiple experts	8
Knowledge	Public	0
	Restricted	3
	Sensitive	7
	Critical	11
Opportunity	Unnecessary/ unlimited access	0
	Easy	1
	Moderate	4
	Difficult	10
	None (see note 2)	999
Equipment	Standard	0
	Specialized (see note 3)	4
	Bespoke	7
	Multiple bespoke	9
NOTE 1: A successful attack requires in excess of 6 months. NOTE 2: None means that the window of opportunity is not sufficient to perform the attack. NOTE 3: If clearly different groups of specialized equipment are required for distinct steps of an attack, this should be rated as bespoke.		

Table 8: Vulnerability rating

Attack potential values	Attack potential required to exploit attack	Resistant to attacker with attack potential of
0 to 9	Basic	No rating
10 to 13	Enhanced-basic	Basic
14 to 19	Moderate	Enhanced basic
20 to 24	High	Moderate
> 24	Beyond High	High

The method for threat analysis defined in ETSI ETR 332 [i.9] combines the likelihood with the impact of the attack in determining if a countermeasure should be applied. The form of countermeasures can include redesign of the element at risk in the system to remove the vulnerability that is to be attacked, and application of a defensive system component that masks the vulnerability. The vulnerability rating and threat level can be mapped to the likelihood of attack as shown in table 9.

Table 9: Mapping of vulnerability rating with Threat level to identify likelihood of attack

Vulnerability rating	Threat level				
	Negligible	Low	Moderate	Severe	Critical
Basic	Possible	Likely	Very Likely	Very Likely	Very Likely
Enhanced Basic	Unlikely	Possible	Likely	Very Likely	Very Likely
Moderate	Very Unlikely	Unlikely	Possible	Likely	Very Likely
High	Very Unlikely	Very Unlikely	Unlikely	Possible	Likely
Beyond High	Very Unlikely	Very Unlikely	Very Unlikely	Unlikely	Possible

6.8 Step 7: Establishment of the risks

6.8.0 Overview

For each of the assets in the system under study one can identify their vulnerabilities and corresponding threats and weaknesses. For each vulnerability the likelihood should be computed as described in the clause above. For each asset the risk associated with each vulnerability should be computed. The computation template to support step 7 is given in annex H.

6.8.1 Impact of intensity

The overall impact on a system of a particular threat can vary with the intensity with which the attack is mounted. The resulting impact, shown in table 10, is determined by summing the asset impact value (from table 2) and the attack intensity value (from table 3).

Table 10: Result on overall Impact of varying attack intensity

Asset Impact	Attack Intensity	Resulting Impact
1	0	1
1	1	2
1	2	3
2	0	2
2	1	3
2	2	3 (see note)
3	0	3
3	1	3 (see note)
3	2	3 (see note)

NOTE: The Asset Impact is assigned a value in the range of 1 to 3. Consequently, any Resulting Impact value calculated to be greater than 3 is given the value of 3.

6.8.2 Classification of risk

6.8.2.1 Overview

Risk is defined in ETSI standards as the product of the likelihood of an attack (occurrence likelihood) and the impact of the attack on the system.

The likelihood of a threat occurring (occurrence likelihood) may be estimated with values from 1 to 3 as explained in table 11 (Occurrence likelihood). Capability and motivation are each taken into account in the calculation of likelihood. A highly motivated and capable threat agent (e.g. a nation state with a cyber division) will be able to attack successfully even if the vulnerability rating is "beyond high" which results in a likelihood evaluation of possible.

Table 11: Occurrence likelihood

Value	Likelihood of occurrence	Explanation
1 (note)	Very unlikely	According to up-to-date knowledge, there are no means of solving the technical difficulties to state the threat irrespective of the motivation or resources available to the attacker.
1	Unlikely	According to up-to-date knowledge, a possible attacker needs to solve strong technical difficulties to state the threat or the motivation for an attacker is very low.
2	Possible	The technical requirements necessary to state this threat are not high and could be solved without significant effort; furthermore, there is a reasonable motivation for an attacker to perform the threat.
3	Likely	There are no sufficient mechanisms installed to counteract this threat and the motivation for an attacker is quite high.
3 (note)	Very likely	As for very likely but the threat is considered more imminent.
NOTE: The values assigned to "Very unlikely" and "Unlikely" are identical, similarly the values assigned to "Likely" and "Very likely" are identical. The rationale is that they represent extreme poles but in each case do not equate to risk escalation.		

The impact of a threat is also estimated with values from 1 to 3 as explained in table 2 in clause 6.2 and extended in table 10 when attack intensity is considered.

The product of occurrence likelihood (from table 11) and impact value (from table 10) as defined in clause 6.6 gives the risk which serves as a measurement for the risk that the concerned asset is compromised. The result is classified into three categories of risk as shown in table 12.

Table 12: Risk

Value	Risk	Explanation
1, 2	Minor	No essential assets are concerned, or the attack is unlikely. Threats causing minor risks have no primary need for counter measures.
3, 4	Major	Threats on relevant assets are likely to occur although their impact is unlikely to be fatal. Major risks should be handled seriously and should be minimized by the appropriate use of countermeasures.
6, 9	Critical	The primary interests of the providers and/or subscribers are threatened and the effort required from a potential attacker's to implement the threat(s) is not high. Critical risks should be minimized with highest priority.
NOTE: Because risk is calculated as the product of likelihood and impact the values 5, 7 and 8 cannot occur.		

6.9 Step 8: Security countermeasure identification

6.9.0 Introduction

Security Countermeasures are assets that are added to the system to reduce the weighted risk to the system. The purpose of countermeasures is to reduce either the likelihood of an attack or to the attack impact. Security countermeasures are modelled in the TVRA as instances of assets and whilst primarily logical may also be human or physical.

There might be several alternative countermeasures and these should first be identified, then evaluated and compared to identify the costs and benefits of each so that an informed decision can be made of which countermeasures to select.

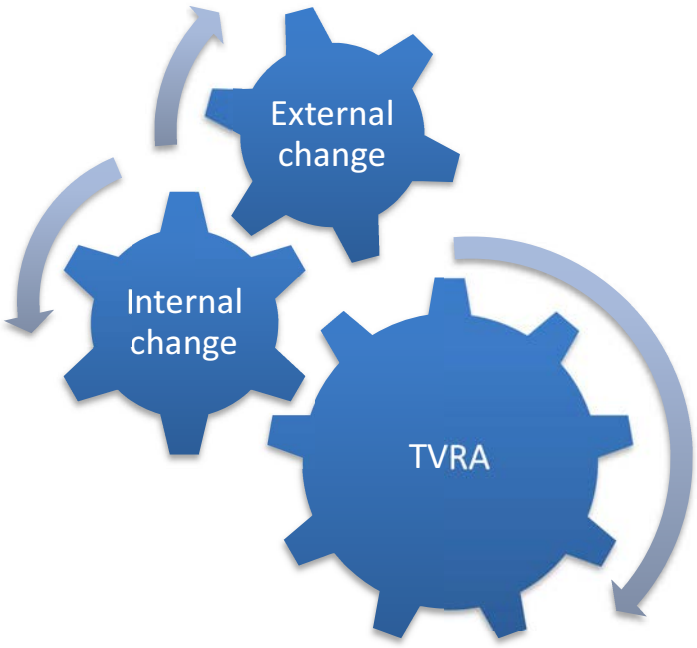


Figure 9: Cyclical nature of TVRA

Figure 9 shows that countermeasures are added as internal changes to the system and thus for change to the system the TVRA process shall be repeated. This should continue either until no further countermeasures are able to be applied (indicating stability in the system) or until the level of risk identified is considered as acceptable (residual risk).

NOTE: Some countermeasures may be inferred by inspection of the security requirements.

6.9.1 Countermeasures in the system

Where a countermeasure has been defined, or is implemented, as a logical asset it will require to be deployed in a corresponding physical assets (e.g. a firewall rule requires a firewall). The countermeasures and their supporting physical assets bring their own vulnerabilities and as noted above the TVRA shall be re-applied with the countermeasures included in the scope of the TOE.

6.9.2 Composite countermeasures applied to the system

More than one countermeasures may be applied against a single threat agent, or to protect a single asset. In such case the residual risk is only identified by re-performing the TVRA.

6.9.3 Impact of composite countermeasures applied to the system

The impact of countermeasures on the overall risks analysis takes a similar approach as the automated threat agents. In this case the least likely of the two values is taken for each of the likelihood parameters. The impact of the countermeasures on the impact is similarly calculated by taking the least impact. This calculation shall be applied after assessing the impact of automated threat agents.

6.10 Step 9: Countermeasure Cost-benefit analysis

6.10.0 Introduction

More than one countermeasure may be effective in reducing particular risks or the overall set of risks. The TVRA method specifies a countermeasure cost-benefit analysis for this purpose. The goal of the analysis is to identify the most cost-effective countermeasure of the alternatives. The main benefit of any countermeasure is the mitigation of attack measures that results in both added security and in the introduction of explicit attack protection. Other benefits may be increased market acceptance and improved regulatory compliance. Costs are not merely economical aspects, but affect standardization, implementation and operation. The countermeasure cost-benefit template and tool is given in annex H.

6.10.1 Standards design

Introducing countermeasures to a standard under development or an existing standard (published) may impose changes affecting the time schedule and resulting in additional effort and cost. The level to which a countermeasure affects the standard design is measured according to the scale in table 13.

Table 13: Standards design evaluation

Scale	Description	Assigned value
No Impact	No effect on the time schedule and resources needed of standards under development or no changes needed on existing and published standards.	0
Low Impact	No significant time delay or additional resource demand for standards under development or changes needed on existing and published standards.	1
Medium Impact	Significant time delay and additional resource demand for standards under development and significant changes needed on existing and published standards.	4
Major Impact	Unacceptable time delay and additional resource demand for standards under development and unacceptable changes needed on existing and published standards.	9

6.10.2 Implementation

Adding countermeasures to standards may affect its adoption and implementation in the targeted user community. This is an important aspect of standards adoption and crucial for countermeasure cost-benefit analysis. The level to which a countermeasure affects implementation of the standard is measured according to the scale in table 14.

Table 14: Implementation evaluation

Scale	Description	Assigned value
No Impact	No effect on standards adoption in the targeted user community.	0
Low Impact	No significant effect on standards adoption in the targeted user community.	1
Medium Impact	Significant effect on standards adoption in the targeted user community.	4
Major Impact	Unacceptable effect on standards adoption in the targeted user community.	9

6.10.3 Operation

Countermeasures may impact the ongoing operation of standardized products or systems once they have been deployed into an operational environment. The level to which a countermeasure affects the operation of standardized products is measured according to the scale in table 15.

Table 15: Operation evaluation

Scale	Description	Assigned value
No Impact	No effect on operation of realized standards design and targeted operational environment.	0
Low Impact	No significant effect on operation of realized standards design or targeted operational environment.	1
Medium Impact	Significant effect on operation of realized standards design and targeted operational environment.	4
Major Impact	Unacceptable effect on operation of realized standards design and targeted operational environment.	9

6.10.4 Regulatory impact

Regulatory impacts concern the influence that the countermeasure may have on ensuring regulatory compliance. Regulatory impact is evaluated according to the scale in table 16.

Table 16: Regulatory impact evaluation

Scale	Description	Assigned value
Severe Negative Impact	Unacceptable effect on regulatory compliance requirements.	-9
Negative Impact	Significant negative effect on regulatory compliance requirements.	-4
No Impact	No effect on regulatory compliance requirements.	0
Positive Impact	Significant positive effect on regulatory compliance requirements.	4
Severe Positive Impact	Very favourable effect on regulatory compliance requirements.	9

6.10.5 Market acceptance

Adoption of a standard into industrial products and its acceptance by the targeted user community determine the success of a standard. Therefore, countermeasures with negative predicted effect on market acceptance should be carefully analysed. The level to which a countermeasure affects market acceptance of the standard is measured according to the scale in table 17.

Table 17: Market acceptance evaluation

Scale	Description	Assigned value
Severe Negative Impact	Unacceptable effect on market acceptance.	-9
Negative Impact	Significant negative effect on market acceptance.	-4
No Impact	No effect on market acceptance.	0
Positive Impact	Significant positive effect on market acceptance.	4
Severe Positive Impact	Very favourable effect on market acceptance.	9

6.11 Step 10: Specification of detailed requirements

Security requirements should be identified for both the asset and, where applicable, its environment. Detailed requirements are refined from the functional security requirements from step 3 and the security services and capabilities of the countermeasures and security requirements identified in step 8 and analysed in step 9. Guidelines for the specification of detailed requirements are given in ETSI TR 187 011 [i.2].

Annex A (normative): TVRA pro forma

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the TVRA definition pro forma in this annex so that it can be used for its intended purposes and may further publish the completed TVRA definition.

A Security Environment			
a.1 Assumptions			
a.1.1	*Text of assumption*		*Citation for full text*
a.1.2			
a.2 Assets			
a.2.1	*Short text describing asset*		*Citation for full text*
a.2.2			
a.3 Threat agents			
a.3.1	*Short text describing threat agent*		*Citation for full text*
a.3.2			
a.4 Threats			
a.4.1	*Short text describing threat*		*Citation for full text*
a.4.2			
a.5 Security policies (OPTIONAL)			
a.5.1	*Short text describing security policy*		*Citation for full text*
a.5.2			
B Security Objectives			
b.1 Security objectives for the asset			
b.1.1	*Short text describing objective for the asset*		*Citation for full text*
b.1.2			
b.2 Security objectives for the environment			
b.2.1	*Short text describing objective for the requirement*		*Citation for full text*
b.2.2			
C IT Security Requirements			
c.1 Asset security requirements			
c.1.1 Asset security functional requirements			
c.1.1.1	*Short text describing security functional requirement*	*ISO15408] class*	*Citation for full text*
c.1.1.2			
c.1.2 Asset security assurance requirements			
c.1.2.1	*Short text describing security assurance requirement*	*ISO15408] class*	*Citation for full text*
c.1.2.2			
c.2 Environment security requirements (OPTIONAL)			
c.2.1	*Short text describing security environment requirement*	*ISO15408] class*	*Citation for full text*
c.2.2			
D Application notes (OPTIONAL)			
E Rationale			
The eTVRA should define the full rational, if this is true only a citation (reference) to the full text is required			

Annex B (informative): The role of motivation

A full critique of the role of motivation in attacking a system when viewed in the context of Common Criteria evaluation can be found in clause B.4.1.1 of the Common Criteria Evaluation methodology [i.32]. In the present document motivation is addressed in broadly similar terms as a factor in determining attack potential.

Motivation can be used to describe aspects both of the attacker, and of the system (assets) he is attacking. The following key criteria may be considered when evaluating motivation:

- The likelihood of an attack:
  - If a threat is highly motivated an attack can be considered imminent, with a corollary of.
  - If a threat is unmotivated no attack can be anticipated.
- The value of the asset, monetarily or otherwise, to either the attacker or the asset holder:
  - An asset of very high value is likely to motivate an attack, with a corollary of.
  - An asset of little value is unlikely to motivate an attack.
- The expertise and resources with which an attacker is willing to effect an attack:
  - A highly motivated attacker is likely to acquire sufficient expertise and resources to defeat the measures protecting an asset, with a corollary of.
  - An attacker with significant expertise and resources is not willing to effect an attack using them if the attacker's motivation is low.

In each case there is no probabilistic means of determining the role of motivation in mounting an attack. However in assessing threat potential it is essential to consider motivation in order to minimize the effect of motivation on the attacker.

Whilst it may be attested that mitigation of common attacks against known vulnerabilities may be reduced by the development of a degree of cyber-herd immunity by the encouragement of a significant proportion of the community to implement a proven countermeasure there is a corollary that attackers may be motivated by similar herd behaviour. Thus it may be that attack and countermeasures move in and out of fashion and a visibly successful attack may motivate similar, copycat attacks. The role of cyber-herd immunity in such cases requires that a countermeasure is spread across all potentially vulnerable systems with an associated impact of reducing the likelihood of an exploit finding an attack surface. This herd immunity is particularly effective in demotivating those seeking to use simple attack vectors across multiple targets.

NOTE: For common platforms the attack surface may be, for example, an operating system vulnerability but if there are millions or 10 s or 100 s of millions of instances of the vulnerable code then only herd immunity will work to demotivate an attacker.

Annex C:
Void

Annex D (informative): Denial of service attacks

D.0 Introduction

A "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include:

- attempts to "flood" a network, thereby preventing legitimate network traffic;
- attempts to disrupt connections between two machines, thereby preventing access to a service;
- attempts to prevent a particular individual from accessing a service;
- attempts to disrupt service to a specific system or person.

Not all service outages, even those that result from malicious activity, are necessarily denial-of-service attacks. Other types of attack may include a denial of service as a component, but the denial of service may be part of a larger attack.

Illegitimate use of resources may also result in denial of service.

Denial-of-service attacks come in a variety of forms and aim at a variety of services. There are three basic aims of the attacker:

- To cause consumption of scarce, limited, or non-renewable resources.
- To lead to destruction or alteration of configuration information.
- To cause physical destruction or alteration of network components.

D.1 Void

D.2 DDoS characteristics

D.2.1 Introduction

Distributed Denial of Service (DDoS) attacks extend conventional Denial of Service (DoS) attacks by the additional characteristic of being distributed attacks (i.e. the attack is from many points at once). For a DDoS attack the multiplicity of the attack relationship in figure D.1 is 1 to many (1 victim, many attackers), whereas in most conventional attacks the multiplicity is 1 to 1.

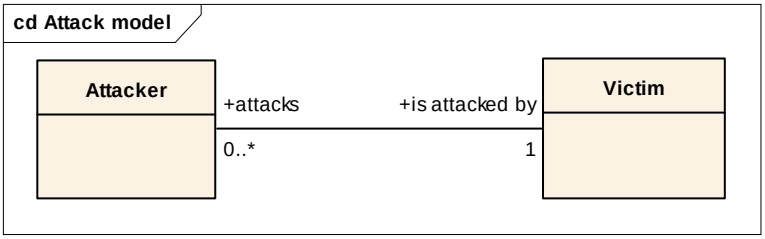


Figure D.1: Attack model (static state)

There are two primary assets of a system that are victimised in DDoS attacks:

- Bandwidth.
- Processing resources (CPU cycles, memory, process tables).

Bandwidth is consumed by flooding the network with useless packets. Attacks against processing resource may be achieved by generating several thousands of useless processes on the victim's system.

Each Distributed DOS attack enters several network ISO OSI layers and can use its different functions to achieve result. The method of operation if based on specific purposes of each level, i.e. broadcasting on L2, overflowing connects on L4 or abusing L7 service. Some layers or generic protocols have vulnerabilities which help DDoS. As result this leads to strong layer-based classification of such attacks.

D.2.2 L2 DDoS attacks

L2 attacks are common in LAN and can lead to network equipment outage. One of the methods could be ARP floods or DDoS, based on configuration or discovery protocols.

D.2.3 L3 DDoS attacks

L3 attacks use general Internet protocols such as IP, ICMP and other. This layer serves packet delivery and can be exploited many ways. "Ping of Death" and "Teardrop" attacks use illegal packet size vulnerability of weak equipment. "Smurf Attack" and similar uses ICMP service to multiply packet count and realize channel consumption or resource exhaustion. Many Internet Service Providers allow their users to manipulate source IP addresses which leads to spoofing possibility and complicate DDoS blocking. Moreover it is possible to redirect attack traffic by setting the victim's IP address as source and sending packet to an open service.

EXAMPLE 1: Ping of Death attacks wherein the attacker creates a packet that contains more than 65 536 bytes, which is the limit that the IP protocol defines. This packet can cause different kinds of damage to the machine that receives it, such as crashing and rebooting.

EXAMPLE 2: Teardrop attack wherein the attacker takes advantage of packet fragmentation policies whereby in normal operation whilst a packet is travelling from the source machine to the destination machine, it may be broken up into smaller fragments, through the process of fragmentation. A Teardrop attack creates a stream of IP fragments with their offset field overloaded. The destination host that tries to reassemble these malformed fragments eventually crashes or reboots.

EXAMPLE 3: Smurf attack wherein the victim is flooded with *Internet Control Message Protocol* (ICMP) "echo-reply" packets. The attacker sends numerous ICMP "echo-request" packets to the broadcast address of many subnets. These packets contain the victim's address as the source IP address. Every machine that belongs to any of these subnets responds by sending ICMP "echo-reply" packets to the victim. Smurf attacks are very dangerous, because they are strongly distributed attacks.

D.2.4 L4 DDoS attacks

TCP and UDP introduce port for service and give new abilities of DDoS. More complicated attacks realize connect flood which requires full SYN, SYN-ACK, ACK sequence. UDP is much more vulnerable protocol because it does not provide peer checking. This allows dangerous attacks from unlimited spoofed sources which are very difficult to mitigate.

EXAMPLE 1: SYN flood attacks occur during the three-way handshake that marks the onset of a TCP connection. In the three-way handshake, a client requests a new connection by sending a TCP SYN packet to a server. After that, the server sends a SYN/ACK packet back to the client and places the connection request in a queue. Finally, the client acknowledges the SYN/ACK packet. If an attack occurs, however, the attacker sends an abundance of TCP SYN packets to the victim, obliging it both to open a lot of TCP connections and to respond to them. Then the attacker does not execute the third step of the three-way handshake that follows, rendering the victim unable to accept any new incoming connections, because its queue is full of half-open TCP connections.

EXAMPLE 2: In Land attacks, the attacker sends the victim a TCP SYN packet that contains the same IP address as the source and destination addresses. Such a packet completely locks the victim's system.

EXAMPLE 3: TCP Reset attacks are enabled by monitoring the network "tcpconnection" requests to the victim. As soon as such a request is found, the malevolent attacker sends a spoofed TCP RESET packet to the victim and obliges it to terminate the TCP connection.

EXAMPLE 4: An attacker exploits a User Datagram Protocol (UDP) connection to pair a character generation ("chargen") service to generate a series of characters each time it receives a UDP packet, whilst the paired echo service echoes any character it receives. Exploiting these two services, the attacker sends a packet with the source spoofed to be that of the victim to another machine. Then, the echo service of the former machine echoes the data of that packet back to the victim's machine and the victim's machine, in turn, responds in the same way. Hence, a constant stream of useless load is created that burdens the network, resulting in a UDP Storm attack.

D.2.5 L7 DDoS attacks

There are many kinds of L7 services and many of them are vulnerable. One way this services are used in DDoS is amplification. DNS, NTP, Chargen, SNMP and other UDP services are famous for amplifying small spoofed requests to big responses addressed to victim. This makes gigabits of traffic from megabits of requests and allows very cheap and dangerous attacks. Another way of modern DDoS is using masses of compromised equipment i.e. IoT devices to generate multiple plausible L7 sessions that put victim under huge load. In case of thousands of devices in such a botnet there is no need to provide large traffic from each device to force victim's outage.

EXAMPLE 1: A Process Table attack exploits the feature of some network services to generate a new process each time a new TCP/IP connection is set up. The attacker tries to make as many uncompleted connections to the victim as possible in order to force the victim's system to generate a very large number of processes, where at some point the number of processes that are running on the system renders the victim unable to serve any other request.

EXAMPLE 2: An SSH Process table attack makes hundreds of connections to the victim with the *Secure Shell* (SSH) Protocol without completing the login process. In this way, the daemon contacted by the SSH on the victim's system is obliged to start so many SSH processes that it is exhausted.

D.2a Difficulties of defence

Development of detection and defending tools is unlikely to prove 100 % effective and some of the more common problems include:

- DDoS attacks flood victims with packets. The rate of change of network activity that leads to an attack may be greater than the speed at which countermeasures can be brought into play.
- Any attempt of filtering the incoming flow may mean that legitimate traffic will be rejected.
- Filtering may rob processor time and more advanced filtering rules take more of the resource.
- Attack packets often have spoofed IP addresses so tracing the real attacker rather than a masqueraded victim may be impossible.
- Botnets of any significant size can provide many plausible L7 requests which will be difficult to distinguish from valid traffic.

D.3 Defence against DDoS

D.3.0 Overview

From the beginning, all legitimate users have tried to respond against these threats. University communities and software corporations have proposed several methods against the DDoS threat. Despite the efforts, the solution remains a dream. The attackers manage to discover other weaknesses of the protocols and, what is worse, they exploit the defence mechanisms in order to develop attacks. They discover methods to overcome these mechanisms or they exploit them to generate false alarms and to cause catastrophic consequences.

Many experts have tried to classify the DDoS defence mechanisms in order to clarify them. This classification gives users an overall view of the situation and helps defence-mechanism developers cooperate against the threat. The basic discrimination is between preventive and reactive defence mechanisms.

D.3.1 Preventive Mechanisms

D.3.1.0 Introduction

The preventive mechanisms try to eliminate the possibility of DDoS attacks altogether or to enable potential victims to endure the attack without denying services to legitimate clients. With regard to attack prevention, countermeasures can be taken on either victims or on zombies. In both cases the system configuration is modified to eliminate the possibility of accepting a DDoS attack or participating in a DDoS attack.

Filtering of input and output traffic may be possible and may offer simple rules, for example, the source IP address of output traffic should belong to the sub-network, whereas the source IP address of input traffic should not.

D.3.1.1 Firewalling

Simple attack types can be mitigated by enabling a firewall and firewall specific rules. The simplest option is limiting TCP/UDP ports, IP masks, etc. Other options include limiting maximum connection time, connection speed and/or request size.

NOTE: A generic role of a firewall can be seen in the definition of gateway cyber defence.

D.3.1.2 TCP anti-spoofing

SYN-cookie mechanisms allow for the automatic mitigation of TCP spoofing. The attacked service resources are not allocated for TCP connection until the full and valid TCP handshake has occurred. Hidden SYN-cookie based peer checking can be provided by special equipment.

D.3.1.3 Traffic shaping

By using this mechanism packets, connect requests and messages per second rates can be controlled for each client IP address. Known peers can get prioritization.

D.3.1.4 Border Session Manager

Special equipment, for example a Session Border Controller, can be used for high level protocol validation for services including SIP, HTTP and DNS. Such equipment can provide application security policies for all ingoing sessions and help to prevent attacks.

D.3.1.5 GeoIP blocking

An amount of geographical IP rules can be applied once the system is subject to an attack to reconstruct the geographical sources of traffic. Any attack detected from a specific region may lead to full region access prohibition. However the technique may be seen to be effective when other methods do not help.

D.3.2 Reactive Mechanisms

D.3.2.0 Introduction

Reactive mechanisms try to detect the attack and respond to it immediately and by doing so restrict the impact of the attack on the victim.

RISK: Characterizing a legitimate connection as an attack.

D.3.2.1 Signature detection mechanisms

Signature-based methods search for patterns (signatures) in observed network traffic that match known attack signatures from a database. The advantage of these methods is that they can easily and reliably detect known attacks, but they cannot recognize new attacks. Moreover, the signature database is always kept up-to-date in order to retain the reliability of the system.

D.3.2.2 Anomaly detection mechanisms

Anomaly-based methods compare the parameters of the observed network traffic with normal traffic. Hence it is possible for new attacks to be detected. However, in order to prevent a false alarm, the model of "normal traffic" is always kept updated and the threshold of categorizing an anomaly is properly adjusted.

D.3.3 Void

D.3.4 Information sharing schemes for prevention and reaction

Any attack that may be used against more than one victim may be mitigated in part by sharing knowledge of the attack. The overall impact is to bring a greater community of interested defenders (potential victims of the attack) to a state of awareness of the attack and may allow for more assets (time and expertise) to be applied to mitigate any future instantiation of the attack.

Annex E (informative): TVRA database structure

E.1 Database structure

The database Entity Relationship Diagram (ERD) shown in figure E.1 has been extracted from the database used in development. For readability the lookup tables have been omitted.

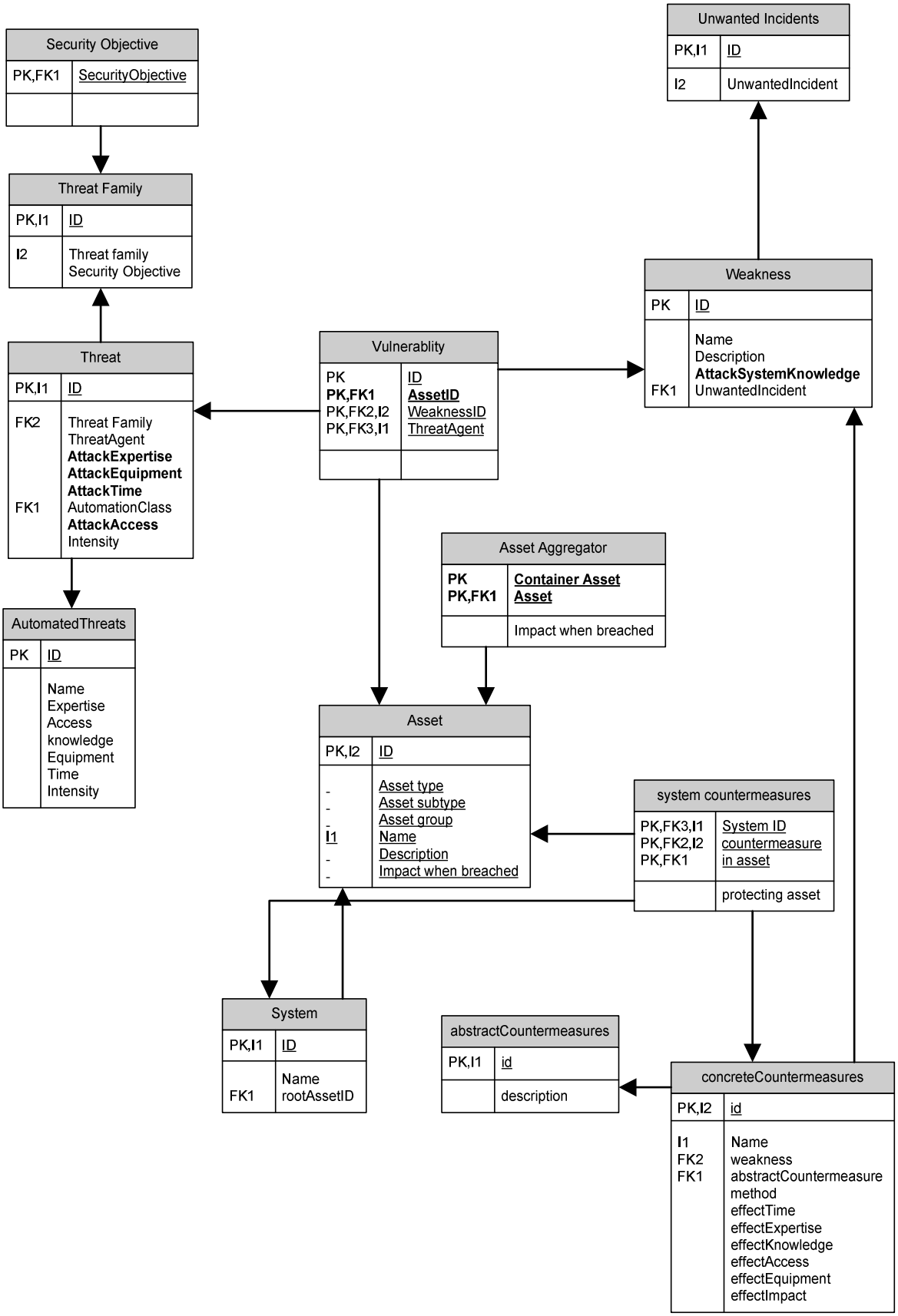


Figure E.1: Database structure extracted from MS-Access™ TVRA test database

E.2 SQL code for TVRA database

E.2.0 Introduction

The following SQL code is offered without claims for completeness but to allow readers of the present document to incorporate them into an existing database environment. The code follows the ANSI-SQL language syntax wherever possible and has been tested using the open source mySQL database without optimization.

NOTE: For use in mySQL databases the database engine has to be set to InnoDB in order to allow foreign key relationships to work.

E.2.1 Lookup tables

Lookup tables are used throughout the database to store data that is either immutable, or which may be referenced in more than one of the core tables. This covers the criteria for weighting a risk as defined in clauses 5 and 6 of the present document, the use of Common Criteria Functional and Assurance classes as defined in ISO/IEC 15408 [i.30] and referred to in clause 5 of the present document, and citations used to record the source material used in analysis.

NOTE: Lookup tables are used to resolve many-to-one relationships identified in the UML models in the core of the present document.

```
CREATE TABLE Citation_LU (
  CitationId INT NOT NULL AUTO_INCREMENT,
  PRIMARY KEY (CitationId),
  Publisher Text(50) NOT NULL,
  DocumentName Text(255),
  Notes Text(255)
) ENGINE = InnoDB
;
```

```
CREATE TABLE RequirementType_LU (
  RequirementTypeId INT NOT NULL AUTO_INCREMENT,
  PRIMARY KEY (RequirementTypeId),
  RquirementType Text(25) NOT NULL,
  RequirementTypeDescription Text(127)
)
;
```

```
CREATE TABLE CC_Components_LU (
    ComponentId INT NOT NULL AUTO_INCREMENT,
    PRIMARY KEY (ComponentId),
    Citation INT,
    INDEX (Citation),
    FOREIGN KEY (Citation) REFERENCES Citation_LU (CitationId),
    CC_ComponentShortName Text(7) NOT NULL,
    CC_ComponentLevel INT NOT NULL,
    CC_ComponentLongName Text(80) NOT NULL
)
;
```

```
CREATE TABLE Likelihood_LU (
    LikelihoodId INT NOT NULL,
  PRIMARY KEY (LikelihoodId),
    Likelihood Text(50),
    Description Text(1024)
) ENGINE = InnoDB
;
```

```
CREATE TABLE AssetValue_LU (
    AssetImpact INT NOT NULL,
  PRIMARY KEY (AssetImpact),
    AssetImpactShortText Text(50) NOT NULL,
    AssetImpactLongDescription Text(1024)
) ENGINE = InnoDB
;
```

```
CREATE TABLE AttackEquipment_LU (
    AttackEquipment INT NOT NULL,
  PRIMARY KEY (AttackEquipment),
    Equipment Text(50) NOT NULL,
    AttackEquipmentLongDescription Text(1024)
) ENGINE = InnoDB
;
```

```
CREATE TABLE AttackExpertise_LU (
    AttackExpertise INT NOT NULL,
  PRIMARY KEY (AttackExpertise),
    Expertise Text(50) NOT NULL,
    AttackExpertiseLongDescription Text(1024)
) ENGINE = InnoDB
;
```

```
CREATE TABLE AttackKnowledge_LU (
    AttackKnowledge INT NOT NULL,
  PRIMARY KEY (AttackKnowledge),
    Knowledge Text(50) NOT NULL,
  AttackKnowledgeLongDescription Text(1024)
) ENGINE = InnoDB
;
```

```
CREATE TABLE AttackOpportunity_LU (
    AttackOpportunity INT NOT NULL,
  PRIMARY KEY (AttackOpportunity),
    OpportunityText Text(50) NOT NULL,
  OpportunityLongDescription Text(1024)
) ENGINE = InnoDB
;
```

```
CREATE TABLE Motivation_LU (
    Motivation INT NOT NULL,
  PRIMARY KEY (Motivation),
    MotivationText Text(50) NOT NULL,
  MotivationLongDescription Text(1024)
) ENGINE = InnoDB
;
```

```
CREATE TABLE Capability_LU (
    Capability INT NOT NULL,
  PRIMARY KEY (Cpability),
    CapabilityText Text(50) NOT NULL,
  CapabilityLongDescription Text(1024)
) ENGINE = InnoDB
;
```

E.2.1a Lookup table initialization

The initialization data for the lookup tables is derived from the text of clause 6 of the present document.

```
INSERT INTO AttackIntensity_LU VALUES
  (0, 'Single', 'The attack is considered to consist of discrete events where the impact is not
cumulative'),
  (1, 'Moderate', 'The attack is considered to appear to be continuous (i.e. discrete events cannot
be distinguished)'),
  (2, 'High', 'The attack is considered to be continuous with cumulative impact')
;
```

```
INSERT INTO AssetValue_LU VALUES
  (1, 'Low', 'The concerned party is not harmed very strongly; the possible damage is low'),
  (2, 'Medium', 'The threat addresses the interests of providers/subscribers and cannot be
neglected'),
  (3, 'High', 'A basis of business is threatened and severe damage might occur in this context')
;
```

```
INSERT INTO AttackEquipment_LU VALUES
  (0, 'Standard', 'Standard equipment is readily available to the attacker, either for the
identification of a vulnerability or for an attack. This equipment may be a part of the asset itself
(e.g. a debugger in an operating system), or can be readily obtained (e.g. Internet downloads,
protocol analyser or simple attack scripts)'),
  (3, 'Specialised', 'Specialised equipment is not readily available to the attacker, but could be
acquired without undue effort. This could include purchase of moderate amounts of equipment (e.g.
power analysis tools, use of hundreds of PCs linked across the Internet would fall into this
category), or development of more extensive attack scripts or programs'),
  (7, 'Bespoke', 'Bespoke equipment is not readily available to the public as it may need to be
specially produced (e.g. very sophisticated software), or because the equipment is so specialised
that its distribution is controlled, possibly even restricted. Alternatively, the equipment may be
very expensive'),
  (9,'Multiple bespoke', 'extends the definition of bespoke equipment to address where multiple
instances of equipment are used by the attacker, e.g. addressing the recruitment of multiple devices
in establishing a botnet.')
;
```

```
INSERT INTO AttackExpertise_LU VALUES
  (0, 'Layman', 'Laymen are unknowledgeable compared to experts or proficient persons, with no
particular expertise'),
  (3, 'Proficient', 'Proficient persons are knowledgeable in that they are familiar with the
security behaviour of the product or system type'),
  (6, 'Expert', 'Experts are familiar with the underlying algorithms, protocols, hardware,
structures, security behaviour, principles and concepts of security employed, techniques and tools
for the definition of new attacks, cryptography, classical attacks for the product type, attack
methods, etc. implemented in the product or system type'),
  (8, 'Multiple experts', 'As for expert but addressing the case where multiple experts are brought
together to work as a team')
;
```

```
INSERT INTO AttackKnowledge_LU VALUES
  (0, 'Public', 'Public information concerning the asset (e.g. as gained from the Internet)'),
  (3, 'Restricted', 'Restricted information concerning the asset (e.g. knowledge that is controlled
within the developer organisation and shared with other organisations under a non-disclosure
agreement)'),
  (7, 'Sensitive', 'Sensitive information about the asset (e.g. knowledge that is shared between
discreet teams within the developer organisation, access to which is constrained only to members of
the specified teams)'),
  (11, 'Critical', 'Critical information about the asset (e.g. knowledge that is known by only a few
individuals, access to which is very tightly controlled on a strict need to know basis and
individual undertaking)')
;
```

```
INSERT INTO AttackOpportunity_LU VALUES
  (0,'Unlimited','the attack does not need any kind of opportunity to be realised'),
  (1, 'Easy','access is required for less than a day or that the number of asset samples required to
perform the attack is less than ten'),
  (4, 'Moderate','access is required for less than a month or that the number of asset samples
required to perform the attack is less than fifty'),
  (10,'Difficult','access is required for at least a month or that the number of asset samples
required to perform the attack is less than one hundred'),
  (999,'None','the opportunity window is not sufficient to perform the attack (the length for which
the asset to be exploited is available or is sensitive is less than the opportunity length needed to
perform the attack -for example, if the asset key is changed each week and the attack needs two
weeks)')
;
```

```
INSERT INTO Likelihood_LU VALUES
  (1,'Unlikely','According to up-to-date knowledge, a possible attacker needs to solve strong
technical difficulties to state the threat or the motivation for an attacker is very low.'),
  (2,'Possible','The technical requirements necessary to state this threat are not high and could be
solved without significant effort; furthermore, there is a reasonable motivation for an attacker to
perform the threat'),
  (3,'Likely','There are no sufficient mechanisms installed to counteract this threat and the
motivation for an attacker is quite high')
;
```

```
INSERT INTO Motivation_LU VALUES
  (1,'Very low (indifferent)', 'The system is considered to have limited to no value to the threat
agent, thus the threat agent is very unlikely to attempt any attack on the system'),
  (2, 'Low (curious)', 'The system is considered to have minimal value to the threat agent. Threat
agents may attempt to attack the system out of curiosity or opportunistic motivation. Non system
deterrents may be sufficient to deter the threat agent from initiating the attack (e.g. due to
potential ramifications if the agent can be linked to the attack)'),
  (3, 'Medium (interested)', 'The system is considered to have moderate value to the threat agent.
The threat agent will attempt to attack the system on a frequent basis. It is also considered
unlikely that the threat agent can be deterred from initiating the attack by the existence of non-
system deterrents'),
  (4, 'High (committed)', 'The system is considered to have significant value to the threat agent.
The threat agent will attempt to attack the system on a persistent and frequent basis. It is
considered highly unlikely that the threat agent can be deterred from initiating the attack by the
existence of non-system deterrents'),
  (5, 'Very high (focused)', 'Threat agent has a primary aim to attack the system')
;
```

```
INSERT INTO Capability_LU VALUES
  (0, 'Very little', 'Threat agent has almost no capabilities or resources. Matches an attack
potential of Basic'),
  (1, 'Little', 'Threat agent has very modest capabilities and resources. Matches an attack
potential of Enhanced-Basic'),
  (2, 'Limited', 'Threat agent has modest capabilities and resources. Matches an attack potential of
Moderate'),
  (3, 'Significant', 'Threat agent is capable and has significant resources. Matches an attack
potential of High'),
  (4, 'Formidable', 'Threat agent is extremely capable and well-resourced. Matches an attack
potential of Beyond High')
;
```

E.2.2 Core tables

Core tables are those that contain the main body of the analysis. This covers the assets, threats, threat agents, weaknesses, vulnerabilities and unwanted-incidents. The tables make use of many foreign key relationships that ensure that terms stored in the database are restricted to those values found in the lookup tables using only the index of the lookup tables. As such a *SELECT * FROM <<table-name>>* query may return non-user readable output.

```
CREATE TABLE Asset_T (
    AssetId INT NOT NULL AUTO_INCREMENT,
  AssetName Text(50) NOT NULL,
  AssetDescription Text(1024),
  CitationId INT,
  AssetImpactWeight INT,
  PRIMARY KEY (AssetId),
  INDEX (AssetImpactWeight),
  FOREIGN KEY (AssetImpactWeight) REFERENCES AssetValue_LU (AssetImpact),
  INDEX (CitationId),
  FOREIGN KEY (CitationId) REFERENCES Citation_LU (CitationId)
) ENGINE = InnoDB
;
```

```
CREATE TABLE System_T (
    SystemId INT NOT NULL AUTO_INCREMENT,
  PRIMARY KEY (SystemID),
  SystemName Text(50) NOT NULL,
    SystemDescription Text(1024),
  CitationId INT,
  INDEX (CitationId),
  FOREIGN KEY (CitationId) REFERENCES Citation_LU (CitationId)
) ENGINE = InnoDB
;
```

```
CREATE TABLE ThreatAgent_T (
    ThreatAgentId INT NOT NULL AUTO_INCREMENT,
  PRIMARY KEY (ThreatAgentId),
    TA_name Text(50) NOT NULL,
    TA_description Text(1024) NOT NULL,
    AttackTimeValue INT,
    AttackExpertise INT,
  AttackKnowledge INT,
  AttackOpportunity INT,
  AttackEquipment INT,
  INDEX (AttackExpertise),
  FOREIGN KEY (AttackExpertise) REFERENCES AttackExpertise_LU (AttackExpertise),
  INDEX (AttackKnowledge),
  FOREIGN KEY (AttackKnowledge) REFERENCES AttackKnowledge_LU (AttackKnowledge),
  INDEX (AttackOpportunity),
  FOREIGN KEY (AttackOpportunity) REFERENCES AttackOpportunity_LU (AttackOpportunity),
  INDEX (AttackEquipment),
  FOREIGN KEY (AttackEquipment) REFERENCES AttackEquipment_LU (AttackEquipment)
) ENGINE = InnoDB
;
```

```
CREATE TABLE Threat_T (
    ThreatId INT NOT NULL AUTO_INCREMENT,
  PRIMARY KEY (ThreatId),
  ThreatName Text(50),
    ThreatDescription Text(1024)
) ENGINE = InnoDB
;
```

```
CREATE TABLE UnwantedIncident_T (
    UnwantedIncidentId INT NOT NULL AUTO_INCREMENT,
  PRIMARY KEY (UnwantedIncidentId),
  Name Text(50),
    Description Text(1024)
) ENGINE = InnoDB
;
```

```
CREATE TABLE Weakness_T (
    WeaknessId INT NOT NULL AUTO_INCREMENT,
  PRIMARY KEY (WeaknessId),
    WeaknessName Text(50),
    WeaknessDescription Text(1024)
) ENGINE = InnoDB
;
```

```
CREATE TABLE Objective_T (
    ObjectiveId INT NOT NULL AUTO_INCREMENT,
    Objective Text(255) NOT NULL,
    Citation INT,
    INDEX (Citation),
    FOREIGN KEY (Citation) REFERENCES Citation_LU (CitationId),
  PRIMARY KEY (ObjectiveId)
)
;
```

```
CREATE TABLE Requirement_T (
    RequirementId INT NOT NULL AUTO_INCREMENT,
  PRIMARY KEY (RequirementId),
    Requirement Text(255) NOT NULL,
  Citation INT,
    RequirementType INT NOT NULL,
    CCReference INT,
    INDEX (CCReference),
    FOREIGN KEY (CCReference) REFERENCES CC_Components_LU (ComponentID),
    INDEX (RequirementType),
    FOREIGN KEY (RequirementType) REFERENCES RequirementType_LU (RequirementTypeId),
    INDEX (Citation),
    FOREIGN KEY (Citation) REFERENCES Citation_LU (CitationId)
)
;
```

E.2.3 Linking tables

Linking tables are used throughout the database to store data that combines two or more tables. For example an asset may appear in many systems, an objective may be tied to an asset.

NOTE: Linking tables are used to resolve many-to-many relationships identified in the UML models in the core of the present document.

```
CREATE TABLE AssetObjective_LT (
  ObjectiveId INT,
  AssetId INT,
  INDEX (ObjectiveId),
  INDEX (AssetId),
  FOREIGN KEY (ObjectiveId) REFERENCES Objective_T (ObjectiveId),
  FOREIGN KEY (AssetId) REFERENCES Asset_T (AssetId)
)
;
```

```
CREATE TABLE SystemObjective_LT (
  ObjectiveId INT,
  SystemId INT,
  INDEX (ObjectiveId),
  INDEX (SystemId),
  FOREIGN KEY (ObjectiveId) REFERENCES Objective_T (ObjectiveId),
  FOREIGN KEY (SystemId) REFERENCES System_T (SystemId)
)
;
```

```
CREATE TABLE ProblemsToAvoid_LT (
    UnwantedIncidentId INT,
  SystemId INT,
  ObjectiveId INT,
  INDEX (UnwantedIncidentId),
  INDEX (SystemId),
  INDEX (ObjectiveId),
  FOREIGN KEY (ObjectiveId) REFERENCES Objective_T (ObjectiveId),
  FOREIGN KEY (SystemId) REFERENCES System_T (SystemId),
  FOREIGN KEY (UnwantedIncidentId) REFERENCES UnwantedIncident_T (UnwantedIncidentId)
) ENGINE = InnoDB
;
```

```
CREATE TABLE RiskAssesment_LT (
    VulnerabilityId INT NOT NULL AUTO_INCREMENT,
  PRIMARY KEY (VulnerabilityId),
    AssetId INT,
    WeaknessId INT,
    ThreatAgentId INT,
  Likelihood INT,
    RiskAssesmentDate DateTime,
  INDEX (AssetId),
  INDEX (WeaknessId),
  INDEX (ThreatAgentId),
  INDEX (Likelihood),
  FOREIGN KEY (AssetId) REFERENCES Asset_T (AssetId),
  FOREIGN KEY (WeaknessId) REFERENCES Weakness_T (WeaknessId),
  FOREIGN KEY (ThreatAgentId) REFERENCES ThreatAgent_T (ThreatAgentId),
  FOREIGN KEY (Likelihood) REFERENCES Likelihood_LU (LikelihoodId)
)
ENGINE = InnoDB
;
```

```
CREATE TABLE SystemComponents_LT (
    SystemId INT,
    AssetId INT,
  INDEX (SystemId),
  FOREIGN KEY (SystemId) REFERENCES System_T (SystemId),
  INDEX (AssetId),
  FOREIGN KEY (AssetId) REFERENCES Asset_T (AssetId)
) ENGINE = InnoDB
;
CREATE TABLE ThreatEnabler_LT (
    ThreatAgentId INT,
  ThreatId INT,
  INDEX (ThreatAgentId),
  INDEX (ThreatId),
  FOREIGN KEY (ThreatAgentId) REFERENCES ThreatAgent_T (ThreatAgentId),
  FOREIGN KEY (ThreatId) REFERENCES Threat_T (ThreatId)
) ENGINE = InnoDB
;
```

E.2.4 Void

Annex F:
Void

Annex G (informative): TVRA Risk Calculation Template and Tool

The evaluation and calculation of the factors that affect the risks posed by particular threat groups (as defined in steps 4, 5, 6 and 7 of the TVRA method) have been consolidated into a MS Excel® spreadsheet available as an electronic attachment in ts_10216501v050205p0.zip which accompanies the present document. An example entry in this spreadsheet is shown in table G.1.

NOTE: Excel® is the trade name of a product supplied by Microsoft. This information is given for the convenience of users of the present document and does not constitute an endorsement by ETSI of the product named. Equivalent products may be used if they can be shown to lead to the same results.

Table G.1: Example row entry in the TVRA risk calculation spreadsheet

Description of attack	Attack analysis					Impact (resultant)	Risk
	Factor	Analyst estimation	Value	Potential	Likelihood		
To be added	Time	<= 1 day	0	Beyond High	Very unlikely	Low	**Minor**
	Expertise	Expert	6				
	Knowledge	Critical	11				
	Opportunity	Unnecessary	0				
	Equipment	Multiple bespoke	9				
	Attacker Theat level		Moderate				
	Attacker motivation	Low (curious)					
	Attacker capability	Formidable					
	Asset Impact	Low	1				
	Resultant impact	Low	1				
	Intensity	Single instance	0				

Each of the values in the "Analyst estimation" column can be selected from drop-down lists which limit the entry to legitimate values only as shown in table G.2.

Table G.2: Entering data into the risk calculation spreadsheet

Description of attack	Attack analysis					Impact (resultant)	Risk
	Factor	Analyst estimation	Value	Potential	Likelihood		
To be added	Time	<= 1 day	0	Beyond High	Very unlikely	Low	**Minor**
	Expertise	Expert	6				
	Knowledge	Critical	11				
	Opportunity	Unnecessary	0				
	Equipment	Unnecessary	9				
	Attacker Theat level	Easy	Moderate				
	Attacker motivation	Moderate					
	Attacker capability	Difficult					
	Asset Impact	None	1				
	Resultant impact	Low	1				
	Intensity	Single instance	0				

The attached spreadsheet provides for auto-calculation of the content of the Potential, Likelihood, Impact and Risk columns.

Annex H (informative): TVRA Countermeasure Cost-Benefit Analysis Template and Tool

The calculations described in step 8 of the TVRA method for analysing the costs and benefits of specific countermeasure solutions have been consolidated into a MS Excel® spreadsheet that is available as an electronic attachment in ts_10216501v050205p0.zip which accompanies the present document. An example entry in this spreadsheet is shown in table H.1.

Each of the values in the "Cost/Value" column and the "Regulatory Impact" and "Market Acceptance" can be selected from drop-down lists which limit the entry to legitimate values only as shown in table H.2. The "Original Count" column in the "Benefits" section of the sheet should show number of critical, major and minor risks related to the countermeasure calculated before its implementation. The "Revised Count" column shows the appropriate numbers of risks calculated after the countermeasure has been implemented.

Table H.1: Example row entry in the Countermeasures Cost-Benefit Analysis table

Countermeasure	Cost		Benefit			Result
	Category	Value	Risk Level	Original Count	Revised Count	
Reduce frequency of repeated messages	**Standards design**	Low Impact	**Minor**	0	0	**14**
	Implementation	No Impact	**Major**	0	3	
	Operation	No Impact	**Critical**	3	0	
	Regulatory Impact			No Impact		
	Market Acceptance			No Impact		

Table H.2: Entering data into the cost/benefit calculation spreadsheet

Countermeasure	Cost		Benefit			Result
	Category	Value	Risk Level	Original Count	Revised Count	
Reduce frequency of repeated messages	**Standards design**	Low Impact	**Minor**	0	0	**14**
	Implementation	Low Impact	**ajor**	0	3	
	Operation		**itical**	3	0	
	Regulatory Impact			No Impact		
	Market Acceptance			No Impact		

No Impact
Low Impact
Medium Impact
Major Impact

Annex I (informative): Bibliography

I.1 UML

The following sources may give the reader a deeper understanding of the use and application of UML and of UML2 in particular.

[UML2-Style] "The elements of UML™ 2.0 style", Scott W. Ambler, Cambridge University Press, 2005. ISBN 0-521-61678-6.

[UML2-Doldi] "UML 2 illustrated: Developing real-time & communications systems", Laurent Doldi, TMSO 2003. ISBN 2-9516600-1-4.

[UML2-OReilly] "UML 2.0 in a nutshell", Dan Pilone with Neil Pitman, O'Reilly. ISBN 0-596-00795-7.

I.2 Others

- ETSI ES 282 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub-System (NASS)".
- IETF RFC 2535: "Domain Name System Security Extensions".
- IETF RFC 3403: "Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database".
- IETF RFC 2915: "The Naming Authority Pointer (NAPTR) DNS Resource Record".
- Draft-ietf-dnsext-dnssec-protocol-06 (2004): "Protocol Modifications for the DNS Security Extensions".
- Draft-ietf-dnsext-dnssec-records-08 (2004): "Resource Records for DNS Security Extensions".
- Draft-ietf-dnsext-dnssec-intro-11 (2004): "DNS Security Introduction and Requirements".
- ETSI TR 102 420: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Review of activity on security".

Annex J (informative): Change history

Date	WG Doc.	CR	Rev	CAT	Title / Comment	Current Version	New Version
19-10-2010	TISPAN07(10)0139R1	1	-	F/D	ETSI TS 102 165-1 CR to introduce requirements and countermeasure cost-benefit analysis and to make minor editorial changes to clause 4.	4.2.1	4.2.2
19-10-2010	TISPAN07(10)0140R2	2	-	B	ETSI TS 102 165-1 CR to revise title of eTVRA method to TVRA method and to add three new steps to the TVRA method based on experience from TVRA exercises in TISPAN and ITS and to make minor editorial changes to clause 5.	4.2.1	4.2.2
19-10-2010	TISPAN07(10)0141R1	3	-	B	ETSI TS 102 165-1 CR to add three new steps to the TVRA method based on experience from TVRA exercises in TISPAN and ITS and to make minor editorial changes to clause 6.	4.2.1	4.2.2
2-12-2010	TISPAN07(10)0164	4	-	D	Removal of ENUM analysis.	4.2.2	4.2.3
16-9-2017	CYBER(16)008022				Transfer to ETSI CYBER for maintenance.	4.2.3	5.0.1
5-1-2017	CYBER(16)008021r1	1		B	Modification to the mapping of vulnerability rating to likelihood of attack.	5.0.1	5.2.1
7-8-2017	CYBER(17)011009	2		B	Revision addressing removal of bulk of Common Criteria text and replacement by simple example and reference.	5.2.1	5.2.2
8-8-2017	CYBER(17)011010	3		B	Revision of annex E adding database tables for new motivation treatment.	5.2.2	5.2.3
22-11-2021	CYBER(21)026011	1	-	F	TVRA method fix of spreadsheet and method description in Annex G.	5.2.3	5.2.4
01-2022					Publication with removal of outdated introduction.	5.2.4	5.2.5

History

Document history		
V4.1.1	February 2003	Publication
V4.2.1	December 2006	Publication
V4.2.3	March 2011	Publication
V5.2.3	October 2017	Publication
V5.2.5	January 2022	Publication