TECHNICAL REPORT

ISO/IEC TR 20004

Second edition
2015-12-15

Information technology — Security techniques — Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045

Technologies de l'information — Techniques de sécurité — Redéfinition de l'analyse de vulnérabilité de logiciel selon l'ISO/CEI 15408 et l'ISO/CEI 18045

Reference number
ISO/IEC TR 20004:2015(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC/TR 20004:2012), which has been technically revised.

Introduction

This Technical Report is intended to provide added refinement, detail and guidance to the vulnerability analysis activities outlined in ISO/IEC 18045:2008 for the software elements of a TOE. Specifically, it is intended to add refinement and clarification of the "Potential vulnerability identification from public sources" (AVA_VAN.1.2E/2.2E/3.2E/4.2E) and "Penetration testing" (AVA_VAN.1.3E/2.4E/3.4E/4.4E) evaluator actions, which are currently imprecise in regards to searching for, identifying and testing relevant potential vulnerabilities. This Technical Report provides guidance on an approach to objectively search for, identify, filter and test potential vulnerabilities utilizing international ad hoc standard resources for software weaknesses and attack patterns. The set of relevant software weaknesses and attack patterns identified through this guidance represent a minimal set for analysis under the AVA_VAN assurance family in an ISO/IEC 15408 evaluation. Additional weaknesses and attack patterns may be determined relevant by specific national schemes, technical communities, associated protection profiles or other sources. In utilizing these standard structured resources, the approach defined here has the added benefit of being equally applicable to the TOE development process as it does to the TOE security evaluation process. This means that relevant weaknesses and attack patterns identified and tested for during development, whether defined ad hoc or as part of a structured assurance case, can provide a head start template for a TOE-specific set of relevant weaknesses and attack patterns for use in the security evaluation.

This Technical Report is intended to be used in conjunction with and, as an addendum to, ISO/IEC 18045.

This Technical Report does not address all possible vulnerability analysis methods, in particular those that fall outside the scope of the activities outlined in ISO/IEC 18045. It uses the common weakness enumeration (CWE) and the common attack pattern enumeration and classification (CAPEC) to identify possible attacks. It does not preclude the use of other appropriate identification resources by evaluators.

The target audience for this Technical Report is evaluators applying ISO/IEC 15408 and certifiers confirming evaluator actions, developers, PP/ST authors (to include Technical Communities), evaluator sponsors and other parties interested in IT security.

This Technical Report recognizes that not all questions concerning IT security evaluation will be answered herein and that further interpretations will be needed. Individual schemes will determine how to handle such interpretations and other guidance, although these can be subject to mutual recognition agreements.

Information technology — Security techniques — Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045

1 Scope

This Technical Report refines the AVA_VAN assurance family activities defined in ISO/IEC 18045 and provides more specific guidance on the identification, selection and assessment of relevant potential vulnerabilities in order to conduct an ISO/IEC 15408 evaluation of a software target of evaluation. This Technical Report leverages publicly available information security resources to support the method of scoping and implementing ISO/IEC 18045 vulnerability analysis activities. The Technical Report currently uses the common weakness enumeration (CWE) and the common attack pattern enumeration and classification (CAPEC), but does not preclude the use of any other appropriate resources. Furthermore, this Technical Report is not meant to address all possible vulnerability analysis methods, including those that fall outside the scope of the activities outlined in ISO/IEC 18045.

This Technical Report does not define evaluator actions for certain high assurance ISO/IEC 15408 components, where there is as yet no generally agreed guidance.

2 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

2.1
assurance case
structured set of claims, arguments and a corresponding body of evidence to demonstrate that a system satisfies specific claims with respect to its security properties

2.2
attack pattern
abstracted approach utilized to attack software

2.3
attack potential
measure of the effort to be expended in attacking a TOE, expressed in terms of an attacker's expertise, resources and motivation

[SOURCE: ISO/IEC 15408-1:2009, 3.1.5]

2.4
confirm
declare that something has been reviewed in detail with an independent determination of sufficiency

Note 1 to entry: The level of rigour required depends on the nature of the subject matter. This term is only applied to evaluator actions.

[SOURCE: ISO/IEC 15408-1:2009, 3.1.14]

2.5
CVE vulnerability
vulnerability listed in CVE

2.6
determine
affirm a particular conclusion based on independent analysis with the objective of reaching a particular conclusion

Note 1 to entry: The usage of this term implies a truly independent analysis, usually in the absence of any previous analysis having been performed. Compare with the terms "confirm" or "verify" which imply that an analysis has already been performed which needs to be reviewed.

[SOURCE: ISO/IEC 15408-1:2009, 3.1.22]

2.7
encountered potential vulnerabilities
potential weakness in the TOE identified by the evaluator while performing evaluation activities that could be used to violate the SFRs

[SOURCE: ISO/IEC 15408-1:2009, 3.5.2]

2.8
evaluation
assessment of a PP, an ST or a TOE, against defined criteria

[SOURCE: ISO/IEC 15408-1:2009, 3.1.26]

2.9
exploitable vulnerability
weakness in the TOE that can be used to violate the SFRs in the operational environment for the TOE

[SOURCE: ISO/IEC 15408-1:2009, 3.5.3]

2.10
potential vulnerability
suspected, but not confirmed, weakness

Note 1 to entry: Suspicion is by virtue of a postulated attack path to violate the SFRs.

[SOURCE: ISO/IEC 15408-1:2009, 3.5.5]

2.11
Protection Profile
implementation-independent statement of security needs for a TOE type

[SOURCE: ISO/IEC 15408-1:2009, 3.1.52]

2.12
residual vulnerability
weakness that cannot be exploited in the operational environment for the TOE, but that could be used to violate the SFRs by an attacker with greater attack potential than is anticipated in the operational environment for the TOE

[SOURCE: ISO/IEC 15408-1:2009, 3.5.6]

2.13
Security Target
implementation-dependent statement of security needs for a specific identified TOE

[SOURCE: ISO/IEC 15408-1:2009, 3.1.63]

2.14
selection
specification of one or more items from a list

[SOURCE: ISO/IEC 15408-1:2009, 3.1.64]

2.15
target of evaluation
set of software, firmware and/or hardware possibly accompanied by guidance

[SOURCE: ISO/IEC 15408-1:2009, 3.1.70]

2.16
threat agent
entity that can adversely act on assets

[SOURCE: ISO/IEC 15408-1:2009, 3.1.71]

2.17
TOE evaluation
assessment of a TOE against defined criteria

[SOURCE: ISO/IEC 15408-1:2009, 3.1.72]

2.18
TOE-relevant CVE vulnerabilities
CVE vulnerabilities from all versions of the TOE product family or CVE vulnerabilities associated with products of the same technology type

2.19
verify
rigorously review in detail with an independent determination of sufficiency

Note 1 to entry: Also see *confirm* (2.4). The term *verify* has more rigorous connotations. It is used in the context of evaluator actions where an independent effort is required of the evaluator.

[SOURCE: ISO/IEC 15408-1:2009, 3.1.84]

2.20
vulnerability
weakness in the TOE that can be used to violate the SFRs in some environment

[SOURCE: ISO/IEC 15408-1:2009, 3.5.7]

2.21
weakness
characteristic or property of a TOE that, in proper conditions, could contribute to the introduction of vulnerabilities within that TOE

3 Abbreviated terms

The following abbreviations are used in one or more parts of ISO/IEC 20004.

CAPEC™[a] Common Attack Pattern Enumeration and Classification

CVE®[a] Common Vulnerabilities and Exposures

CWE™[a] Common Weakness Enumeration

ETR Evaluation Technical Report

PP Protection Profile

SAR Security Assurance Requirement

SFR Security Functional Requirement

ST Security Target

TOE Target of Evaluation

TSF TOE Security Functionality

TSFI TSF Interface

a CAPEC, CVE and CWE are examples of suitable products available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO of these products.

4 Background context

ISO/IEC 15408-3:2008, 15.1 defines "development vulnerabilities" as vulnerabilities which take advantage of some properties of the TOE which were introduced during its development. In the same sub-clause, ISO/IEC 15408-3 states that an assessment of development vulnerabilities is covered by the assurance family called "vulnerability analysis" (AVA_VAN). ISO/IEC 15408-3 expects this assessment to determine whether potential vulnerabilities identified could allow attackers to violate the SFRs and to deal with the threat that an attacker will be able to discover flaws [as the identified potential vulnerabilities] (ISO/IEC 15408-3:2008, 15.2.1).

The levels in the AVA_VAN assurance family are ordered as follows:

— AVA_VAN.1 "vulnerability survey" (ISO/IEC 15408-3:2008, 15.2.3);

— AVA_VAN.2 "vulnerability analysis" (ISO/IEC 15408-3:2008, 15.2.4);

— AVA_VAN.3 "focused vulnerability analysis" (ISO/IEC 15408-3:2008, 15.2.5);

— AVA_VAN.4 "methodical vulnerability analysis" (ISO/IEC 15408-3:2008, 15.2.6);

— AVA_VAN.5 "advanced methodical vulnerability analysis" (ISO/IEC 15408-3:2008, 15.2.7).

AVA_VAN.1 is the lowest level and AVA_VAN.5 is the highest level in the AVA_VAN assurance family.

ISO/IEC 15408-3 states the following two evaluator actions for each of the AVA_VAN levels.

— "Potential vulnerability identification from public sources" action

  The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

  — AVA_VAN.1.2E (ISO/IEC 15408-3:2008, 15.2.3.4.2);

  — AVA_VAN.2.2E (ISO/IEC 15408-3:2008, 15.2.4.4.2);

  — AVA_VAN.3.2E (ISO/IEC 15408-3:2008, 15.2.5.4.2);

  — AVA_VAN.4.2E (ISO/IEC 15408-3:2008, 15.2.6.4.2);

  — AVA_VAN.5.2E (ISO/IEC 15408-3:2008, 15.2.7.4.2).

— "Penetration testing" action

  The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing.

  — Basic attack potential" in AVA_VAN.1.3E (ISO/IEC 15408-3:2008, 15.2.3.4.3);

  — Basic attack potential" in AVA_VAN.2.4E (ISO/IEC 15408-3:2008, 15.2.4.4.4);

— Enhanced-Basic attack potential" in AVA_VAN.3.4E (ISO/IEC 15408-3:2008, 15.2.5.4.4);

— Moderate attack potential" in AVA_VAN.4.4E (ISO/IEC 15408-3:2008, 15.2.6.4.4);

— High attack potential" in AVA_VAN.5.4E (ISO/IEC 15408-3:2008, 15.2.7.4.4).

ISO/IEC 18045 further specifies certain work units associated with the "Potential vulnerability identification from public sources" action (in ISO/IEC 18045:2008, 14.2.1.5, 14.2.2.5, 14.2.3.5 and 14.2.4.5) as follows.

— AVA_VAN.1-3, AVA_VAN.2-3, AVA_VAN.3-3, AVA_VAN.4-3

The evaluator shall examine sources of information publicly available to identify potential vulnerabilities in the TOE.

The availability of information, that may be readily available to an attacker that helps to identify and facilitate attacks, effectively operates to substantially enhance the attack potential of a given attacker. The accessibility of vulnerability information and sophisticated attack tools on the Internet makes it more likely that this information will be used in attempts to identify potential vulnerabilities in the TOE and exploit them. Modern search tools make such information easily available to the evaluator, and the determination of resistance to published potential vulnerabilities and well known generic attacks can be achieved in a cost-effective manner.

The search of the information publicly available should be focused on those sources that refer specifically to the product from which the TOE is derived. The extensiveness of this search should consider the following factors: TOE type, evaluator experience in this TOE type, expected attack potential and the level of ADV evidence available.

— AVA_VAN.1-4, AVA_VAN.2-5, AVA_VAN.3-5, AVA_VAN.4-5

The evaluator shall record in the ETR the identified potential vulnerabilities that are candidates for testing and applicable to the TOE in its operational environment.

It may be identified that no further consideration of the potential vulnerability is required if, for example, the evaluator identifies that measures in the operational environment, either IT or non-IT, prevent exploitation of the potential vulnerability in that operational environment.

The evaluator records any reasons for exclusion of potential vulnerabilities from further consideration if the evaluator determines that the potential vulnerability is not applicable in the operational environment. Otherwise, the evaluator records the potential vulnerability for further consideration.

A list of potential vulnerabilities applicable to the TOE in its operational environment, which can be used as an input into penetration testing activities, shall be reported in the ETR by the evaluators.

NOTE As stated in ISO/IEC 18045:2008, 14.2.5, ISO/IEC 18045 does not specify any work units at the AVA_VAN.5 level.

The content of the "Potential vulnerability identification from public sources" evaluator action is summarized in the following diagram.

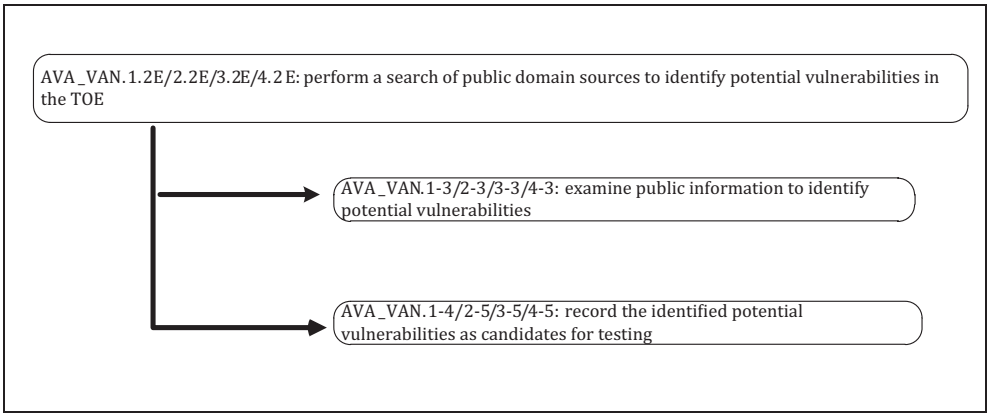

Figure 1 — "Potential vulnerability identification from public sources" evaluator action summary

ISO/IEC 18045 further specifies certain work units associated with the "Penetration testing" action (in ISO/IEC 18045:2008, 14.2.1.6, 14.2.2.7, 14.2.3.7 and 14.2.4.7) as follows.

— AVA_VAN.1-5, AVA_VAN.2-6, AVA_VAN.3-6, AVA_VAN.4-6

The evaluator shall devise penetration tests, based on the independent search for potential vulnerabilities.

The evaluator prepares for penetration testing as necessary to determine the susceptibility of the TOE, in its operational environment, to the potential vulnerabilities identified during the search of the sources of information publicly available. Any current information provided to the evaluator by a third party (e.g. evaluation authority) regarding known potential vulnerabilities will be considered by the evaluator.

The evaluator is not expected to test for potential vulnerabilities (including those in the public domain) beyond those which required the following:

— a Basic attack potential (in the case of AVA_VAN.1-5);

— a Basic attack potential (in the case of AVA_VAN.2-6);

— a Enhanced-Basic attack potential (in the case of AVA_VAN.3-6);

— a Moderate attack potential (in the case of AVA_VAN.4-6).

— AVA_VAN.1-6, AVA_VAN.2-7, AVA_VAN.3-7, AVA_VAN.4-7

The evaluator shall produce penetration test documentation for the tests based on the list of potential vulnerabilities in sufficient detail to enable the tests to be repeatable.

With an understanding of the potential vulnerability, the evaluator determines the most feasible way to test for the TOE's susceptibility. Specifically, the evaluator considers the following:

a) the TSFI or other TOE interface that will be used to stimulate the TSF and observe responses;

b) initial conditions that will need to exist for the test (i.e. any particular objects or subjects that will need to exist and security attributes they will need to have);

c) special test equipment that will be required to either stimulate a TSFI or make observations of a TSFI;

d) whether theoretical analysis should replace physical testing, particularly relevant where the results of an initial test can be extrapolated to demonstrate that repeated attempts of an attack are likely to succeed after a given number of attempts.

— AVA_VAN.1-7, AVA_VAN.2-8, AVA_VAN.3-8, AVA_VAN.4-8

The evaluator shall conduct penetration testing.

The evaluator uses the penetration test documentation resulting from work unit

— AVA_VAN.1-5 (in the case of AVA_VAN.1-7),

— AVA_VAN.2-6 (in the case of AVA_VAN.2-8),

— AVA_VAN.3-6 (in the case of AVA_VAN.3-8), or

— AVA_VAN.4-6 (in the case of AVA_VAN.4-8)

as a basis for executing penetration tests on the TOE, but this does not preclude the evaluator from performing additional ad hoc penetration tests.

— AVA_VAN.1-8, AVA_VAN.2-9, AVA_VAN.3-9, AVA_VAN.4-9

The evaluator shall record the actual results of the penetration tests.

— AVA_VAN.1-9, AVA_VAN.2-10, AVA_VAN.3-10, AVA_VAN.4-10

The evaluator shall report in the ETR the evaluator penetration testing effort, outlining the testing approach, configuration, depth and results.

— AVA_VAN.1-10 and AVA_VAN.2-11

The evaluator shall examine the results of all penetration testing to determine that the TOE, in its operational environment, is resistant to an attacker possessing a Basic attack potential.

If the results reveal that the TOE, in its operational environment, has vulnerabilities exploitable by an attacker possessing less than Enhanced-Basic attack potential, then this evaluator action (namely AVA_VAN.1.3E or AVA_VAN.2.4E) fails.

The guidance in ISO/IEC 18045:2008, B.4 should be used to determine the attack potential required to exploit a particular vulnerability and whether it can therefore be exploited in the intended environment.

— AVA_VA.3-11

The evaluator shall examine the results of all penetration testing to determine that the TOE, in its operational environment, is resistant to an attacker possessing an Enhanced-Basic attack potential.

If the results reveal that the TOE, in its operational environment, has vulnerabilities exploitable by an attacker possessing less than Moderate attack potential, then this evaluator action (namely AVA_VAN.3.4E) fails.

The guidance in ISO/IEC 18045:2008, B.4 should be used to determine the attack potential required to exploit a particular vulnerability and whether it can therefore be exploited in the intended environment.

— AVA_VAN.4-11

The evaluator shall examine the results of all penetration testing to determine that the TOE, in its operational environment, is resistant to an attacker possessing a Moderate attack potential.

If the results reveal that the TOE, in its operational environment, has vulnerabilities exploitable by an attacker possessing less than a High attack potential, then this evaluator action (namely AVA_VAN.4.4E) fails.

The guidance in ISO/IEC 18045:2008, B.4 should be used to determine the attack potential required to exploit a particular vulnerability and whether it can therefore be exploited in the intended environment.

— AVA_VAN.1-11, AVA_VAN.2-12, AVA_VAN.3-12, AVA_VAN.4-12

The evaluator shall report in the ETR all exploitable vulnerabilities and residual vulnerabilities, detailing for each of the following:

a) its source (e.g. ISO/IEC 18045 evaluation methodology activity being undertaken when it was conceived, known to the evaluator, read in a publication);

b) the SFR(s) not met;

c) a description;

d) whether it is exploitable in its operational environment or not (i.e. exploitable or residual);

e) the amount of time, level of expertise, level of knowledge of the TOE, level of opportunity and the equipment required to perform the identified vulnerabilities, and the corresponding values using the ISO/IEC 18045:2008, Annex B.4, Tables B.2 and B.3

NOTE As stated in ISO/IEC 18045:2008, 14.2.5, ISO/IEC 18045 does not specify any work units at the AVA_VAN.5 level.

The content of the "Penetration testing" evaluator action is summarized in the following diagram.

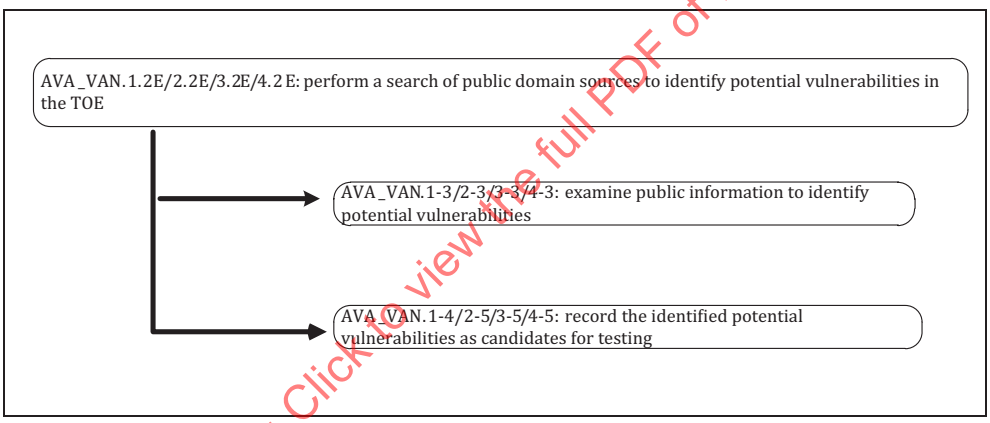

Figure 2 — "Penetration testing" evaluator action summary

5 Vulnerability assessment activities

ISO/IEC 15408 and ISO/IEC 18045 support an assurance case based framework for the specification and evaluation of the security of IT products in the following way. Under ISO/IEC 15026-2, the elements of these assurance cases can be captured and conveyed in a consistent and structured fashion. Within an ISO/IEC 15026-2 structured assurance case context, the vulnerability assessment activities defined under ISO/IEC 18045 can be characterized as identifying specific assurance claims (through the determination of relevant potential vulnerabilities and patterns of attack for which the TOE is tested), identifying relevant and acceptable argumentation for those claims [through the determination of relevant and acceptable techniques for evaluation (by default this is penetration planning and execution)], and capturing relevant and acceptable evidence for that argumentation (through the structured reporting of evaluation activities and results). In aggregate, the results of following the guidance outlined in 5.1 and 5.2 can be related and conveyed in the form of a ISO/IEC 15026 compliant structured assurance case potentially yielding improved consistency of evaluation as well as the potentially improved coordination between development and evaluation.

5.1 Determine relevant potential vulnerabilities

ISO/IEC 18045 defines the work units for determining relevant potential vulnerabilities in the following subclauses:

— ***14.2.1.5.1 Work unit AVA_VAN.1-3***;

— ***14.2.2.5.1 Work unit AVA_VAN.2-3***;

— ***14.2.3.5.1 Work unit AVA_VAN.3-3***;

— ***14.2.4.5.1 Work unit AVA_VAN.4-3***.

Common Vulnerabilities and Exposures (CVE®, ITU-T x.1520) is a dictionary of common names (i.e., CVE Identifiers) for publicly known information security vulnerabilities, while its Common Configuration Enumeration (CCE™) provides identifiers for security configuration issues and exposures. CVE's common identifiers make it easier to share data across separate network security databases and tools, and provide a baseline for evaluating the coverage of an organization's security tools.

CVE is:

— One name for one vulnerability or exposure.

— One standardized description for each vulnerability or exposure.

— A dictionary rather than a database.

— How disparate databases and tools can "speak" the same language.

— A way to interoperability and better security coverage.

— A basis for evaluation among tools and databases.

— Free for public download and use.

— Industry-endorsed via the CVE Editorial Board and CVE-Compatible Products.

CVE was launched in 1999 when most information security tools used their own databases with their own names for security vulnerabilities. At that time, there was no significant variation among products and no easy way to determine when the different databases were referring to the same problem. The consequences were potential gaps in security coverage and no effective interoperability among the disparate databases and tools. In addition, each tool vendor used different metrics to state the number of vulnerabilities or exposures they detected, which meant there was no standardized basis for evaluation among the tools.

CVE's common, standardized identifiers provided a systematic approach to these problems.

CVE is now a widely adopted industry standard for vulnerability and exposure names. CVE Identifiers provide reference points for data exchange so that information security products and services can speak with each other. CVE Identifiers also provides a baseline for evaluating the coverage of tools and services to help users determine which tools are most effective and appropriate for their organization's needs. In short, products and services compatible with CVE provide better coverage, easier interoperability, and enhanced security.

There now exists a publicly available, substantive standardized enumeration of potential software vulnerabilities (weaknesses) in the form of the Common Weakness Enumeration (CWE™, ITU-T x.1524).[1)] The Common Weakness Enumeration is an international community-developed formal collection of common software weaknesses. It serves as a common language for describing software security weaknesses, a standard measuring stick for software security tools targeting these vulnerabilities, and as a baseline standard for weakness identification, mitigation, and prevention efforts. Leveraging the diverse thinking on this topic from academia, the commercial sector, and government, CWE unites a

1) http://cwe.mitre.org.

valuable breadth and depth of content and structure to serve as a unified standard. Its objective is to help shape and mature the code security assessment industry and also accelerate the use and utility of software assurance capabilities for organizations in reviewing the software systems they acquire or develop. CWE content will continue to evolve with public participation and contributions to form a standard mechanism for identifying, collecting, refining, and sharing software weaknesses among the software community.

Given the comprehensiveness of the CWE and with the additional objective of a more focused bounding of scope for IT security evaluations, this Technical Report specifies the use of the CWE as one of the standard resources for identification of potential vulnerabilities as specified in ISO/IEC 18045:2008, 14.2.1.5.1, 14.2.2.5.1, 14.2.3.5.1, 14.2.4.5.1.

In addition to more objectively characterize attack potential in relation to relevant potential vulnerabilities and to support the specification of relevant security/penetration tests, this Technical Report also specifies the identification and selection of relevant attack patterns using the Common Attack Pattern Enumeration and Classification (CAPEC™, ITU-T x.1544)[2)], as the associated standard publicly available resource. To identify and mitigate relevant vulnerabilities in software, the software community needs more than just good software engineering and analytical practices, a solid grasp of software security features, and a powerful set of tools. All of these things are necessary but not sufficient. To be effective, the community needs to think outside of the box and to have a *firm grasp of the attacker's perspective and the approaches used to exploit software*. An appropriate defense can only be established once you know how it will be attacked. The Common Attack Pattern Enumeration and Classification is an international community-developed formal collection of common software attack patterns. Attack patterns are descriptions of common methods for exploiting software providing the attacker's perspective and guidance on ways to mitigate their effect. They derive from the concept of design patterns applied in a destructive rather than constructive context and are generated from in-depth analysis of specific real-world exploit examples. This information when captured in such a formalized way can bring considerable value for software security considerations through all phases of the software development lifecycle (SDLC) and other security-related activities, including the following:

— Requirements gathering

  — identification of relevant security requirements, misuse and abuse cases.

— Architecture and design

  — provide context for architectural risk analysis and guidance for security architecture.

— Implementation and coding

  — prioritize and guide activities of secure code review.

— Software testing and quality assurance

  — provide context for appropriate risk-based and penetration testing.

— Systems operation

  — leverage lessons learned from security incidents into preventative guidance.

— Policy and standard generation

  — guide the identification of appropriate prescriptive organizational policies and International Standards.

Leveraging the diverse thinking on this topic from academia, the commercial sector, and government, CAPEC unites a valuable breadth and depth of content and structure to serve as a unified standard. Its objective is to provide a better understanding of software weaknesses through characterization of how they are likely to be attacked and to guide security/penetration testing efforts. CAPEC content

2) http://capec.mitre.org.

will continue to evolve with public participation and contributions to form a standard mechanism for identifying, collecting, refining, and sharing attack patterns among the software community.

The set of relevant software weaknesses (CWEs) and attack patterns (CAPECs) for a given TOE evaluation are identified through one of two mechanisms: 1) an existing structured assurance case specifying relevant weaknesses and attack patterns or, 2) directly from the public CWE and CAPEC resources.

Both CWE and CAPEC are actively and persistently versioned such that at any time an evaluator can reference the specific version of content that was used to identify the set of relevant software weaknesses (CWEs) and attack patterns (CAPECs) for a given TOE evaluation.

5.1.1 Identify relevant weaknesses and attack patterns from existing structured assurance case

The simplest and most concrete mechanism for identifying relevant weaknesses and attack patterns for a given TOE evalution is the existence of a CWE/CAPEC-adorned ISO/IEC 15026 structured assurance case specified as relevant for that TOE evaluation. If a structured assurance case exists for the TOE then the CWEs and CAPECs identified in the structured assurance case should be considered the relevant set for the IT security evaluation. If multiple structured assurance cases exists for the TOE then the CWEs and CAPECs identified in the most TOE-specific structured assurance case should be considered the relevant set for the IT security evaluation.

5.1.2 Identify relevant weaknesses and attack patterns from public sources

Where no relevant existing structured assurance case is available, the minimal set of relevant potential software weaknesses and attack patterns should be identified from the publicly available CWE and CAPEC resources according to the processes outline in the following two sections.

5.1.2.1 Identify initial set of potentially relevant weaknesses and attack patterns from public sources

The evaluator should identify an initial set of potentially relevant software weaknesses and attack patterns by searching the publicly available CWE and CAPEC lists for relevant entries using the criteria below.

a) Identify initial set of potentially relevant weaknesses.

Search the publicly available CWE list for CWE weaknesses where the following criteria are all true.

1) CWE weaknesses with a minimum adequate level of defined detail.

— For a given CWE weakness, the weakness will be deemed relevant if the following properties are all true.

— The CWE schema element Weakness_Abstraction is defined and equal to “Base” or “Variant”.

— The CWE schema element Applicable_Platforms is defined.

— The CWE schema element Detection_Methods is defined.

— The CWE schema element Related_Attack_Patterns is defined.

Without this minimum adequate level of defined detail weaknesses would be too ambiguous for objective and consistent use as a guiding element of IT security evaluations. Therefore, requiring this minimum level of defined detail for CWE weaknesses does not reduce the effectiveness of the “Penetration testing” (AVA_VAN.1.3E/2.4E/3.4E/4.4E) evaluator actions.

2) CWE weaknesses whose technical context factors are relevant to the TOE and its operational environment.

NOTE For a given CWE weakness, the CWE schema element of "Applicable_Platforms" indicates the relevant technical context for a given weakness including things like language, operating system, hardware architecture, architectural paradigm, environment, technology class, and common platform references. The CWE schema element "Functional_Area" indicates the area of software functionality where a given weakness would typically instantiate within a TOE.

Special consideration should be given to ensure that the initial set contains CWE weaknesses that are identifiable from TOE-relevant CVE vulnerabilities.

b) Identify initial set of potentially relevant attack patterns.

Search the publicly available CAPEC list for CAPEC attack patterns where the following criteria are all true.

1) CAPEC attack patterns with a minimum adequate level of defined detail.

— For a given CAPEC attack pattern, the pattern will be deemed relevant if the following properties are all true.

— The CAPEC schema element Pattern_Completeness is defined and equal to "Complete".

— The CAPEC schema element Pattern_Abstraction is defined and equal to " Standard" or "Detailed".

— The CAPEC schema element Attack_Execution_Flow is defined.

— The CAPEC schema element Technical_Context is defined.

— The CAPEC schema element Related_Weaknesses is defined.

Without this minimum adequate level of defined detail attack patterns would be too ambiguous for objective and consistent use as a guiding element of IT security evaluations. Therefore, requiring this minimum level of defined detail for CAPEC attack patterns does not reduce the effectiveness of the "Penetration testing" (AVA_VAN.1.3E/2.4E/3.4E/4.4E) evaluator actions.

2) CAPEC attack patterns whose technical context factors are relevant to the TOE and its operational environment.

NOTE For a given CAPEC attack pattern, the CAPEC schema element of "Technical Context" indicates the relevant technical context for a given attack pattern including things like architectural paradigm, framework, and platform factors of a CAPEC attack pattern. The CAPEC schema element of "Attack Prerequisites" identifies characteristics or features of the TOE that are to be present for the CAPEC attack pattern to be relevant for a given context. If these factors are not relevant to the TOE, then the corresponding CAPEC attack pattern would not be relevant for a given evaluation and would be filtered out of the set used to identify relevant potential vulnerabilities (CWE weaknesses) for the TOE. Therefore, filtering out these CAPEC attack pattern does not reduce the effectiveness of the "Penetration testing" (AVA_VAN.1.3E/2.4E/3.4E/4.4E) evaluator actions. Given that the complexity of technical context is too great to completely structure in this Technical Report, some level of evaluator interpretation is required for determining relevance for these elements.

c) Correlate relationships between identified CWEs and CAPECs.

The evaluator should examine the relationships between identified weaknesses and attack patterns as defined in the "Related_Attack_Patterns" element of the CWE schema and the "Related_Weaknesses" element of the CAPEC schema. Any CAPEC entries referenced by identified CWEs but not in the list of identified CAPECs and any CWE entries referenced by identified CAPECs but not in the list of identified CWEs should be reevaluated for potential inclusion in the list of relevant weakenesses and attack patterns.

5.1.2.2 Filter initial set of potentially relevant weaknesses and attack patterns

The evaluator should identify and document the set of potentially relevant software weaknesses and attack patterns by applying the following filtering criteria to the initial set identified according to the processes outlined in the previous section above.

ISO/IEC 18045 defines the work units for recording relevant potential vulnerabilities in the following subclauses:

— ***14.2.1.5.2 Work unit AVA_VAN.1-4***;

— ***14.2.2.6.2 Work unit AVA_VAN.2-5***;

— ***14.2.3.6.2 Work unit AVA_VAN.3-5***;

— ***14.2.4.6.2 Work unit AVA_VAN.4-5***.

The purpose of CWE and CAPEC are to enumerate a very broad set of software weaknesses and attack patterns that may be relevant across a wide range of TOE contexts. To bound the set of potential vulnerabilities to a reasonable scope for the IT security evaluation, the initial set of potentially relevant weaknesses and attack patterns identified through the process outlined in 5.1.1 should be filtered by a set of appropriate criteria.

a) Filter relevant weaknesses.

The initial set of potentially relevant weaknesses identified through the process outlined in 5.1.1 are further filtered according to the following criteria to establish the set of relevant weaknesses for the IT security evaluation.

1) Filter out CWE weaknesses which do not contain Detection_Method schema elements specifying automated or black box forms of analysis.

2) Filter out CWE weaknesses which are not relevant due to measures in the operational environment, either IT or non-IT, preventing exploitation of the potential vulnerability in that operational environment. The evaluator should clearly record the specific reasoning involved for each weakness excluded.

By using the above filtering step to filter CWE weaknesses for a TOE, we refine the AVA_VAN.1-3/2-3/3-3/4-3 work units to consider CWE weaknesses for a TOE and arrive at a relevant set of CWE weaknesses.

b) Filter relevant attack patterns.

The initial set of potentially relevant attack patterns identified through the process outlined in 6.1.1 are further filtered according to the following criteria to establish the set of relevant attack patterns for the IT security evaluation.

1) Filter out CAPEC attack patterns whose intent and nature of impact are not relevant to the security sensitivity and critical security properties of the TOE.

NOTE For a given CAPEC attack pattern, the CAPEC schema element of "Attack Motivation-Consequences" indicates the nature of security property violation typically resulting from that attack pattern. The CAPEC schema element of "Purposes" indicates the general purpose (Reconnaissance, Penetration, Exploitation, and Obfuscation) of the attack pattern within the attack lifecycle. The CAPEC schema element of "CIA Impact" indicates the typical level of effect that the attack pattern has on the Confidentiality property, the Integrity property and the Availability property of the TOE. If these characterizations of intent and effect do not directly impact security properties of the TOE deemed to be critical or important, then the corresponding CAPEC attack pattern would not be relevant for a given evaluation and would be filtered out of the set used to identify relevant potential vulnerabilities (CWE weaknesses) for the TOE. Therefore, filtering out these CAPEC attack pattern does not reduce the effectiveness of the AVA_VAN.1.3E action.

2) Filter out CAPEC attack patterns which are not relevant due to measures in the operational environment, either IT or non-IT, preventing effective implementation of the attack pattern in that operational environment. The evaluator should clearly record the specific reasoning involved for each attack pattern excluded.