

FMEA for improving independent testing and vulnerability detection

2008.09.



Korea Testing Laboratory



Part 1. Introduction

Part 2. The requirements of CEM

Part 3. Present state

Part 4. Adoption FEMA

Part 1. Introduction



1.1 Independent testing

1.2 Vulnerability

Part 2. The requirements of CEM

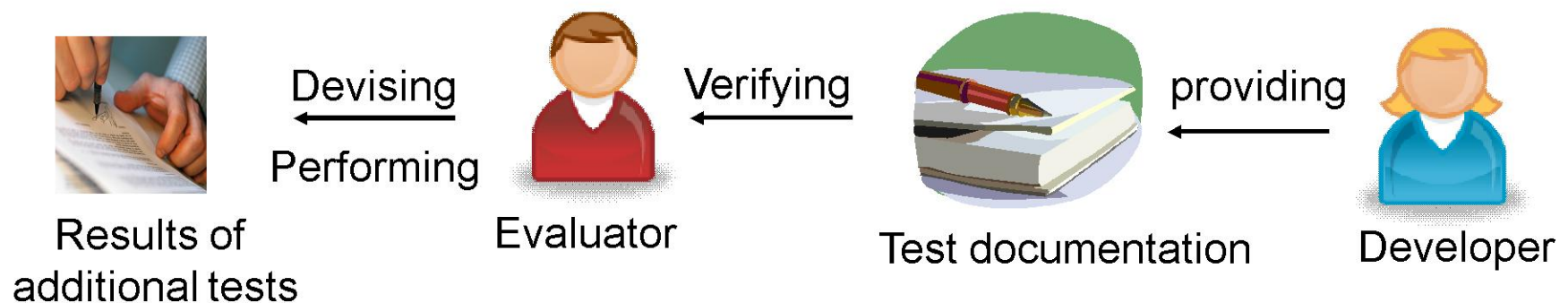
Part 3. Present state

Part 4. Adoption FEMA

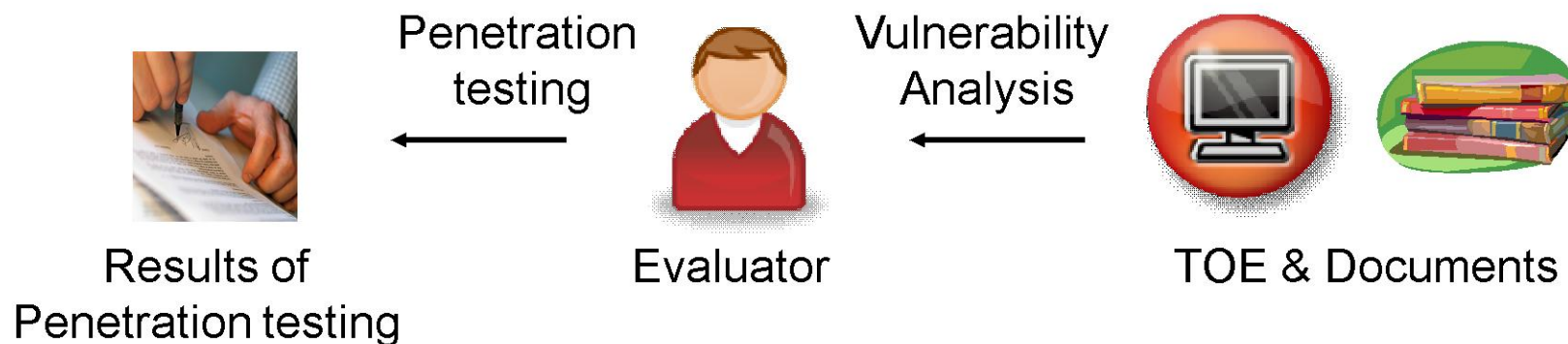
 Independent testing (ATE_IND)

The objectives of this family are built upon the assurances achieved in the ATE_FUN, ATE_COV, and ATE_DPT families by verifying the developer testing and **performing additional tests by the evaluator**.

- From CC Version 3.1



- ➔ **Vulnerability**
A weakness in the TOE that can be used to violate the SFRs in some environment. - From CC Version 3.1
- ➔ **Vulnerability Analysis**
An assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs. - From CC Version 3.1



Part 1. Introduction

Part 2. The requirements of CEM



2.1 The requirements of independent testing

2.2 The requirements of vulnerability analysis

Part 3. Present state

Part 4. Adoption FEMA

ATE_IND.2-6 The evaluator *shall devise* a test subset.

ATE_IND.2-7 The evaluator *shall produce* test documentation for the test subset that is sufficiently detailed to enable the tests to be reproducible.

The evaluator *shall conduct* testing.

AVA_VAN.3-4 The evaluator *shall conduct* a focused search of ST, guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify possible potential vulnerabilities in the TOE.

Annex B. Vulnerability Assessment (AVA)

B.2.2 Identification of Potential Vulnerabilities

B.2.2.2.3 Methodical

The methodical analysis approach takes the form of a **structured examination of the evidence**.

Part 1. Introduction

Part 2. The requirements of CEM

Part 3. Present state and Problems



3.1 Present state

3.2 Problems

Part 4. Adoption FEMA



Independent testing

- An evaluator should perform additional testing referred evaluation evidences
- Evaluation evidences : ST, DEL, ATE etc.
- Test Case generation in accordance with an evaluator's experience or knowledge

Vulnerability Analysis procedure

1) Listing Vulnerabilities

- Known vulnerability lists : Investigated from CVE, Websites of Device development companies and papers

	Site	URL
Known vulnerability	CERT	http://www.cert.org/nav/index_red.html
	ICAT	http://nvd.nist.gov/
	CVE	http://www.cve.mitre.org/cve/
Security Configuration Check lists	NIST	http://csrc.nist.gov/checklists/repository/category.htm
Security recommendation of device development company	SUN	http://sunsolve.sun.com/pub-cgi/show.pl?target=home
	MS	http://www.microsoft.com/security/default.msp
	CISCO	http://www.cisco.com/en/US/products/products_security_advisories_listing.html



Vulnerability Analysis procedure (Cont'd)

- Listing Vulnerabilities derived from pre-evaluated product

- . Referred from evaluation reports

- Listing Vulnerabilities during evaluation

- . Analyzing whether Vulnerability possibility exists in development evaluation reports

- . Performing Vulnerability analysis by recording anticipated vulnerability points in document analysis and functional testing

2) Vulnerability analysis (penetration testing) planning

3) Vulnerability testing

4) Reporting the results of Vulnerability analysis



Consistency absence between evaluators

Insufficiency in a guidelines for vulnerability evaluation

Absence of vulnerability evaluation method



Solution

Introduce a structured examination of the evidence recommended in CEM

→ Adopting FMEA which is enable to make a formal analysis method

Part 1. Introduction

Part 2. The requirements of CEM

Part 3. Present state and Problems

Part 4. Adopting FEMA to CC



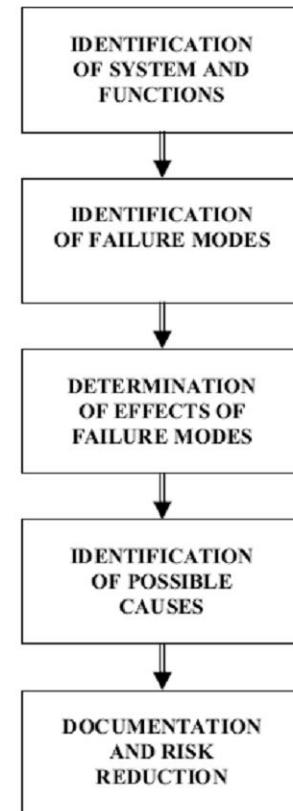
4.1 Overview of FEMA

4.2 Examples

➔ FMEA (Failure Mode and Effect Analysis)

a systematic way of identifying failure modes of a system, item or function, and evaluating the effects of the failure modes on the higher level.

Failure causes are any errors or defects in process, design, or item especially ones that affect the customer, and can be potential or actual. Effects analysis refers to studying the consequences of those failures



Example FMEA Worksheet

Function	Failure mode	Effects	S (severity rating)	Cause(s)	O (occurrence rating)	Current controls	D (detection rating)	CRIT (critical characteristic)	RPN (risk priority number)	Recommended actions	Responsibility and target completion date	Action taken
Fill tub	High pressure sensor never trips	Liquid spills on customer floor	8	Pressure sensor failed Pressure sensor disconnected	2	Fill timeout based on time to fill to low pressure sensor	5	N	80	Perform cost analysis of adding additional sensor halfway between low and high pressure sensors	Jane Doe 10-Oct-2010	



Software FMEA

For software-based systems, the failure modes of software are generally unknown. The software modules do not fail, they only display incorrect behaviour. To find out this incorrect behaviour the safety engineer has to apply his own knowledge about the software to set up an appropriate FMEA approach.

Example of SW-FMEA

Ref-No	Component	Fault	Cause	Failure effect

 Software FMEA for Independent testing

Ref-No	TSF	Fault	Cause	Failure effect	Test case

- TSF : Name of TOE Security Function considered
- Fault : Potential faults that the TSF would have
- Cause : any error or defect arising problems in TSF
- Failure effect : consequences of those failures
- Test case : test methods which need to validate the TSF



Software FMEA for Vulnerability Analysis


Ref-No	Subsystem	vulnerability	Cause	vulnerability effect	Test case

- Subsystem : Individual sub-system that consist of TOE
- Vulnerability : Potential Vulnerability in the subsystem
- Cause : factors arising vulnerabilities
- Vulnerability effect : consequences of those vulnerabilities
- Test case : test methods which need to validate the vulnerabilities



Simple case study – Independent testing

Ref-No	TSF		Fault	Cause	Failure effect	TestCase
Ex-D1	EX_TSF.UAU EX_TSF.UID	Identifi- cation and Authen- tication	Any other protocols can access to TOE not SSL based protocol(HTTPS)	Not implemented	Covert channel failure	TC_D-1
			Event logging failure	Call error from Log-in module (EX_AdminLogin) to Event logging module(EX_LogWriter_event_Log)	Logging failure	TC_D-2
				Module error in EX_LogWriter_event_Log		
			Re-log in even though accessed management exists	Module error in EX_AdminLogin	There are excessive accessed management	TC_D-3
Ex-D2	EX_TSF.AFL	Authen- tication failure	Do not make an alert message if ID/PW is not matched	Module error in EX_AdminLogin	Unauthenticated person can log-in	TC_D-4
			Do not perform Authentication delay if ID/PW is wrong over five times	Module error in EX_AdminLogin	Security function failure	TC_D-5

 Simple case study – Vulnerability Analysis

Ref-No	subsystem	Vulnerability	Cause	Vulnerability effect	TestCase
Ex-V1	Security audit	System stop due to recording excessive audit data	Shortage of storage capacity	Shut down because of TOE error Logging failure of system audit records	TC_P-1
		Loss of audit records			
		System shut down			
Ex-V2	Security management	Unnecessary sevice/open port	Open port in OS	TOE'd being attacked	TC_P-2
Ex-V3	User data protection	Function stop for DoS attacks	Impossibility of providing a normal service due to a system overroad from DoS attack	Service delayed and function stopped	TC_P-3
Ex-V4	Identification and authentication	사전공격	Simple combination of ID/PW generation	Getting management authority	TC_P-4
Ex-V5	Protection of The TSF	Not implemented trusted channels	System information exposed because of not being implemented trusted channels	Getting TSF data	TC_P-5

➡ Advantage of FEMA

Performing independence testing and vulnerability analysis by the structured method using FMEA


Improvement inconsistency between evaluators

Enable to make DB if using FMEA tool

➡ Disadvantage of FEMA

Cost for performing FMEA (time, human resource)

Needed sufficient communication between an evaluator and a developer



Q&A

Thanks for your attention.