www.avispa-project.org

IST-2001-39252

Automated Validation of Internet Security Protocols and Applications

Deliverable D7.3: Assessment of the AVISPA Tool v.2

Abstract

In this document, we report on the assessment of the AVISPA Tool at project month 24. The results of the assessment demonstrate the achievement of the project's objectives for the reporting period. We have been able to formalise in the HLPSL 112 problems from 14 groups, and the AVISPA Tool v.2 successfully analyses 110 problems in less than 25 minutes of CPU time per problem (globally, the whole library of 110 problems requires 69 minutes to be analysed). All of the success criteria set out in the Technical Annex (namely coverage, effectiveness, and performance) are therefore largely fulfilled by the AVISPA Tool v.2. Moreover, the tool is able to detect the same new (i.e. previously unknown in literature) attacks discovered by the AVISPA Tool v.1 and with better performance.

Deliverable details

Deliverable version: *v1.0*
Person-months required: *5*
Date of delivery: *18.02.2005*
Due on: *31.12.2004*
Classification: *public*
Total pages: *19*

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 v.2 against the library of security problems selected in WP6 [3], which comprises a total of 384 security problems and 79 protocols divided into 33 groups.[1]

As described in Deliverable 6.1 [3], 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 under the analysed scenario 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 Deliverable 6.1 [3]; 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.

Thus, the project is on track at month 24 if the tool meets the following criteria:

Coverage: at least 40 security problems taken from at least 10 of the 33 groups given in [3] should be specifiable in the HLPSL.

Effectiveness: at least 75% (i.e. 30) 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 v.2 are given in Table 2. We have been able to formalise in the HLPSL 112 problems from 14 groups, and the tool successfully analyses 110 problems in less than 25 minutes of CPU time per problem (globally, the entire library of 110 problems requires 69 minutes of CPU time to be analysed). Only on 2 of the 112 problems, the time granted (i.e. 1 hour) to the AVISPA Tool v.2 is not

[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 24	**Objectives**	**Results**
Coverage	40 problems from 10 groups	112 problems from 14 groups
Effectiveness	30 problems	110 problems
Performance	$<$ 1 hour per problem	$<$ 25 minutes per problem (all 110 problems in 69 minutes)

sufficient for the analyses (the dimension of the search space associated to these problems is huge) and a time-out is returned. Therefore, all the above requirements (namely coverage, effectiveness, and performance) are largely fulfilled by the AVISPA Tool v.2. Moreover, the tool is able to detect the same new (i.e. previously unknown in literature) attacks discovered by the AVISPA Tool v.1 (see Deliverable 7.2 [4]) with better performance. Besides this, it is worth pointing out that a new back-end, called TA4SP, has been recently integrated into the AVISPA Tool v.2. TA4SP verifies the input protocol with respect to secrecy by considering an *unbounded number of protocol sessions*. This enhances considerably the "spectrum" of the AVISPA Tool v.2 that from being particularly efficient at finding flaws in a bounded number of sessions (falsification-based approach), it becomes also able to prove the correctness of protocols in an unbounded number of sessions (verification-based approach).

In the following sections we present in detail the results of the experimental evaluation of the coverage (Section 2), effectiveness (Section 3), and the performance (Section 4) of the tool. We conclude with a discussion on the new attacks found by the AVISPA Tool (Section 5).

2 Coverage

The set of security protocols 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 De-

Table 3: Coverage of the AVISPA Tool v.2

Protocol			Property		
Name	**Group**	**Reference**	**Secrecy**	**W.Auth.**	**S.Auth.**
UMTS-AKA	3GPP	[2]	1	2	
ISO-PK1	ISO	[19]			1
ISO-PK2	ISO	[19]			1
ISO-PK3	ISO	[19]		2	
ISO-PK4	ISO	[19]			2
ChapV2	ppp-wg	[33]	1		2
EKE	PAKE	[8]	1		2
SRP	PAKE	[32]	1		2
EKE2	PAKE	[7]	1		2
SPEKE	PAKE	[23]	1		2
AAAMobileIP	mobileip-wg	[11]	1	6	
IKEv2-CHILD	ipsec	[24]	1		2
IKEv2-DS	ipsec	[24]	1		2
IKEv2-DSx	ipsec	[24]	1		2
IKEv2-MAC	ipsec	[24]	1		2
IKEv2-MACx	ipsec	[24]	1		2
TLS	TLS	[13]	1		2
LPD-MSR	LPD	[9]	1	1	
LPD-IMSR	LPD	[9]	1	1	
Kerb-basic	krb-wg	[30]	1	7	
Kerb-Cross-Realm	krb-wg	[30]	1	2	5
Kerb-Ticket-Cache	krb-wg	[30]	1	1	4
Kerb-Forwardable	krb-wg	[30]	1	1	4
Kerb-PreAuth	krb-wg	[17]	1	2	4
Kerb-PKINIT	krb-wg	[31]	1	2	4
CRAM-MD5	challenge-response	[25]	1		1
PBK	ipv6	[10]			1
PBK-fixed	ipv6	[10]			1
PBK-fix-weak-auth	ipv6	[10]		1	
DHCP-delayed-auth	DHC	[15]	1		1
h.530	H323 Suite	[20, 22]	1		2
h.530-fix	H323 Suite	[20, 22]	1		2
lipkey-spkm-known-initiator	CAT	[1, 16]	1		1
lipkey-spkm-unknown-initiator	CAT	[1, 16]	1		1
		Total	27	28	57
		Grand total	112		

liverable 6.1 [3]),[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 the 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 24 asks for the ability to formalise HLPSL-specifications of 40 problems from 10 groups, and automatically translate them into IF-specifications (by means of the HLPSL2IF translator). We have specified in HLPSL 112 problems from 14 groups. The AVISPA Tool v.2 successfully translated all these 112 problems in IF via the HLPSL2IF translator. Therefore, the AVISPA Tool v.2 largely fullfills the coverage requirement.

3 Effectiveness

We recall that the back-ends integrated into the AVISPA Tool v.2 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,

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

TA4SP, tree automata-based automatic tool developed and maintained by the CASSIS group at INRIA.

The last one has been recently incorporated into the AVISPA Tool v.2. TA4SP (Tree Automata based automatic approximations for the analysis of Security Protocols) is a protocol analyser that computes approximations of the intruder knowledge by using regular tree languages and rewriting. In more details TA4SP analyses the input protocol with respect to secrecy by considering an unbounded number of protocol sessions played by two agents [12].[3] The introduction of TA4SP enhances significantly the "spectrum" of the AVISPA Tool v.2. In fact, while the others back-ends of the AVISPA Tool v.2 are particularly efficient at finding flaws in a *bounded number of sessions* (falsification-based approach), TA4SP attempts to prove the correctness of protocols in an *unbounded number of sessions* (verification-based approach).

Note that the IF specifications 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

[2] Notice that "PAKE" is an acronym for the "Password-Authenticated Key Exchange" group.

[3] This abstraction currently requires a number of minor modifications to the IF specifications generated by the HLPSL2IF translator. These modifications are currently carried out manually, but we expect this step will be automated by the end of the project.

the case, we say that the back-end considers the *untyped model* of the security problem. If 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, [18]). All the four back-ends are able to carry out the analysis with respect to the typed model, whereas CL-AtSe and OFMC are also able to adopt the untyped model. The AVISPA Tool can thus analyse protocols by considering both models.

We have run the AVISPA Tool v.2 against three classes of problems modelling a typed scenario with a bounded number of protocol sessions (denoted by TY&B), an untyped scenario with a bounded number of protocol sessions (denoted by UNTY&B), and a typed scenario with an unbounded number of protocol sessions (denoted by TY&UNB).[4]

By running the back-ends of the AVISPA Tool v.2 against all the 112 problems under the TY&B and UNTY&B scenarios, we obtained the results listed in Table 4, Table 5, and Table 6, and those reported in Table 8, Table 9, and Table 10, respectively.[5] For each problem, we report whether an attack is found (YES) or not (NO) (see the column "Attack")[6] and the time in seconds spent by each back-end to analyse the problem (columns "OFMC", "CL-AtSe", and "SATMC").[7] A boxed "YES" denotes that the AVISPA Tool v.2 has found a new (previously unknown in literature) attack under the typed model. 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. "MO" means that a "memory-out" has been reached, and "TO" indicates that a "time-out" occurred. When using the untyped model (see Tables 8, 9, and 10), CL-AtSe uses the associativity property of pairing, while OFMC does not. This explains why CL-AtSe finds attacks on problems for which OFMC does not find any. A "Y" next to the time spent by CL-AtSe indicates when this is the case. In this context it must be said that the majority of these attacks are not of practical significance, since they can be easily prevented in actual implementations (in fact, the length of each message field is usually known in advance and can be simply checked). Nevertheless, there are situations in which these attacks are indeed meaningful, e.g. when the protocol is implemented in low-powered devices that do not have enough resources to perform the above checks.

[4]Notice that, while we thoroughly assessed the AVISPA Tool on TY&B and UNTY&B, experimentation with TY&UNB has started recently and therefore the results in this case are still preliminary. More will be reported on this in the final assessment.

[5]Results 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.

[6]It must be noted that a NO indicates that the AVISPA Tool v.2 has been able to establish that the protocol satisfies the security property under the analysed scenario.

[7]For SATMC, both the time spent by the back-end to generate the SAT formula ("Enc") and that spent by the SAT-solver—we used the Chaff solver [29] for these experiments—to solve the formula ("Sol") are reported.

Table 4: Effectiveness of the AVISPA Tool v.2 on the TY&B scenario, part I

Problem	**Attack**	**OFMC**	**CL-atse**	**SATMC (Enc/Sol)**
UMTS_AKA-secrecy	NO	0.00	0.00	0.02 /0.00
UMTS_AKA-wauth-1	NO	0.01	0.00	0.04 /0.00
UMTS_AKA-wauth-2	NO	0.01	0.01	0.05 /0.00
AAAMobileIP-secrecy	NO	0.12	0.02	0.10 /0.00
AAAMobileIP-wauth-1	NO	0.09	0.01	0.20 /0.00
AAAMobileIP-wauth-2	NO	0.11	0.02	0.22 /0.00
AAAMobileIP-wauth-3	NO	0.12	0.02	0.18 /0.01
AAAMobileIP-wauth-4	NO	0.11	0.02	0.22 /0.00
AAAMobileIP-wauth-5	NO	0.10	0.05	0.18 /0.00
AAAMobileIP-wauth-6	NO	0.10	0.06	0.22 /0.00
ISO1-auth-1	YES	0.02	0.00	0.05 /0.00
ISO2-auth-1	NO	0.05	0.00	1.62 /0.00
ISO3-wauth-1	YES	0.02	0.01	0.05 /0.00
ISO3-wauth-2	YES	0.02	0.00	0.22 /0.00
ISO4-auth-1	NO	0.27	0.02	579.37 /0.60
ISO4-auth-2	NO	0.27	0.01	573.14 /0.56
LPD-MSR-secrecy	YES	0.01	0.01	0.04 /0.01
LPD-MSR-wauth-1	YES	0.01	0.01	0.13 /0.01
LPD-IMSR-secrecy	NO	0.04	0.01	0.21 /0.00
LPD-IMSR-wauth-1	NO	0.04	0.00	0.22 /0.01
CHAPv2-auth-1	NO	0.11	0.01	0.20 /0.00
CHAPv2-auth-2	NO	0.09	0.00	0.17 /0.00
CHAPv2-secrecy	NO	0.12	0.00	0.18 /0.00
EKE-auth-1	YES	0.04	0.01	0.07 /0.00
EKE-auth-2	YES	0.05	0.01	0.12 /0.00
EKE-secrecy	NO	0.10	0.02	0.03 /0.00
TLS-auth-1	NO	0.73	0.09	TO
TLS-auth-2	NO	0.72	0.06	TO
TLS-secrecy	NO	0.75	0.17	TO
DHCP-delayed-auth-auth-1	NO	0.03	0.00	0.15 /0.00
DHCP-delayed-auth-secrecy	NO	0.04	0.00	0.04 /0.00

Legenda:

YES	:	a known attack has been found
NO	:	the protocol is safe under the analysed scenario
YES	:	a new attack has been found
TO	:	time-out

Table 5: Effectiveness of the AVISPA Tool v.2 on the TY&B scenario, part II

Problem	**Attack**	**OFMC**	**CL-atse**	**SATMC (Enc/Sol)**
Kerb-Cross-Realm-auth-1	NO	1.47	0.51	14.00 /0.17
Kerb-Cross-Realm-auth-2	NO	1.46	0.49	13.89 /0.20
Kerb-Cross-Realm-auth-3	NO	1.44	0.51	14.02 /0.17
Kerb-Cross-Realm-auth-4	NO	1.47	0.61	14.06 /0.16
Kerb-Cross-Realm-auth-5	NO	1.44	0.50	13.89 /0.18
Kerb-Cross-Realm-secrecy	NO	1.67	0.52	15.58 /0.42
Kerb-Cross-Realm-wauth-1	NO	1.44	0.50	14.05 /0.20
Kerb-Cross-Realm-wauth-2	NO	1.47	0.50	14.11 /0.19
Kerb-Ticket-Cache-auth-1	NO	0.40	0.06	79.84 /1.02
Kerb-Ticket-Cache-auth-2	NO	0.41	0.06	82.36 /0.89
Kerb-Ticket-Cache-auth-3	NO	0.40	0.07	79.23 /0.85
Kerb-Ticket-Cache-auth-4	NO	0.39	0.06	82.97 /0.93
Kerb-Ticket-Cache-secrecy	NO	0.44	0.07	88.48 /3.04
Kerb-Ticket-Cache-wauth-1	NO	0.39	0.06	82.78 /1.02
Kerb-basic-secrecy	NO	0.43	0.06	20.53 /0.41
Kerb-basic-wauth-1	NO	0.39	0.04	18.99 /0.73
Kerb-basic-wauth-2	NO	0.38	0.05	18.80 /0.73
Kerb-basic-wauth-3	NO	0.41	0.05	18.88 /0.36
Kerb-basic-wauth-4	NO	0.37	0.06	18.88 /0.36
Kerb-basic-wauth-5	NO	0.35	0.06	18.55 /0.17
Kerb-basic-wauth-6	NO	0.37	0.06	18.48 /0.19
Kerb-basic-wauth-7	NO	0.38	0.04	6.45 /0.00
Kerb-Forwardable-auth-1	NO	4.99	1.69	TO
Kerb-Forwardable-auth-2	NO	5.00	1.70	TO
Kerb-Forwardable-auth-3	NO	5.00	2.36	TO
Kerb-Forwardable-auth-4	NO	4.94	1.70	TO
Kerb-Forwardable-secrecy	NO	5.48	1.73	TO
Kerb-Forwardable-wauth-1	NO	4.93	1.71	TO
Kerb-PKINIT-auth-1	NO	0.60	0.09	101.26 /1.28
Kerb-PKINIT-auth-2	NO	0.61	0.08	94.95 /1.10
Kerb-PKINIT-auth-3	NO	0.63	0.10	100.57 /1.09
Kerb-PKINIT-auth-4	NO	0.62	0.07	34.14 /0.00
Kerb-PKINIT-secrecy	NO	0.69	0.09	105.93 /5.46
Kerb-PKINIT-wauth-1	NO	0.63	0.09	100.62 /1.26
Kerb-PKINIT-wauth-2	NO	0.63	0.12	102.86 /1.46

Legenda:

NO : the protocol is safe under the analysed scenario

TO : time-out

Table 6: Effectiveness of the AVISPA Tool v.2 on the TY&B scenario, part III

Problem	**Attack**	**OFMC**	**CL-atse**	**SATMC** (**Enc**/**Sol**)
Kerb-preauth-auth-1	NO	0.27	0.08	55.02 /0.31
Kerb-preauth-auth-2	NO	0.26	0.08	56.24 /0.32
Kerb-preauth-auth-3	NO	0.26	0.10	54.01 /0.26
Kerb-preauth-auth-4	NO	0.25	0.08	55.05 /0.33
Kerb-preauth-secrecy	NO	0.29	0.08	53.89 /0.64
Kerb-preauth-wauth-1	NO	0.27	0.08	50.54 /0.33
Kerb-preauth-wauth-2	NO	0.26	0.12	48.97 /0.38
CRAM-MD5-auth-1	NO	0.36	0.73	0.33 /0.00
CRAM-MD5-secrecy	NO	0.35	0.01	0.07 /0.00
PBK-auth-1	YES	0.25	0.01	0.34 /0.02
PBK-fix-weak-auth-wauth-1	NO	2.02	22.03	0.43 /0.01
PBK-fix-auth-1	YES	0.10	0.01	0.08 /0.00
SRP_siemens-auth-1	NO	0.88	-	-
SRP_siemens-auth-2	NO	0.91	-	-
SRP_siemens-secrecy	NO	1.07	-	-
EKE2-auth-1	NO	0.06	-	-
EKE2-auth-2	NO	0.05	-	-
EKE2-secrecy	NO	0.05	-	-
SPEKE-auth-1	NO	1.02	-	-
SPEKE-auth-2	NO	1.00	-	-
SPEKE-secrecy	NO	1.09	-	-
IKEv2-CHILD-auth-1	NO	0.39	-	-
IKEv2-CHILD-auth-2	NO	0.40	-	-
IKEv2-CHILD-secrecy	NO	0.40	-	-
IKEv2-DS-auth-1	NO	2.58	-	-
IKEv2-DS-auth-2	YES	0.08	-	-
IKEv2-DS-secrecy	NO	2.56	-	-
IKEv2-DSx-auth-1	NO	14.00	-	-
IKEv2-DSx-auth-2	NO	14.23	-	-
IKEv2-DSx-secrecy	NO	14.33	-	-
IKEv2-MAC-auth-1	NO	2.66	-	-
IKEv2-MAC-auth-2	NO	2.67	-	-
IKEv2-MAC-secrecy	NO	2.70	-	-

Legenda:

YES	:	a known attack has been found
NO	:	the protocol is safe under the analysed scenario
YES	:	a new attack has been found
-	:	special properties of cryptographic operators are not supported

Table 7: Effectiveness of the AVISPA Tool v.2 on the TY&B scenario, part IV

Problem	**Attack**	**OFMC**	**CL-atse**	**SATMC (Enc/Sol)**
IKEv2-MACx-auth-1	NO	13.36	-	-
IKEv2-MACx-auth-2	NO	13.50	-	-
IKEv2-MACx-secrecy	NO	13.68	-	-
h.530-auth-1	TO	TO	-	-
h.530-auth-2	YES	0.64	-	-
h.530-secrecy	TO	TO	-	-
h.530-fix-auth-1	NO	1,420.06	-	-
h.530-fix-auth-2	NO	1,435.07	-	-
h.530-fix-secrecy	NO	1,422.41	-	-
lipkey-spkm-known-initiator-auth-1	NO	0.12	-	-
lipkey-spkm-known-initiator-secrecy	NO	0.11	-	-
lipkey-spkm-unknown-initiator-auth-1	NO	3.43	-	-
lipkey-spkm-unknown-initiator-secrecy	NO	3.90	-	-

Legenda:

NO : the protocol is safe under the analysed scenario
YES : a new attack has been found
\- : special properties of cryptographic operators are not supported
TO : time-out

It is immediate to see that on both the TY&B and UNTY&B scenarios the AVISPA Tool v.2 is very effective: it is able to successfully analyse 110 of the 112 problems specified in HLPSL. On only 2 problems, the time granted to the AVISPA Tool v.2 for the analyses is not sufficient and a TO is returned. This is due to the huge dimension of the search space associated to these problems.

Table 12 shows the results obtained by running the TA4SP back-end of the AVISPA Tool v.2 under the TY&UNB scenario. For each problem, we report whether the absence of any attack has been established (YES) or not (†) in the considered scenario (see the column "Safe") and the time in seconds spent by the TA4SP back-end to analyse the problem (column "TA4SP"). It must be noted that when a "†" is returned, then the analysis conducted by the TA4SP back-end is inconclusive, i.e. the intersection between the computed over-approximation and the set of secrecy terms is not empty (see Deliverable 4.5 [5] for more details).

Even if the analysis has been conducted on a few instances, this preliminary step has been very successful and the planned extensions of HLPSL and IF to cover the description of a scenario with an unbounded number of sessions, will enable us to cover a larger number of protocols.

The AVISPA Tool v.2 achieves also the effectiveness requirement as it successfully and automatically analyses 110 of the 112 problems specified (i.e. a percentage of 98%).

Table 8: Effectiveness of the AVISPA Tool v.2 on the UNTY&B scenario, part I

Problem	**Attack**	**OFMC**	**CL-atse**
UMTS_AKA-secrecy	NO	0.02	0.00
UMTS_AKA-wauth-1	NO	0.01	0.00
UMTS_AKA-wauth-2	NO	0.00	0.00
AAAMobileIP-secrecy	NO	0.13	0.01
AAAMobileIP-wauth-1	NO	0.11	0.02
AAAMobileIP-wauth-2	NO	0.12	0.02
AAAMobileIP-wauth-3	NO	0.11	0.02
AAAMobileIP-wauth-4	NO	0.12	0.02
AAAMobileIP-wauth-5	YES	0.01	0.00
AAAMobileIP-wauth-6	YES	0.02	0.01
ISO1-auth-1	YES	0.01	0.01
ISO2-auth-1	NO	0.05	Y 0.01
ISO3-wauth-1	YES	0.02	0.01
ISO3-wauth-2	YES	0.02	0.00
ISO4-auth-1	NO	0.43	Y 0.01
ISO4-auth-2	NO	0.40	Y 0.01
LPD-MSR-secrecy	YES	0.01	0.00
LPD-MSR-wauth-1	YES	0.00	0.00
LPD-IMSR-secrecy	NO	0.03	0.02
LPD-IMSR-wauth-1	NO	0.03	0.01
CHAPv2-auth-1	NO	0.08	0.00
CHAPv2-auth-2	NO	0.09	0.00
CHAPv2-secrecy	NO	0.10	0.01
EKE-auth-1	YES	0.03	0.00
EKE-auth-2	YES	0.05	0.01
EKE-secrecy	NO	0.10	0.02
TLS-auth-1	NO	1.13	0.13
TLS-auth-2	NO	1.17	Y 0.02
TLS-secrecy	NO	1.16	0.30
DHCP-delayed-auth-auth-1	NO	0.04	0.02
DHCP-delayed-auth-secrecy	NO	0.03	0.00

Legenda:

YES : a known attack has been found
Y : an attack based on the associativity of pairing has been found
NO : the protocol is safe under the analysed scenario

Table 9: Effectiveness of the AVISPA Tool v.2 on the UNTY&B scenario, part II

Problem	**Attack**	**OFMC**	**CL-atse**	
Kerb-Cross-Realm-auth-1	NO	1.20	Y	0.03
Kerb-Cross-Realm-auth-2	NO	1.25	Y	0.04
Kerb-Cross-Realm-auth-3	NO	1.22	Y	0.04
Kerb-Cross-Realm-auth-4	NO	1.26		10.09
Kerb-Cross-Realm-auth-5	NO	1.23		8.37
Kerb-Cross-Realm-secrecy	NO	1.47		8.52
Kerb-Cross-Realm-wauth-1	NO	1.21		8.38
Kerb-Cross-Realm-wauth-2	NO	1.21		8.39
Kerb-Ticket-Cache-auth-1	NO	0.35	Y	0.03
Kerb-Ticket-Cache-auth-2	NO	0.37	Y	0.48
Kerb-Ticket-Cache-auth-3	NO	0.35		MO
Kerb-Ticket-Cache-auth-4	NO	0.36	Y	0.49
Kerb-Ticket-Cache-secrecy	NO	0.38	Y	0.01
Kerb-Ticket-Cache-wauth-1	NO	0.36	Y	0.01
Kerb-basic-secrecy	NO	0.44		0.31
Kerb-basic-wauth-1	NO	0.37	Y	0.01
Kerb-basic-wauth-2	NO	0.38	Y	0.02
Kerb-basic-wauth-3	NO	0.37	Y	0.03
Kerb-basic-wauth-4	NO	0.38	Y	0.02
Kerb-basic-wauth-5	NO	0.37		0.36
Kerb-basic-wauth-6	NO	0.36		0.30
Kerb-basic-wauth-7	NO	0.38		0.30
Kerb-Forwardable-auth-1	NO	6.73	Y	0.04
Kerb-Forwardable-auth-2	NO	6.70	Y	2.25
Kerb-Forwardable-auth-3	NO	6.54		MO
Kerb-Forwardable-auth-4	NO	6.70	Y	2.29
Kerb-Forwardable-secrecy	NO	7.48	Y	0.03
Kerb-Forwardable-wauth-1	NO	6.66	Y	0.03
Kerb-PKINIT-auth-1	NO	0.53		MO
Kerb-PKINIT-auth-2	NO	0.52	Y	0.02
Kerb-PKINIT-auth-3	NO	0.50		MO
Kerb-PKINIT-auth-4	NO	0.48	Y	0.37
Kerb-PKINIT-secrecy	NO	0.59	Y	0.35
Kerb-PKINIT-wauth-1	NO	0.53	Y	50.09
Kerb-PKINIT-wauth-2	NO	0.51		MO

Legenda:

Y : an attack based on the associativity of pairing has been found
NO : the protocol is safe under the analysed scenario
MO : memory out

Table 10: Effectiveness of the AVISPA Tool v.2 on the UNTY&B scenario, part III

Problem	**Attack**	**OFMC**	**CL-atse**
Kerb-preauth-auth-1	NO	0.37	Y 0.02
Kerb-preauth-auth-2	NO	0.36	Y 0.56
Kerb-preauth-auth-3	NO	0.34	MO
Kerb-preauth-auth-4	NO	0.36	Y 0.57
Kerb-preauth-secrecy	NO	0.39	Y 0.02
Kerb-preauth-wauth-1	NO	0.38	Y 0.02
Kerb-preauth-wauth-2	NO	0.36	MO
CRAM-MD5-auth-1	NO	1.04	0.83
CRAM-MD5-secrecy	NO	1.01	0.01
PBK-auth-1	YES	0.23	0.02
PBK-fix-weak-auth-wauth-1	NO	3.34	22.51
PBK-fix-auth-1	YES	0.09	0.02
SRP_siemens-auth-1	NO	0.72	-
SRP_siemens-auth-2	NO	0.71	-
SRP_siemens-secrecy	NO	0.90	-
EKE2-auth-1	NO	0.06	-
EKE2-auth-2	NO	0.04	-
EKE2-secrecy	NO	0.04	-
SPEKE-auth-1	NO	1.04	-
SPEKE-auth-2	NO	1.02	-
SPEKE-secrecy	NO	1.09	-
IKEv2-CHILD-auth-1	NO	0.34	-
IKEv2-CHILD-auth-2	NO	0.33	-
IKEv2-CHILD-secrecy	NO	0.33	-
IKEv2-DS-auth-1	NO	2.62	-
IKEv2-DS-auth-2	YES	0.08	-
IKEv2-DS-secrecy	NO	2.65	-
IKEv2-DSx-auth-1	NO	18.69	-
IKEv2-DSx-auth-2	NO	18.79	-
IKEv2-DSx-secrecy	NO	19.13	-
IKEv2-MAC-auth-1	NO	2.81	-
IKEv2-MAC-auth-2	NO	2.79	-
IKEv2-MAC-secrecy	NO	2.78	-

Legenda:

YES	:	a known attack has been found
Y	:	an attack based on the associativity of pairing has been found
NO	:	the protocol is safe under the analysed scenario
-	:	special properties of cryptographic operators are not supported
MO	:	memory out

Table 11: Effectiveness of the AVISPA Tool v.2 on the UNTY&B scenario, part IV

Problem	Attack	OFMC	CL-atse
IKEv2-MACx-auth-1	NO	18.08	-
IKEv2-MACx-auth-2	NO	18.03	-
IKEv2-MACx-secrecy	NO	17.93	-
h.530-auth-1	TO	TO	-
h.530-auth-2	YES	0.54	-
h.530-secrecy	TO	TO	-
h.530-fix-auth-1	NO	1,320.53	-
h.530-fix-auth-2	NO	1,315.75	-
h.530-fix-secrecy	NO	1,323.50	-
lipkey-spkm-known-initiator-auth-1	NO	0.10	-
lipkey-spkm-known-initiator-secrecy	NO	0.10	-
lipkey-spkm-unknown-initiator-auth-1	NO	2.86	-
lipkey-spkm-unknown-initiator-secrecy	NO	3.22	-

Legenda:

NO : the protocol is safe under the analysed scenario
YES : a new attack has been found
\- : special properties of cryptographic operators are not supported
TO : time-out

4 Performance

The time spent by the AVISPA Tool v.2 for compiling HLPSL into IF is always negligible (a few milliseconds), and therefore we do not report it in the above Tables.

The AVISPA Tool v.2 analyses 110 problems in less than 25 minutes per problem of CPU time (globally the 110 problems require 69 minutes of CPU time to be analysed) and, therefore, also the performance requirement is successfully met by the tool. In more detail, the majority of the problems (namely, 86 problems) require less than 1 second of CPU time each; and 104 problems require less than 15 seconds of CPU time each to be analysed. Hence, the time required by the AVISPA Tool v.2 for analysing most of the problems is very low and thus acceptable for a modeller involved in security protocol design.

For what concerns the performance of each single back-end, OFMC analyses all 110 problems in 75 minutes of CPU time. 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. Finally, the preliminary results obtained with TA4SP are good enough to be classified as acceptable for protocol designers and indeed very promising especially considering that TA4SP has been integrated in the AVISPA Tool only recently and that it analyses scenarious with an

Table 12: Effectiveness of the AVISPA Tool v.2 on the TY&UNB scenario

Problem	**Safe**	**TA4SP**
EKE-secrecy	YES	13.55
EKE2-secrecy	YES	5.66
IKEv2-CHILD-secrecy	YES	121.94
IKEv2-DS-secrecy	TO	TO
IKEv2-DSx-secrecy	TO	TO
IKEv2-MAC-secrecy	YES	12.08
IKEv2-MACx-secrecy	TO	TO
LPD-MSR-secrecy	†	1.17
SPEKE-secrecy	†	16.15
TLS-secrecy	YES	65.36
UMTS_AKA-secrecy	YES	3.05
CHAPv2-secrecy	YES	2.61

Legenda:

YES	:	the protocol is proved to be secure with respect to secrecy
†	:	the analysis is inconclusive
TO	:	time out has been reached

unbounded number of sessions.

5 New Attacks

The experimental analysis demonstrates that the AVISPA Tool v.2 meets all the success criteria at month 24. Moreover, besides for some attacks that were already known (for instance, the weak authentication attack on the ISO-PK1 protocol [14], also known as "ISO Public Key One-Pass Unilateral Authentication Protocol"), the AVISPA Tool v.2 also finds, as its predecessor AVISPA Tool v.1, 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 [19]. It was already known that ISO-PK3 is vulnerable to replay attacks and hence it does not provide strong authentication [14]: 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 [24] is new,[8] though it is similar to a well-known attack on the Station-2-Station protocol [26]. As pointed out in [28], several protocols that were inspired by Station-2-

[8]Notice that, in parallel the same attack has been reported in [27].

Station (e.g. also the first version of IKE) exhibit the same vulnerability. Also, as described in both [26] and [28], 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.

Further we want to note that, shortly before the start of the AVISPA project, the ETHZ and Siemens partners have applied OFMC to analyse the H.530 protocol of the ITU [21], a protocol developed by Siemens to provide mutual authentication and key agreement in mobile roaming scenarios in multimedia communication. As discussed in detail in [6], OFMC detects a previously unknown attack to H.530. The attack is based on replaying old messages. The attack is caused by the lack of information in one protocol message and allows the intruder to masquerade as any honest agent. The weakness is serious enough that Siemens has changed the protocol accordingly, and Sebastian Mödersheim of ETHZ participated in the new patent that was recently submitted. We have formalized H.530 in new HLPSL and have included it into this assessment for the first time; therefore we have marked this attack as new.

Finally, in the first assessment of the AVISPA Tool, with CL-AtSe we have found two attacks (namely on 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 the untyped model that were due to the associativity of pairing. Such attacks had never been reported before, so we have declared them as new. For this second assessment of the AVISPA tool, we have modeled many more complex protocols, containing larger messages that are often composed by concatenating several sub-messages; as a consequence, with this concatenation represented by pairing, CL-AtSe finds many errors under the untyped model. These attacks show that the implemention of the protocols has to be very precise, and has to avoid a naive use of pairing of sub-messages. Even if all these attacks had never been reported before, because of their high number and because of their specificity, we have decided to indicate their existence (see the "Y" occurrences in Tables 8, 9, and 10), but not to emphasize them too much.

References

[1] C. Adams. RFC 2025: The Simple Public-Key GSS-API Mechanism (SPKM), Oct. 1996. Status: Proposed Standard.

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

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

[4] AVISPA. Deliverable 7.2: Assessment of the AVISPA tool v.1. Available at `http://www.avispa-project.org`, 2003.

[5] AVISPA. Deliverable 4.5: AVISPA tool v.2. Available at `http://www.avispa-project.org`, 2004.

[6] 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`.

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

[8] 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.

[9] C. Boyd and A. Mathuria. Key establishment protocols for secure mobile communications: A selective survey. *Lecture Notes in Computer Science*, 1438:344ff, 1998.

[10] S. Bradner, A. Mankin, and J. Schiller. A Framework for Purpose-Built Keys (PBK), June 2003. Work in Progress.

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

[12] H. Comon-Lundh and V. Cortier. Security properties: two agents are sufficient. In *Proceedings of ESOP'2003*, LNCS 2618, pages 99–113. Springer-Verlag, 2003.

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

[14] 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.

[15] R. Droms and W. Arbaugh. RFC 3118: Authentication for DHCP Messages, June 2001. Status: Proposed Standard.

[16] M. Eisler. RFC 2847: LIPKEY - A Low Infrastructure Public Key Mechanism Using SPKM, June 2000. Status: Proposed Standard.

[17] S. Hartman. A Generalized Framework for Kerberos Pre-Authentication, Oct. 2004. `http://www.ietf.org/internet-drafts/draft-ietf-krb-wg-preauth-framework-02.txt`, Work in Progress.

[18] 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.

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

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

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

[22] ITU. ITU H.530 Corrigendum 1: Symmetric security procedures for H.323 mobility in H.510, July 2003. Available through http://www.itu.int/ITU-T/studygroups/com16/index.html.

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

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

[25] J. Klensin, R. Catoe, and P. Krumviede. RFC 2195: IMAP/POP AUTHorize Extension for Simple Challenge/Response, Sept. 1997. Status: Proposed Standard.

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

[27] W. Mao and K. G. Paterson. On the plausible deniability feature of internet protocols. 2004.

[28] 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.

[29] 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.

[30] C. Neuman, T. Yu, S. Hartman, and K. Raeburn. The Kerberos Network Authentication Service (V5), Sept. 2004. `http://www.ietf.org/internet-drafts/draft-ietf-krb-wg-kerberos-clarifications-07.txt`, Work in Progress.

[31] B. Tung, C. N. L., Z. M. Hur, and S. Medvinsky. Public Key Cryptography for Initial Authentication in Kerberos, Dec. 2004. `http://www.ietf.org/internet-drafts/draft-ietf-cat-kerberos-pk-init-22.txt`, Work in Progress.

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

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