



Technical Report

**Methods for Testing and Specification (MTS);
Security Testing;
Case Study Experiences**

ReferenceDTR/MTS-101582 SecTestCase

Keywordsanalysis, security, testing

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2014.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	6
Foreword.....	6
Modal verbs terminology.....	6
1 Scope	7
2 References	7
2.1 Normative references	7
2.2 Informative references.....	7
3 Definitions and abbreviations.....	8
3.1 Definitions.....	8
3.2 Abbreviations	9
4 Overview on case studies	11
5 Banknote processing case study results.....	11
5.1 Case study characterization	11
5.1.1 Background.....	11
5.1.2 System under test.....	13
5.1.3 Security risk assessment	14
5.2 Security testing approaches	15
5.2.1 Detection of vulnerability to injection attacks	15
5.2.1.1 Data Fuzzing with TTCN-3.....	16
5.2.1.2 TTCN-3.....	17
5.2.1.3 Data Fuzzing Library	18
5.2.2 Usage of unusual behaviour sequences.....	19
5.2.2.1 Behavioural fuzzing of UML sequence diagrams	20
5.2.2.2 Online model-based behavioural fuzzing.....	22
5.3 Results	23
5.3.1 Requirements coverage.....	23
5.3.2 Test results	24
5.4 Summary and conclusion	25
6 Banking case study results	25
6.1 Case study characterization	25
6.2 Security testing approaches	26
6.3 Results	29
6.4 Summary and conclusion	32
7 Radio case study results	32
7.1 Case study characterization	32
7.1.1 Context of Mobile ad-hoc networks	32
7.1.2 Status of the test of security testing at the beginning of the project.....	33
7.1.3 Security testing capabilities targeted.....	33
7.1.3.1 Frames analysis	34
7.1.3.2 Data alteration	34
7.1.3.3 Frames replay.....	35
7.1.3.4 Denial of service	36
7.1.3.5 Tampering, malicious code injection	36
7.1.3.6 Combination of threats.....	37
7.1.4 Description of the use-case	37
7.1.4.1 Specific application used as Use Case	38
7.1.4.2 Specific context of the application of security testing tools.....	38
7.1.4.3 Specific context of the initial validation framework	38
7.2 Security testing approaches	38
7.2.1 General principles of the security testing tools integration.....	38
7.2.1.1 Verification framework adaptation	39

7.2.1.2	Adaptation of the event driven simulation environment	39
7.2.2	Properties validated.....	41
7.2.3	Active testing	41
7.3	Results	42
7.4	Summary and conclusion	43
8	Automotive case study results.....	43
8.1	Case study characterization	43
8.2	Security testing approaches	45
8.2.1	Security risk assessment	45
8.2.2	Fuzzing	46
8.2.3	IOSTS-based passive testing approach.....	47
8.2.3.1	Experimentation results.....	48
8.2.3.2	Future works	48
8.2.4	Security monitoring	48
8.2.5	Framework.....	50
8.3	Results	51
8.4	Summary and conclusion	53
9	eHealth case study results.....	54
9.1	Case study characterization	54
9.1.1	Patient consent	55
9.1.2	Device pairing.....	56
9.1.3	New application features	56
9.2	Security testing approaches	56
9.2.1	Formalization.....	56
9.2.1.1	Entity overview	56
9.2.1.2	Environment and sessions	58
9.2.1.3	Messages	58
9.2.1.4	Goals	61
9.2.2	Analysis results using a model checker	63
9.2.3	Technical details	63
9.2.3.1	eHealth web front-end.....	64
9.2.3.2	Device management platform	64
9.2.3.3	Two-factor authentication service	64
9.2.4	Improvements of the security model.....	65
9.2.5	Considered security properties and vulnerabilities	65
9.2.5.1	Security properties	66
9.2.5.2	Vulnerabilities	66
9.3	Results by applying the VERA tool	66
9.3.1	Password brute force.....	66
9.3.2	File enumeration	67
9.3.3	CSRF token checking	68
9.3.4	SQL injection.....	69
9.3.5	XSS injection.....	70
9.3.6	Path traversal attack.....	70
9.3.7	Access control.....	71
9.4	Summary and conclusion	73
10	Document management system case study results.....	74
10.1	Case study characterization	74
10.2	Security testing approaches	74
10.2.1	Security risk assessment of the Infobase application scenario.....	74
10.2.1.1	Background	74
10.2.1.2	Scope and goal of the case study.....	75
10.2.1.3	Method walk-through.....	75
10.2.1.3.1	Describe general usage scenarios	75
10.2.1.3.2	List assets	75
10.2.1.3.3	Define security requirements	75
10.2.1.3.4	Identify relevant threats	75
10.2.1.3.5	Define or derive a Business Worst Case Scenario (BWCS)	76
10.2.1.3.6	Generate Security Overview.....	76
10.2.1.3.7	Map BWCS to Technical Threat Scenario (TTS).....	76

10.2.1.3.8	Map TTSs to test types	77
10.2.1.4	Lessons learned	77
10.2.2	Improvements of the security model – detecting Cross-Site Request Forgery at ASLan++ level	78
10.2.2.1	Description of CSRF in Infobase	78
10.2.2.2	Modeling CSRF in ASLan++	79
10.2.2.2.1	Client	80
10.2.2.2.2	Server	81
10.2.2.2.3	Goal	82
10.2.2.3	Result of the analysis of the Infobase model	82
10.2.3	Mutation-based test generation	83
10.2.4	Test automation	83
10.2.4.1	The ScenTest tool for scenario-based testing	83
10.2.4.2	General approach to test automation of AATs	83
10.2.4.3	Derived test case, test execution and test results	84
10.2.4.3.1	Test scenario 1:	84
10.2.4.3.2	Test scenario 2:	85
10.2.4.3.3	Test Scenario 3:	86
10.3	Results by applying the VERA Tool	87
10.3.1	Considered vulnerabilities	87
10.3.2	Cross-Site Scripting (XSS)	88
10.3.3	SQL injection	89
10.3.4	Password brute-forcing	89
10.3.5	Cross-Site Request Forgery (CSRF)	90
10.3.6	File enumeration	91
10.4	Summary and conclusions	92
11	Evaluation and assessment of case study results	93
11.1	Approach: Security Testing Improvements Profiling (STIP)	93
11.1.1	Security risk assessment	95
11.1.2	Security test identification	95
11.1.3	Automated generation of test models	96
11.1.4	Security test generation	96
11.1.5	Fuzzing	97
11.1.6	Security test execution automation	98
11.1.7	Security passive testing/ security monitoring	98
11.1.8	Static security testing	99
11.1.9	Security test tool integration	99
11.2	Evaluation results: STIP evaluation of the Case Studies	100
11.2.1	Evaluation of the banknote processing machine case study	100
11.2.2	Evaluation of the banking case study	101
11.2.3	Evaluation of the radio protocol case study	102
11.2.4	Evaluation of the automotive case study	103
11.2.5	Evaluation of the eHealth case study	103
11.2.6	Evaluation of the document management case study	104
Annex A:	Bibliography	106
History		107

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://ipr.etsi.org>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Methods for Testing and Specification (MTS).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**may not**", "**need**", "**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 reports on the application of model-based security testing in different industrial domain. Relevant case studies and their results are described in terms of system under test, applied tool chain, together with an overview of the technical requirements. The case studies were conducted as part of ITEA2 DIAMONDS project (<http://www.itea2-diamonds.org/index.html>) and SPaCIoS project (<http://www.spacios.eu/>). The document concentrates on the results and conclusions from this work, giving an insight into how applicable such methods are today for testing and indicating the current strengths and weaknesses.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

2.2 Informative references

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] AVANTSSAR Deliverable 2.3 (update): "ASLan++ specification and tutorial", 2011.

NOTE: Available at <http://www.avantssar.eu>.

[i.2] ITEA2 DIAMONDS Deliverable D5.WP2: "Final Security-Testing Techniques", 2013.

[i.3] ITEA2 DIAMONDS Deliverable D5.WP3: "Final Security Testing Tools", 2013.

[i.4] ITEA2 DIAMONDS Deliverable D5.WP4: "DIAMONDS Security Testing Methodology", 2013.

[i.5] SPaCIoS Deliverable 3.3: "SPaCIoS Methodology and technology for vulnerability-driven security testing", 2013.

[i.6] SPaCIoS Deliverable 5.1: "Proof of Concept and Tool Assessment v.1", 2011.

[i.7] SPaCIoS Deliverable 5.2: "Proof of Concept and Tool Assessment v.2", 2012.

[i.8] SPaCIoS Deliverable 5.4: "Final Tool Assessment", 2013.

[i.9] A. Ulrich, E.-H. Alikacem, H. Hallal, and S. Boroday: From scenarios to test implementations via promela: "Testing Software and Systems", pages 236-249, 2010.

[i.10] J. Oudinet, A. Calvi, and M. Büchler: "Evaluation of ASLan mutation operators". In Proceedings of the 7th International Conference on Tests and Proofs. Springer, June 2013. 20 pages.