AVISPA

www.avispa-project.org

IST-2001-39252

Automated Validation of Internet Security Protocols and Applications

Deliverable D7.2: Assessment of the AVISPA Tool v.1

Abstract

In this document, we report on the assessment of the AVISPA Tool at project month 12. The results of the assessment demonstrate the success of our work in the reporting period. We have been able to formalise in the HLPSL 54 problems from 8 groups, and the AVISPA Tool successfully analyses all the 54 problems in a few minutes. All of the success criteria set out in the Technical Annex (namely coverage, effectiveness, and performance) are therefore largely fulfilled by the tool. Moreover, the tool has been able to detect new (i.e. previously unknown) attacks to some of the protocols analysed. These results give evidence that the project is swiftly advancing the specification and deduction technologies towards the point where industrial-scale, security-sensitive protocols can be specified and automatically analysed.

Deliverable details

Deliverable version: *v1.0*
Person-months required: *1*
Date of delivery: *12.01.2004*
Due on: *31.12.2003*
Classification: *public*
Total pages: *11*

Project details

Start date: *January 1st, 2003*
Duration: *30 months*
Project Coordinator: *Alessandro Armando*
Partners: *Università di Genova, INRIA Lorraine, ETH Zürich, Siemens AG*

Project funded by the European Community under the *Information Society Technologies* Programme (1998-2002)

Contents

1 Introduction

The technical achievements of the AVISPA project are assessed by testing the AVISPA Tool against the library of security problems selected in WP6 [2], which comprises a total of 384 security problems and 79 protocols divided into 33 groups.[1] Assessment points are placed at project months 12, 24, and 30 to check and quantitatively measure the progress. In this document, we report on the assessment of the AVISPA Tool at month 12.

As described in Deliverable 6.1 [2], the following criteria, which refine the ones given in the Technical Annex, are used for the assessment of the AVISPA tool:

Coverage: number and variety of security problems specified in the high-level specification language (HLPSL) and successfully translated in the intermediate format (IF).

Effectiveness: number of security problems that the tool is able to *successfully analyse* by either verifying that the protocol satisfies the desired security property (for scenarios consisting of a bounded number of protocol sessions) or by finding a counterexample demonstrating that the property is violated.

Performance: CPU time spent by the tool to carry out the analysis of the problems on standard commercially available computers.

The project is considered on track at months 12, 24, and 30 if the tool meets the target requirements indicated in Table 1. In particular, a coverage requirement of "P problems from G groups" means that the tool must be able to successfully analyse P security problems drawn from G of the 33 groups given in [2]; an effectiveness requirement of "E problems" means that the tool should successfully analyse at least E of the security problems specified in the HLPSL; finally, the performance requirement is set to 1 hour per problem in all the assessment points.

The project is thus on track at month 12 if the tool meets the following criteria:

Coverage: at least 20 security problems taken from at least 5 of the 33 groups given in [2] should be specifiable in the HLPSL.

Effectiveness: at least 75% (i.e. 15) of the problems specified in the HLPSL should be successfully analysed by the tool.

Performance: the processing of the successfully analysed security problems should take less than 1 hour of CPU time per problem on standard commercially available computers.

The results of the assessment of the AVISPA Tool at month 12 demonstrate the success of our work in the reporting period. As summarised in Table 2, we have been able to formalise in the HLPSL 54 problems from 8 groups, and the AVISPA Tool successfully analyses all the 54 problems in a few minutes. All the above requirements (namely coverage,

[1] We recall that a security problem is given by both a protocol and a security property the protocol should satisfy.

Table 1: Target requirements of assessment points

	Month 12	Month 24	Month 30
Coverage	20 problems from 5 groups	40 problems from 10 groups	80 problems from 20 groups
Effectiveness	15 problems	30 problems	60 problems
Performance	$<$ 1 hour per problem	$<$ 1 hour per problem	$<$ 1 hour per problem

Table 2: Results of the AVISPA Tool for the reporting period

Success criteria at month 12	**Objectives**	**Results**
Coverage	20 problems from 5 groups	54 problems from 8 groups
Effectiveness	15 problems	54 problems
Performance	$<$ 1 hour per problem	all 54 problems in $<$ 8 minutes

effectiveness, and performance) are therefore largely fulfilled by the tool. Moreover, the tool has been able to detect new (i.e. previously unknown) attacks to some of the protocols analysed. These results give evidence that the project is swiftly advancing the specification and deduction technologies towards the point where industrial-scale, security-sensitive protocols can be specified and automatically analysed.

In the following sections we present in detail the coverage (Section 2), effectiveness (Section 3), and the performance (Section 4) of the tool. We conclude with a discussion on the new attacks that our tool has found (Section 5).

2 Coverage

The set of security protocols we have used for the assessment is summarised in Table 3. For each protocol, we indicate the group it belongs to (according to the classification given in [2]), references to the relevant literature where a description of the protocol can be found, and the number of secrecy, weak and strong authentication properties that we have formalised for each protocol. When the number in the last two columns is different from 1, then we refer to the various authentication problems that arise by distinguishing several authentication properties, namely on different data or between different roles, where we split mutual authentication into unilateral authentication properties.

We recall that the coverage requirement set for month 12 asks for the ability to formalise HLPSL-specifications of 20 problems from 5 groups, and automatically translate them into IF-specifications (by means of the HLPSL2IF translator). We have given HLPSL-specifications of 54 problems out of 8 groups and successfully translated all of them into

Table 3: Coverage of the AVISPA Tool v.1

Protocol			Property		
Name	**Group**	**Reference**	**Secrecy**	**W.Auth.**	**S.Auth.**
UMTS-AKA	3GPP	[1]	1	2	
ISO-PK1	ISO	[10]			1
ISO-PK2	ISO	[10]			1
ISO-PK3	ISO	[10]		2	
ISO-PK4	ISO	[10]			2
ChapV2	ppp-wg	[20]	1		2
EKE	network-wg	[5]	1		2
SRP	network-wg	[19]	1		2
EKE2	network-wg	[4]	1		2
SPEKE	network-wg	[12]	1		2
AAAMobileIP	mobileip-wg	[6]	1	6	
IKEv2-CHILD	ipsec	[13]	1		2
IKEv2-DS	ipsec	[13]	1		2
IKEv2-DSx	ipsec	[13]	1		2
IKEv2-MAC	ipsec	[13]	1		2
IKEv2-MACx	ipsec	[13]	1		2
TLS	TLS	[7]	1		2
KerberosV	kerberos-wg	[14, 18]	1	4	
Total			14	14	26

the IF. Therefore, the AVISPA Tool has largely fulfilled the coverage requirement.

3 Effectiveness

We recall that the back-ends integrated into the AVISPA Tool are:

OFMC, the on-the-fly model-checker developed and maintained by ETHZ,

CL-atse, the protocol analyser based on Constraint Logic developed and maintained by INRIA, and

SATMC, the SAT-based model-checker developed and maintained by UNIGE.

Note that the IF specifications that we consider are equipped with a signature section describing the type of the messages exchanged among the participating agents. This section may be neglected by the back-ends in order to search for type-flaw attacks; when this is the case, we say that the back-end considers the *untyped model* of the security problem. If

Table 4: Effectiveness of the AVISPA Tool v.1, part I

Problem	**Attack**	**OFMC**	**CL-atse**	**SATMC (Enc/Sol)**
UMTS-AKA - secrecy	NO	1.50	†	0.03/0.00
UMTS-AKA - w.auth. 1	NO	1.41	†	0.20/0.00
UMTS-AKA - w.auth. 2	NO	1.42	0.01	0.04/0.00
ISO-PK1 - s.auth.	YES	0.01	0.01	0.02/0.00
ISO-PK2 - s.auth.	NO	0.07	Y 0.00	2.32/0.03
ISO-PK3 - w.auth. 1	YES	0.04	†	0.02/0.00
ISO-PK3 - w.auth. 2	YES	0.05	†	0.24/0.00
ISO-PK4 - s.auth. 1	NO	0.25	0.01	13.06/0.09
ISO-PK4 - s.auth. 2	NO	0.25	Y 0.01	13.00/0.12
ChapV2 - secrecy	NO	0.31	0.01	0.28/0.03
ChapV2 - s.auth. 1	NO	0.31	0.00	0.31/0.04
ChapV2 - s.auth. 2	NO	0.31	0.01	0.25/0.00
EKE - secrecy	NO	0.25	0.02	0.02/0.00
EKE - s.auth. 1	YES	0.07	0.01	0.05/0.00
EKE - s.auth. 2	YES	0.11	0.01	0.09/0.00
SRP - secrecy	NO	6.27	-	-
SRP - s.auth. 1	NO	5.95	-	-
SRP - s.auth. 2	NO	5.98	-	-
EKE2 - secrecy	NO	0.19	-	-
EKE2 - s.auth. 1	NO	0.18	-	-
EKE2 - s.auth. 2	NO	0.15	-	-
SPEKE - secrecy	NO	0.73	-	-
SPEKE - s.auth. 1	NO	0.67	-	-
SPEKE - s.auth. 2	NO	0.67	-	-

Legenda:

YES	:	a known attack on the typed model has been found;
NO	:	no attack has been found;
YES	:	a new attack on the typed model has been found;
Y	:	a new attack on the untyped model has been found;
-	:	special properties of cryptographic operators are not supported;
†	:	the analysis is inconclusive;
MO	:	memory out has been reached.

Table 5: Effectiveness of the AVISPA Tool v.1, part II

Problem	**Attack**	**OFMC**	**CL-atse**	**SATMC (Enc/Sol)**
AAAMobileIP - secrecy	NO	0.29	0.01	260.49/0.00
AAAMobileIP - w.auth. 1	NO	0.30	0.02	260.63/0.00
AAAMobileIP - w.auth. 2	NO	0.29	0.01	261.77/0.00
AAAMobileIP - w.auth. 3	NO	0.30	0.01	260.96/0.00
AAAMobileIP - w.auth. 4	NO	0.31	0.02	259.51/0.00
AAAMobileIP - w.auth. 5	NO	0.32	†	261.29/0.00
AAAMobileIP - w.auth. 6	NO	0.31	†	261.46/0.00
IKEv2-CHILD - secrecy	NO	0.67	-	-
IKEv2-CHILD - s.auth. 1	NO	0.68	-	-
IKEv2-CHILD - s.auth. 2	NO	0.66	-	-
IKEv2-DS - secrecy	NO	16.32	-	-
IKEv2-DS - s.auth. 1	NO	16.23	-	-
IKEv2-DS - s.auth. 2	YES	0.25	-	-
IKEv2-DSx - secrecy	NO	60.27	-	-
IKEv2-DSx - s.auth. 1	NO	60.07	-	-
IKEv2-DSx - s.auth. 2	NO	60.08	-	-
IKEv2-MAC - secrecy	NO	14.58	-	-
IKEv2-MAC - s.auth. 1	NO	14.49	-	-
IKEv2-MAC - s.auth. 2	NO	14.72	-	-
IKEv2-MACx - secrecy	NO	43.43	-	-
IKEv2-MACx - s.auth. 1	NO	43.28	-	-
IKEv2-MACx - s.auth. 2	NO	42.92	-	-
TLS - secrecy	NO	0.42	0.01	931.87/0.00
TLS - s.auth. 1	NO	0.42	0.01	MO
TLS - s.auth. 2	NO	0.40	0.02	MO
KerberosV - secrecy	NO	1.40	0.31	MO
KerberosV - w.auth. 1	NO	1.27	†	MO
KerberosV - w.auth. 2	NO	1.29	†	MO
KerberosV - w.auth. 3	NO	1.30	0.36	MO
KerberosV - w.auth. 4	NO	1.28	0.30	MO

Legenda:

YES	:	a known attack on the typed model has been found;
NO	:	no attack has been found;
YES	:	a new attack on the typed model has been found;
Y	:	a new attack on the untyped model has been found;
-	:	special properties of cryptographic operators are not supported;
†	:	the analysis is inconclusive;
MO	:	memory out has been reached.

the signature section is taken into account, then type-flaw attacks are excluded from the analysis, and we say that the back-end considers the *typed model* of the security problem. It is fundamental that both models are considered during analysis as, on the one hand, it is important to be able to detect all possible attacks, but on the other hand many type-flaw attacks are of little practical significance as actual implementations of security protocols often enforce simple mechanisms that exclude their applicability (see, for instance, [9]). Both OFMC and SATMC carry out the analysis with respect to the typed model, whereas CL-atse adopts the untyped model. The AVISPA Tool can thus analyse protocols by considering both models.

By running the back-ends of the AVISPA Tool against all the 54 problems associated with the IF specifications automatically generated by the HLPSL2IF translator incorporated in the AVISPA Tool (cf. Section 2), we have obtained the results listed in Table 4 and Table 5. For each problem we report whether an attack is found (YES) or not (NO) by considering the typed model (see the column "Attack") and the time in seconds spent by each back-end to analyse the problem (columns "OFMC", "CL-atse", and "SATMC").[2] A "-" means that the back-end cannot deal with some special properties of cryptographic operators such as exponentiation, and hence that the problem cannot be properly analysed by the back-end.[3] "MO" means that more than 1GB of memory was necessary to analyse the problem and therefore that a "memory-out" occurred. Boxed "YES" and "Y" mean that the AVISPA Tool has detected a previously unknown attack in the typed and untyped models, respectively. Finally, "†" means that the analysis conducted by the back-end is inconclusive. This is the case for the CL-atse back-end which, being not yet able to check negations in goals, can return inconclusive answers when an attack trace is found on either a secrecy or a weak authentication property. More specifically, if CL-atse does not find any attack, then it can positively conclude that the problem analysed satisfies the property checked. If CL-atse finds an attack, then it is sure that it is not a spurious counterexample if, and only if, it is checking for violations against strong authentication.

For SATMC, both the time spent by the back-end to generate the SAT formula ("Enc") and that spent by the SAT-solver[4] to solve the formula ("Sol") are reported. It must be noted that SATMC performs a bounded analysis of the problems by unfolding the transition relation up to 10 times. A negative answer therefore means that no attack has been found by SATMC for the given bound.

Since OFMC alone successfully analyses all the 54 problems, also the effectiveness requirement is achieved by the AVISPA Tool v.1.

[2] Timings are obtained by each single back-end with a resource limit of 1 hour CPU time and 1GB memory, on a Pentium IV 2.4GHz under Linux.

[3] Note that the handling of special properties of cryptographic operators is planned for the second year of the project.

[4] We used the Chaff solver [17] for these experiments.

4 Performance

Note that, since the time required by the AVISPA Tool for compiling from the HLPSL into the IF language is always negligible (a few milliseconds), we do not report it in Table 4 and Table 5.

OFMC analyses *all 54 problems* in less than 8 minutes of CPU time. This is less than the 1 hour limit set by the performance requirement *for a single problem* and therefore also this requirement is successfully met by the AVISPA Tool v.1. Notice that on all the problems for which CL-atse is successful it is also very fast, and it is actually faster than OFMC. As far as SATMC is concerned, it is interesting to observe that the time spent to generate the SAT formula largely dominates that spent by the SAT-solver, and that the latter is negligible in most cases.

5 New Attacks

The experimental analysis demonstrates that the AVISPA Tool meets all the success criteria at month 12. Moreover, besides for some attacks that were already known (for instance, the weak authentication attack on the ISO-PK1 protocol [8], also known as "ISO Public Key One-Pass Unilateral Authentication Protocol"), the AVISPA Tool also finds some new attacks which we now briefly discuss.

The AVISPA Tool finds a new attack on the ISO-PK3 (also known as "ISO Public Key Two-Pass Mutual Authentication") protocol [10]. It was already known that ISO-PK3 is vulnerable to replay attacks and hence it does not provide strong authentication [8]: nothing in the messages ensures the freshness of the messages for the responder role. The analysis with the AVISPA Tool, however, shows that the ISO-PK3 protocol does not even guarantee weak authentication, i.e. after successfully executing the protocol, neither the initiator nor the responder can be sure about the authenticity of the exchanged messages.

The man-in-the-middle attack discovered by the OFMC back-end on the IKEv2-DS protocol [13] is new, though it is similar to a well-known attack on the Station-2-Station protocol [15]. As pointed out in [16], several protocols that were inspired by Station-2-Station (e.g. also the first version of IKE) exhibit the same vulnerability. Also, as described in both [15] and [16], the attack is not very relevant, since the intruder can confuse agents about whom they are talking to, but he cannot find out the key negotiated in such a run. We were able to formally express what it means that these attacks are "not relevant". More precisely, IKEv2 (and, similarly, the other similar protocols) does provide strong authentication when not viewing the key-negotiation in isolation but in relation with the usage of the key. We have checked this with OFMC for several finite scenarios.[5]

[5]It is also important to note that the ETHZ and Siemens partners have applied OFMC to analyse the H.530 protocol of the ITU [11], a protocol developed by Siemens to provide mutual authentication and key agreement in mobile roaming scenarios in multimedia communication. As discussed in detail in [3], OFMC takes only 1.6 seconds to detect a previously unknown attack to H.530. The weakness is serious enough that Siemens has changed the protocol accordingly, and Sebastian Mödersheim of ETHZ participated in

Finally, two new attacks relying on type confusion are detected by the CL-atse back-end as violations of the strong authentication property on the ISO-PK2 and ISO-PK4 protocols (also known as "ISO Public Key Two-Pass Unilateral Authentication Protocol" and "ISO Public Key Three-Pass Mutual Authentication Protocol", respectively). In both these attacks, a message sent by the authenticated principal is received verbatim by the authenticator, but they do not agree on the values of the nonces appearing in the message. However, further enquiries are needed to decide whether these flaws are artificial or can be mounted against actual implementations of the protocol.

the new patent that was recently submitted.

References

[1] J. Arkko and H. Haverinen. EAP AKA Authentication, Oct. 2003. Work in Progress.

[2] AVISPA. Deliverable 6.1: List of selected problems. Available at `http://www.avispa-project.org`, 2003.

[3] D. Basin, S. Mödersheim, and L. Viganò. An On-The-Fly Model-Checker for Security Protocol Analysis. In E. Snekkenes and D. Gollmann, editors, *Proceedings of ESORICS'03*, LNCS 2808, pages 253–270. Springer-Verlag, 2003. Available at `http://www.avispa-project.org`.

[4] M. Bellare, D. Pointcheval, and P. Rogaway. Authenticated key exchange secure against dictionary attacks. In *Proceedings of Eurocrypt 2000*, LNCS 1807. Springer-Verlag, 2000.

[5] S. Bellovin and M. Merritt. Encrypted Key Exchange: Password-based protocols secure against dictionary attacks. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, May 1992.

[6] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko. RFC 3588: Diameter Base Protocol, Sept. 2003. Status: Proposed Standard.

[7] T. Dierks and C. Allen. RFC 2246: The TLS Protocol Version 1.0, Jan. 1999. Status: Proposed Standard.

[8] B. Donovan, P. Norris, and G. Lowe. Analyzing a Library of Security Protocols using Casper and FDR. In *Proceedings of the Workshop on Formal Methods and Security Protocols*, 1999.

[9] J. Heather, G. Lowe, and S. Schneider. How to prevent type flaw attacks on security protocols. In *Proceedings of The 13th Computer Security Foundations Workshop (CSFW'00)*. IEEE Computer Society Press, 2000.

[10] ISO/IEC. ISO/IEC 9798-3: Information technology - Security techniques - Entity authentication - Part 3: Mechanisms using digital signature techniques, 1997.

[11] ITU-T Recommendation H.530: Symmetric Security Procedures for H.510 (Mobility for H.323 Multimedia Systems and Services), 2002.

[12] D. P. Jablon. Strong password-only authenticated key exchange. *Computer Communication Review*, 26(5):5–26, 1996.

[13] C. Kaufman. Internet Key Exchange (IKEv2) Protocol, Oct. 2003. Work in Progress.

[14] J. Kohl and C. Neuman. RFC 1510: The Kerberos Network Authentication Service (V5), Sept. 1993. Status: Proposed Standard.

[15] G. Lowe. Some new attacks upon security protocols. In *Proceedings of The 9th Computer Security Foundations Workshop (CSFW'96)*. IEEE Computer Society Press, 1996.

[16] C. Meadows. Analysis of the Internet Key Exchange Protocol Using the NRL Protocol Analyzer. In *Proceedings of the 1999 IEEE Symposium on Security and Privacy*. IEEE Computer Society Press, 1999.

[17] M. W. Moskewicz, C. F. Madigan, Y. Zhao, L. Zhang, and S. Malik. Chaff: Engineering an Efficient SAT Solver. In *Proceedings of the 38th Design Automation Conference (DAC'01)*, 2001.

[18] C. Neuman. The Kerberos Network Authentication Service (V5), June 2003. Work in Progress.

[19] T. Wu. RFC 2945: The SRP Authentication and Key Exchange System, Sept. 2000. Status: Proposed Standard.

[20] G. Zorn. RFC 2759: Microsoft PPP CHAP Extensions, Version 2, Jan. 2000. Status: Informational.