AVISPA

www.avispa-project.org

IST-2001-39252

Automated Validation of Internet Security Protocols and Applications

---

Deliverable D7.4: Assessment of the AVISPA Tool v.3

Abstract

In this document, we report on the assessment of the AVISPA Tool at project month 30. 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 215 problems from 22 groups, and the AVISPA Tool v.3 successfully analyses 215 problems in less than 24 minutes of CPU time per problem (globally, the whole library of 215 problems requires 87 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.3. Moreover, the AVISPA Tool v.3 is able to detect, besides those already discovered by its previous versions, new attacks (i.e. previously unknown in literature) to some of the protocols recently analysed.

Deliverable details

Deliverable version: *1*
Person-months required: *3*
Date of delivery: *14.07.2005*
Due on: *30.06.2005*
Classification: *public*
Total pages: *35*

Project details

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

Information Society Technologies

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.3 against the library of security problems selected in WP6 [4], which comprises a total of 384 security problems and 79 protocols divided into 33 groups.

We recall that a security problem is given by both a protocol and a security property the protocol should satisfy. With respect to the previous assessment (see Deliverable 7.3 [5]) in which all the secrecy properties specified in a HLPSL specification were kept together in a single problem instance, we have enhanced the HLPSL2IF translator to provide an IF specification for each secrecy property specified. In this way the number of security problems increases, but this allows the AVISPA Tool to be more precise about what secrecy property (if any) has been violated. As we will see below, this modification changes the number of problems in the AVISPA Library but it does not affect the achievement of our success criteria.

As described in Deliverable 6.1 [4], 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 (including at least one problem from each of the first seven groups — in the Technical Annex called the "Main Protocols") 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 [4]; 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 30 if the tool meets the following criteria:

Coverage: at least 80 security problems taken from at least 20 of the 33 groups given in [4] should be specifiable in the HLPSL.

Effectiveness: at least 75% (i.e. 60) of the problems specified in the HLPSL should be successfully analysed by the tool.

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 30	**Objectives**	**Results**
Coverage	80 problems from 20 groups	215 problems from 22 groups
Effectiveness	60 problems	215 problems
Performance	$<$ 1 hour per problem	$<$ 24 minutes per problem—all 215 problems in 87 minutes

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.3 are given in Table 2. We have been able to formalise in the HLPSL 215 problems (i.e. 147 problems if all the secrecy properties specified for a protocol are checked in one single security problem) from 22 groups, and the tool successfully analyses 215 problems (i.e. 147 problems if all the secrecy properties specified for a protocol are checked in one single security problem) in less than 24 minutes of CPU time per problem (globally, the entire library of 215 problems requires 87 minutes of CPU time to be analysed). Therefore, all the above requirements (namely coverage, effectiveness, and performance) are largely fulfilled by the AVISPA Tool v.3. Moreover, the AVISPA Tool v.3 is able to detect, besides those already discovered by its previous versions (see Deliverable 7.2 [5] and Deliverable 7.3 [7]), new attacks (i.e. previously unknown in literature) to some of the protocols recently analysed.

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 v.3 (Section 5).

2 Coverage

The set of security protocols used for the assessment is depicted in Table 3 and in Table 4. The latter table reports on the so called "Main Protocols" (the first seven groups in the Technical Annex) and the former on the others. For each protocol, we indicate the group it belongs to (according to the classification given in Deliverable 6.1 [4]),[1] 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 three columns is different from 1, then we refer to the various authentication and secrecy problems that arise by distinguishing several authentication and secrecy 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 30 asks for the ability to formalise HLPSL-specifications of 80 problems from 20 groups, and to automatically translate them into IF-specifications (by means of the HLPSL2IF translator). As summarized in Table 5 we have specified in HLPSL 215 problems (i.e. 147 problems if all the secrecy properties specified for a protocol are checked in one single security problem) from 22 groups and the AVISPA Tool v.3 successfully translated all these 215 problems in IF via the HLPSL2IF translator. Therefore, the AVISPA Tool v.3 largely fullfills the coverage requirement.

3 Effectiveness

We recall that the back-ends integrated into the AVISPA Tool v.3 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.

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 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

[1] With reference to Table 3, "PAKE" is the acronym for the "Password-Authenticated Key Exchange" group.

Table 3: Coverage of the AVISPA Tool v.3: Protocols

Protocol			**Property**		
Name	**Group**	**Reference**	**Secrecy**	**W.Auth.**	**S.Auth.**
UMTS-AKA	3GPP	[2]	2		2
ISO-PK1	ISO	[29]			1
ISO-PK2	ISO	[29]			1
ISO-PK3	ISO	[29]		2	
ISO-PK4	ISO	[29]			2
CHAPv2	ppp-wg	[53]	2		2
EKE	PAKE	[11]	2		2
SRP	PAKE	[51]	2		2
EKE2	PAKE	[10]	2		2
SPEKE	PAKE	[33]	4		2
IKEv2-CHILD	ipsec	[35]	2		2
IKEv2-DS	ipsec	[35]	2		2
IKEv2-DSx	ipsec	[35]	2		2
IKEv2-MAC	ipsec	[35]	2		2
IKEv2-MACx	ipsec	[35]	2		2
TLS	TLS	[18]	2		2
LPD-MSR	LPD	[13]	1	1	
LPD-IMSR	LPD	[13]	1	1	
Kerb-basic	krb-wg	[43]	6	7	
Kerb-Cross-Realm	krb-wg	[43]	11	2	5
Kerb-Ticket-Cache	krb-wg	[43]	6		5
Kerb-Forwardable	krb-wg	[43]	7		5
Kerb-PreAuth	krb-wg	[27]	6		6
Kerb-PKINIT	krb-wg	[48]	6		6
CRAM-MD5	challenge-response	[36]	1		1
PBK	ipv6	[14]			1
PBK-fixed	ipv6	[14]			1
PBK-fix-weak-auth	ipv6	[14]		1	
hip	IPv6	[42]	1		1
DHCP-delayed-auth	DHC	[20]	1		1
lipkey-spkm-knw-init.	CAT	[1, 23]	4		2
lipkey-spkm-unknw-init.	CAT	[1, 23]	4		1
TSIG	DNSext	[49, 22, 21, 50]		2	
ASW	Payment	[3, 26]	1		2
ASW-abort	Payment	[3, 26]	2		2
FairZG	Payment	[52]			5
SET-purchase	E-Commerce	[39, 9]	2	1	1
SET-p.-hon.-payment-gw	E-Commerce	[39, 9]	2	1	1
		Total	88 (29)	18	74

Table 4: Coverage of the AVISPA Tool v.3: Main Protocols

Main Protocol			**Property**		
Name	**Group**	**Reference**	**Secrecy**	**W.Auth.**	**S.Auth.**
AAAMobileIP	mobileip-wg	[15]	3	6	
h.530	H323 Suite	[30, 32]	2		2
h.530-fix	H323 Suite	[30, 32]	2		2
Simple	impp and simple	[34, 24, 44, 45]	1	2	
CTP-non_predictive-fix	seamoby	[12]	1		2
geopriv	Geopriv	[16]	3	1	1
pervasive	Geopriv	[16]	1		1
two_pseudonyms	Geopriv	[16]	4		1
QoS-NSLP	NSIS	[17]		2	
sip	SIP	[25, 24]			1
		Total	17 (8)	11	10

Table 5: Coverage of the AVISPA Tool v.3: summary

	Main Protocols	**No Protocols**	**No Groups**	**No Problems**
	NO	38	15	177 (118)
	YES	10	7	38 (29)
Grand total		48	22	215 (147)

attacks are of little practical significance as actual implementations of security protocols often enforce simple mechanisms that exclude their applicability (see, for instance, [28]). 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.3 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).[2]

[2]Notice that, while we thoroughly assessed the AVISPA Tool on TY&B and UNTY&B, experimentation with TY&UNB has started only 6 months ago and therefore the results in this case are still preliminary.

Table 6: Effectiveness of the AVISPA Tool v.3 on the TY&B scenario

Problems		CL-Atse			OFMC			SATMC			TA4SP		
Protocol	**#P**	**Time**	**S**	**A**	**Time**	**S**	**A**	**Time**	**S**	**A**	**Time**	**S**	**A**
UMTS_AKA	4	0.01	4	0	0.03	4	0	0.01	4	0	0.56	2	0
ISO1	1	0.02	0	1	0.02	0	1	0.04	0	1	-	0	0
ISO2	1	0.02	1	0	0.07	1	0	0.63	1	0	-	0	0
ISO3	2	0.03	0	$\boxed{2}$	0.03	0	$\boxed{2}$	0.39	0	$\boxed{2}$	-	0	0
ISO4	2	0.03	2	0	0.38	2	0	208.31	2	0	-	0	0
CHAPv2	4	0.02	4	0	0.18	4	0	0.10	4	0	16.29	2	0
EKE	4	0.03	2	2	0.10	2	2	0.09	2	2	2.86	2	0
SRP	4	0.02	4	0	0.07	4	0	-	0	0	-	0	0
EKE2	4	0.03	4	0	0.05	4	0	-	0	0	-	0	0
SPEKE	6	0.07	6	0	1.49	6	0	-	0	0	-	0	0
IKEv2-CHILD	4	0.07	4	0	0.51	4	0	-	0	0	-	0	0
IKEv2-DS	4	0.29	3	$\boxed{1}$	2.38	3	$\boxed{1}$	-	0	0	-	0	0
IKEv2-DSx	4	3.74	4	0	17.28	4	0	-	0	0	-	0	0
IKEv2-MAC	4	0.05	4	0	3.01	4	0	-	0	0	-	0	0
IKEv2-MACx	4	5.27	4	0	15.94	4	0	-	0	0	-	0	0
TLS	4	0.05	4	0	0.29	4	0	1018.28	4	0	TO	0	0
LPD-MSR	2	0.02	0	2	0.02	0	2	0.06	0	2	0.61	0	0
LPD-IMSR	2	0.04	2	0	0.04	2	0	0.10	2	0	3.25	1	0
Kerb-basic	10	0.07	10	0	0.61	10	0	6.24	10	0	TO	0	0
Kerb-Cross-Realm	18	0.52	18	0	2.22	18	0	5.70	18	0	-	0	0
Kerb-Ticket-Cache	11	0.08	11	0	0.60	11	0	28.90	11	0	-	0	0
Kerb-PKINIT	12	0.06	12	0	0.47	12	0	27.21	12	0	-	0	0
Kerb-Forwardable	12	0.16	12	0	7.12	12	0	TO	0	0	-	0	0
Kerb-preauth	12	0.12	12	0	0.39	12	0	20.54	12	0	-	0	0
CRAM-MD5	2	0.04	2	0	0.23	2	0	0.17	2	0	0.97	1	0
PBK	1	0.01	0	1	0.34	0	1	0.25	0	1	-	0	0
PBK-fix	1	0.03	0	1	0.14	0	1	0.09	0	1	-	0	0
PBK-fix-weak-auth	1	0.49	1	0	3.47	1	0	0.33	1	0	-	0	0
hip	2	0.09	2	0	0.23	2	0	-	0	0	-	0	0
DHCP-delayed-auth	2	0.02	2	0	0.06	2	0	0.12	2	0	6.84	1	0
lipkey-spkm-knw-init.	6	0.06	6	0	0.17	6	0	-	0	0	-	0	0
lipkey-spkm-unknw-init.	5	0.12	5	0	4.72	5	0	-	0	0	-	0	0
TSIG	2	0.05	2	0	0.19	2	0	0.38	2	0	-	0	0
ASW	3	0.10	3	0	0.35	3	0	TO	0	0	-	0	0
ASW-abort	4	0.20	3	$\boxed{1}$	1.98	3	$\boxed{1}$	65.75	3	$\boxed{1}$	-	0	0

continued on next page

Legend:

-	the problem is not supported by the back-end
TO	time-out

continued from previous page													
Problems		**CL-Atse**			**OFMC**			**SATMC**			**TA4SP**		
Protocol	**#P**	**Time**	**S**	**A**	**Time**	**S**	**A**	**Time**	**S**	**A**	**Time**	**S**	**A**
FairZG	5	0.37	5	0	8.76	5	0	0.28	5	0	-	0	0
SET-purchase	4	23.66	1	$\boxed{2}$	1.24	0	$\boxed{2}$	TO	0	0	-	0	0
SET-p.-hon.-payment-gw	4	0.61	4	0	0.83	4	0	TO	0	0	-	0	0
AAAMobileIP	9	0.03	9	0	0.14	9	0	0.11	9	0	754.11	3	0
h.530	4	TO	0	0	0.70	0	$\boxed{2}$	-	0	0	-	0	0
h.530-fix	4	TO	0	0	1391.66	4	0	-	0	0	-	0	0
Simple	3	100.17	3	0	78.50	3	0	0.50	3	0	-	0	0
CTP-non_predictive-fix	3	0.06	3	0	0.23	3	0	TO	0	0	-	0	0
geopriv	5	0.04	5	0	0.25	5	0	0.08	5	0	-	0	0
pervasive	2	47.67	2	0	30.52	2	0	4.00	2	0	TO	0	0
two_pseudonyms	5	0.06	5	0	0.30	5	0	0.07	5	0	-	0	0
QoS-NSLP	2	32.16	2	0	16.01	2	0	0.21	2	0	-	0	0
sip	1	0.05	1	0	1.86	1	0	810.01	1	0	-	0	0

Legend:

-	the problem is not supported by the back-end
TO	time-out

By running the back-ends of the AVISPA Tool v.3 against all the 215 problems under the TY&B and UNTY&B scenarios, we obtained the results summarized in Table 6 and Table 7 respectively.[3] For each of the protocols, the tables give the number of security problems ("#P"), and for each back-end,

the number of problems for which no attacks are detected ("S"), the number of problems for which attacks are detected ("A"), and the (average) time ("Time") spent by the back-end to find the attacks or to report that no attack exists in the given (bounded) scenario.[4]

A "–" indicates that the back-end does not support some of the features required by the problem (in most cases this regards with some special properties of cryptographic operators such as exponentiation), and hence that the problems cannot be properly analysed by the back-end. A boxed number in the "A" column denotes that the AVISPA Tool v.3 has found at least one new (previously unknown in literature) attack under the typed model. "TO" indicates that a "time-out" occurred.

[3]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.

[4]For SATMC we report only the time spent to generate the SAT formula since that spent to solve the formula is always negligible.

Table 7: Effectiveness of the AVISPA Tool v.3 on the UNTY&B scenario

Problems		**CL-Atse**			**OFMC**		
Protocol	**#P**	**Time**	**S**	**A**	**Time**	**S**	**A**
UMTS_AKA	4	0.02	4	0	0.04	4	0
ISO1	1	0.01	0	1	0.02	0	1
ISO2	1	0.01	0	1	0.07	1	0
ISO3	2	0.02	0	$\boxed{2}$	0.03	0	$\boxed{2}$
ISO4	2	0.04	0	2	0.63	2	0
CHAPv2	4	0.02	4	0	0.27	4	0
EKE	4	0.04	2	2	0.10	2	2
SRP	4	0.03	4	0	0.08	4	0
EKE2	4	0.02	4	0	0.04	4	0
SPEKE	6	0.08	6	0	1.52	6	0
IKEv2-CHILD	4	0.07	4	0	0.43	4	0
IKEv2-DS	4	0.11	0	$\boxed{4}$	2.52	3	$\boxed{1}$
IKEv2-DSx	4	1.19	0	4	23.63	4	0
IKEv2-MAC	4	0.15	2	2	3.25	4	0
IKEv2-MACx	4	4.82	2	2	22.14	4	0
TLS	4	0.07	4	0	0.27	4	0
LPD-MSR	2	0.02	0	2	0.03	0	2
LPD-IMSR	2	0.03	2	0	0.05	2	0
Kerb-basic	10	0.30	8	2	0.60	10	0
Kerb-Cross-Realm	18	7.75	15	3	1.93	18	0
Kerb-Ticket-Cache	11	0.18	0	6	0.53	11	0
Kerb-Forwardable	12	0.97	0	5	9.74	12	0
Kerb-PreAuth	12	0.20	0	6	0.54	12	0
Kerb-PKINIT	12	0.17	11	1	0.39	12	0
CRAM-MD5	2	0.07	2	0	0.83	2	0
PBK	1	0.01	0	1	0.35	0	1
PBK-fix	1	0.03	0	1	0.12	0	1
PBK-fix-weak-auth	1	0.50	1	0	4.26	1	0
hip	2	0.19	2	0	0.63	2	0
DHCP-delayed-auth	2	0.02	2	0	0.07	2	0
lipkey-spkm-knw-init.	6	0.06	6	0	0.14	6	0
lipkey-spkm-unknw-init.	5	0.29	5	0	3.78	5	0
TSIG	2	0.04	2	0	0.17	2	0
ASW	3	1.10	3	0	0.44	3	0
ASW-abort	4	7.76	3	1	4.92	3	1
FairZG	5	0.34	5	0	7.97	5	0

continued on next page

Legend:

TO time-out

continued from previous page

Problems		**CL-Atse**			**OFMC**		
Protocol	**#P**	**Time**	**S**	**A**	**Time**	**S**	**A**
SET-purchase	4	91.17	0	$\boxed{3}$	1.45	0	$\boxed{2}$
SET-p.-hon.-payment-gw	4	TO	0	0	0.94	4	0
AAAMobileIP	9	0.03	7	2	0.13	7	2
h.530	4	93.43	0	2	0.62	0	2
h.530-fix	4	TO	0	0	1291.39	4	0
Simple	3	102.28	3	0	84.24	3	0
CTP-non_predictive-fix	3	0.05	1	2	0.21	3	0
geopriv	5	0.05	4	1	0.29	5	0
pervasive	2	92.19	2	0	67.25	2	0
two_pseudonyms	5	4.07	5	0	0.39	5	0
QoS-NSLP	2	60.55	2	0	48.59	2	0
sip	1	0.07	1	0	4.05	1	0

Legend:

TO time-out

When using the untyped model (see Table 7), CL-AtSe uses the associativity property of pairing, while OFMC does not. This explains why CL-AtSe finds more attacks on some protocols than OFMC. 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).

It is immediate to see that on both the TY&B and UNTY&B scenarios the AVISPA Tool v.3 is very effective: it is able to successfully analyse all the 215 problems specified in HLPSL. The details (results obtained by each back-end against every problem) of these experimental analysis are reported as appendix in Section A.

Table 8 shows the results obtained by running the TA4SP back-end of the AVISPA Tool v.3 under the TY&UNB scenario. For each problem, we report whether the absence of any attack has been established (YES) in the considered unbounded scenario (see the column "Safe") and the time in seconds spent by the TA4SP back-end to analyse the problem (column "TA4SP"). A "TO" indicates that a "time-out" occurred.

Since the second assessment TA4SP has been completely re-implemented and some of its feature, including the handling of special properties of cryptographic operators (e.g. exponentiation), are still under development. This is why some problems that were analysed by TA4SP in the second assessment have not been considered in this last assessment. However, 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.3 achieves also the effectiveness requirement as it successfully and automatically analyses all the 215 problems (i.e. 147 problems if all the secrecy properties specified for a protocol are checked in one single security problem) specified.

Table 8: Effectiveness of the AVISPA Tool v.3 on the TY&UNB scenario

Problem	Safe	TA4SP
UMTS_AKA-secrecy-sseq1	YES	2.16
UMTS_AKA-secrecy-sseq2	YES	2.13
CHAPv2-secrecy-sec_kab1	YES	113.74
CHAPv2-secrecy-sec_kab2	YES	113.70
EKE-secrecy-sec_k1	YES	4.18
EKE-secrecy-sec_k2	YES	4.15
TLS-secrecy-sec_clientk		TO
TLS-secrecy-sec_serverk		TO
LPD-IMSR-secrecy-secx	YES	3.25
CRAM-MD5-secrecy-sec_SK	YES	0.37
DHCP-delayed-auth-secrecy-sec_k	YES	11.72
AAAMobileIP-secrecy-secFAHA		TO
AAAMobileIP-secrecy-secFAMN		TO
AAAMobileIP-secrecy-secMNHA		TO

Legend:

YES : the protocol is proved to be secure with respect to secrecy

TO : time out has been reached

4 Performance

The time spent by the AVISPA Tool v.3 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.3 analyses 215 problems in less than 24 minutes per problem of CPU time (globally the 215 problems require 87 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, 206 problems) require less than 1 second of CPU time each; and 211 problems require less than 10 seconds of CPU time each to be analysed. Hence, the time required by the AVISPA Tool v.3 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 and CL-AtSe are both very efficient in analysing the AVISPA library. On all the problems for which CL-AtSe is successful it is very fast, and in most cases it is actually faster than OFMC, while OFMC is the only tool that can give a conclusive answer on at least one problem for each of the protocols. As far as SATMC is concerned, it is interesting to observe that the time spent by the SAT-solver is always negligible and that on some protocol also the time spent to generate the SAT formula is very low and even better than those of CL-AtSe and OFMC. Finally, the still 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 scenarios with an unbounded number of sessions.

5 New Attacks

The experimental analysis demonstrates that the AVISPA Tool v.3 meets all the success criteria at month 30. Moreover, besides for some attacks that were already known (for instance, the weak authentication attack on the ISO-PK1 protocol [19], also known as "ISO Public Key One-Pass Unilateral Authentication Protocol"), the AVISPA Tool v.3 also finds new attacks (someone already discovered by the AVISPA Tool v.2) which we now briefly discuss.

SET The Secure Electronic Transactions (SET) Protocol Suite is designed to allow for a secure e-commerce. The key feature is to hide the customer's credit card details from the merchant, and the customer's purchase details from the payment gateway. The AVISPA tool detects an attack where a dishonest payment gateway forwards payment authorisation requests to another payment gateway. This is due to the fact that the part of the message signed by the card-holder (as well as the one signed by the merchant) does not contain the name of the desired payment gateway. This weakness of the protocol was already mentioned in the analysis of the SET protocol by Bella, Massacci, and Paulson using the interactive theorem prover Isabelle [9]. They argue that the attack is not very interesting as a dishonest payment gateway "has more interesting crimes to commit", however we believe that this vulnerability is not uncritical as it may lead to the situation that two payment gateways charge the account of the card-holder and both posses messages that seem to prove that the card-holder authorised the transaction. Like [9], we suggest to include the name of the desired payment gateway into the messages to fix this problem.

ASW The ASW protocol, presented by Asokan, Shoup, and Waidner in [3], is an optimistic fair exchange protocol for contract signing intended to enable two parties to commit themselves to a previously agreed upon contractual text. A trusted third party (T3P) is involved *only* if dispute resolution is required (hence the term *optimistic*). In resolving disputes, the T3P issues either a *replacement contract* asserting that he recognises the contract in question as valid, or an *abort token* asserting that he has never issued, and will never issue, a replacement contract. An important requirement of the protocol is that the intruder cannot block messages between an honest agent and the T3P forever.

The particular challenge in analysing this protocol lies in the formulation of the goals of the protocol. In particular, we cannot directly formulate the main goal, *fair exchange*, which requires that if one party has a valid contract, then the other also has a valid contract or can obtain one from the T3P. This is a liveness property and we thus have approximated the goal by (stronger) safety properties.

The weakness the AVISPA tool has detected on this protocol, described in [26], is related to this approximation of the goal. A first, quite naïve, approximation of the goals implies that it already counts as an attack, if an intruder possesses both a valid contract and an abort token for that contract. This goal is easy to violate: the intruder as initiator can first run a normal exchange with an honest responder (not involving the T3P) and then ask the T3P for an abort. Moreover, after this, the intruder can start another exchange with the same contractual text and abort at any time; when the honest responder asks the T3P for a resolve, it will obtain an abort token. A more appropriate formulation of the goal thus allows the intruder to obtain both a valid contract and an abort token, as long as the other involved party of the contract also possesses a valid contract (with the same contractual text). This goal still implies the desired fair exchange property.

Still, the situation that one party has both a valid contract and an abort token was unexpected for us and it is unclear, whether this situation was anticipated by the designers of the protocol. In fact, it is not unrealistic that an intruder can make another agent execute the protocol once more with the same contractual text by a kind of social engineering.[5] The weakness can be eliminated by replay protection, i.e. logging all commitments used in any exchange and refusing to start a run with commitments that appear in the log.

A similar weakness was discovered by [46] on another contract signing protocol, GJM, while for ASW this weakness was not reported previously in the literature. Last but not least, as already shown in [47], ASW cannot provide strong authentication, and the AVISPA tool can also detect such attacks. However these attacks against strong authentication are not very serious since one should assume that the contracts have some kind of unique identifier, e.g. in bank transactions a unique transaction number, so that accepting the same contractual text several times counts just as one time.

New Attacks of the Previous Assessments Also in the previous assessments of the AVISPA tool, attacks were found that have not been previously reported in the literature, and which we like to quickly summarise here.

The AVISPA Tool finds an attack on the ISO-PK3 (also known as "ISO Public Key Two-Pass Mutual Authentication") protocol [29]. It was already known that ISO-PK3 is vulnerable to replay attacks and hence it does not provide strong authentication [19]: 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.

A man-in-the-middle attack discovered on the IKEv2-DS protocol [35] is new,[6] though it is similar to a well-known attack on the Station-2-Station protocol [37]. As pointed out in [40], several protocols that were inspired by Station-2-Station (e.g. also the first version

[5] For instance, after the first exchange, the intruder could tell the contract partner that his (the intruder's) computer had crashed and he had lost the signed contract and therefore asks to run the contract signing again.

[6] Notice that, independently the same attack has been reported in [38].

of IKE) exhibit the same vulnerability. Also, as described in both [37] and [40], 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.

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 [31], a protocol developed by Siemens to provide mutual authentication and key agreement in mobile roaming scenarios in multimedia communication. As discussed in detail in [8], 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.

A Effectiveness of the AVISPA Tool v.3: details

By running the back-ends of the AVISPA Tool v.3 against all the 215 problems under the TY&B and UNTY&B scenarios, we obtained the results listed in Table 9 and Table 10 respectively.[7] For each problem, that is identified by the protocol (see the column "Protocol"), the kind of property (see the column "property"), and the item on which the property is checked (see the column "on"), we report whether an attack is found (YES) or not (NO) (see the column "Atk")[8] and the time in seconds spent by each back-end to analyse the problem (columns "OFMC", "CL-AtSe", "SATMC", and "TA4SP").[9] A boxed "YES" denotes that the AVISPA Tool v.3 has found a new (previously unknown in literature) attack under the typed model. A "–" indicates that the back-end does not support some of the features required by the problem (in most cases this regards with some special properties of cryptographic operators such as exponentiation), and hence that the problems 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.

For instance, the first row of Table 9 reports on the problem of deciding whether the protocol UMTS_AKA may be violated or not with respect to the authentication property on the specific item r1.[10]. Namely, three of the four back-ends (TA4SP does not perform the analyses of authentication properties) of the AVISPA Tool v.3 return in few milliseconds that the above problem is secure in the analysed scenario.

[7]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.

[8]It must be noted that a NO indicates that the AVISPA Tool v.3 has been able to establish that the protocol satisfies the security property under the analysed scenario.

[9]For SATMC we report only the time spent to generate the SAT formula since that spent to solve the formula—we used the Chaff solver [41] for these experiments—is always negligible.

[10]A detailed explanation of the specific items to which the properties are referring to goes beyond the scope of this deliverable and the interested reader should consult the appropriate HLPSL specification described in Deliverable 6.2 [6]

Table 9: Effectiveness of the AVISPA Tool v.3 on the TY&B scenario

Problem			Atk	Backends			
Protocol	property	on		ofmc	cl-atse	satmc	ta4sp
UMTS_AKA	auth	r1	NO	0.03	0.02	0.02	-
	auth	r2	NO	0.01	0.01	0.00	-
	secrecy	sseq1	NO	0.04	0.00	0.02	0.55
	secrecy	sseq2	NO	0.03	0.01	0.01	0.57
ISO1	auth	na	YES	0.02	0.02	0.04	-
ISO2	auth	ra	NO	0.07	0.02	0.63	-
ISO3	wauth	na	$\boxed{\text{YES}}$	0.02	0.02	0.61	-
	wauth	nb	$\boxed{\text{YES}}$	0.03	0.03	0.16	-
ISO4	auth	na	NO	0.39	0.02	191.13	-
	auth	nb	NO	0.36	0.03	225.49	-
CHAPv2	auth	na	NO	0.17	0.01	0.12	-
	auth	nb	NO	0.19	0.02	0.14	-
	secrecy	sec_kab1	NO	0.18	0.03	0.13	16.46
	secrecy	sec_kab2	NO	0.16	0.01	0.02	16.12
EKE	auth	na	YES	0.09	0.03	0.16	-
	auth	nb	YES	0.06	0.03	0.09	-
	secrecy	sec_k1	NO	0.14	0.02	0.06	2.87
	secrecy	sec_k2	NO	0.12	0.04	0.03	2.85
SRP	auth	k1	NO	0.06	0.03	-	-
	auth	k2	NO	0.07	0.02	-	-
	secrecy	sec_i_K	NO	0.06	0.01	-	-
	secrecy	sec_r_K	NO	0.08	0.03	-	-
EKE2	auth	mk_a	NO	0.05	0.02	-	-
	auth	mk_b	NO	0.04	0.02	-	-
	secrecy	sec_i_MK_A	NO	0.04	0.04	-	-

continued on next page

Legend :

YES	a known attack has been found
$\boxed{\text{YES}}$	a new attack has been found
NO	the protocol is safe under the analysed scenario
†	the analysis is inconclusive
-	the problem is not supported by the back-end
MO	memory out
TO	time-out

continued from previous page							
Problem			**Atk**	**Backends**			
Protocol	**property**	**on**		**ofmc**	**cl-atse**	**satmc**	**ta4sp**
	secrecy	sec_r_MK_B	NO	0.05	0.03	-	-
SPEKE	auth	ca	NO	1.61	0.06	-	-
	auth	cb	NO	1.51	0.07	-	-
	secrecy	sec_i_Ca	NO	1.52	0.07	-	-
	secrecy	sec_i_Cb	NO	1.39	0.07	-	-
	secrecy	sec_r_Ca	NO	1.45	0.09	-	-
	secrecy	sec_r_Cb	NO	1.47	0.07	-	-
IKEv2-CHILD	auth	ni	NO	0.52	0.03	-	-
	auth	nr	NO	0.51	0.12	-	-
	secrecy	sec_a_CSK	NO	0.50	0.11	-	-
	secrecy	sec_b_CSK	NO	0.49	0.03	-	-
IKEv2-DS	auth	sk1	NO	3.16	0.38	-	-
	auth	sk2	$\boxed{\text{YES}}$	0.14	0.04	-	-
	secrecy	sec_a_SK	NO	3.10	0.43	-	-
	secrecy	sec_b_SK	NO	3.10	0.31	-	-
IKEv2-DSx	auth	sk1	NO	17.12	12.28	-	-
	auth	sk2	NO	17.26	1.89	-	-
	secrecy	sec_a_SK	NO	17.20	0.47	-	-
	secrecy	sec_b_SK	NO	17.55	0.32	-	-
IKEv2-MAC	auth	sk1	NO	3.02	0.07	-	-
	auth	sk2	NO	3.08	0.07	-	-
	secrecy	sec_a_SK	NO	2.99	0.03	-	-
	secrecy	sec_b_SK	NO	2.95	0.04	-	-
IKEv2-MACx	auth	sk1	NO	16.16	1.15	-	-
	auth	sk2	NO	15.91	8.75	-	-
	secrecy	sec_a_SK	NO	15.64	9.84	-	-
	secrecy	sec_b_SK	NO	16.05	1.32	-	-
TLS	auth	na_nb1	NO	0.29	0.04	1019.56	-
							continued on next page

Legend :

YES	a known attack has been found
$\boxed{\text{YES}}$	a new attack has been found
NO	the protocol is safe under the analysed scenario
†	the analysis is inconclusive
-	the problem is not supported by the back-end
MO	memory out
TO	time-out

continued from previous page

Problem			Atk	Backends			
Protocol	**property**	**on**		**ofmc**	**cl-atse**	**satmc**	**ta4sp**
	auth	na_nb2	NO	0.29	0.07	1026.48	-
	secrecy	sec_clientk	NO	0.29	0.04	1013.58	TO
	secrecy	sec_serverk	NO	0.29	0.05	1013.49	TO
LPD-MSR	secrecy	secx	YES	0.03	0.04	0.03	† 0.61
	wauth	x	YES	0.01	0.00	0.08	-
LPD-IMSR	secrecy	secx	NO	0.04	0.03	0.09	3.25
	wauth	x	NO	0.04	0.04	0.10	-
Kerb-basic	secrecy	sec_a_K_CG	NO	0.61	0.07	7.22	TO
	secrecy	sec_c_K_CG	NO	0.57	0.06	1.93	TO
	secrecy	sec_c_K_CS	NO	0.60	0.08	1.93	TO
	secrecy	sec_g_K_CG	NO	0.63	0.07	7.31	TO
	secrecy	sec_g_K_CS	NO	0.57	0.07	7.28	TO
	secrecy	sec_s_K_CS	NO	0.59	0.07	7.15	TO
	wauth	k_cg	NO	0.70	0.08	7.41	-
	wauth	k_cs	NO	0.64	0.08	7.52	-
	wauth	t1	NO	0.61	0.07	7.42	-
	wauth	t2a	NO	0.57	0.07	7.28	-
Kerb-Cross-Realm	auth	n1	NO	2.32	0.50	6.70	-
	auth	n1r	NO	2.29	0.52	6.85	-
	auth	n2	NO	2.24	0.53	6.98	-
	auth	t2a	NO	2.21	0.62	7.09	-
	auth	t2b	NO	2.30	0.52	6.88	-
	secrecy	sec_a_KC_TGSlocal	NO	2.26	0.52	6.74	-
	secrecy	sec_c_KC_Sremote	NO	2.19	0.53	1.82	-
	secrecy	sec_c_KC_TGSlocal	NO	2.17	0.52	1.83	-
	secrecy	sec_c_KC_TGSremote	NO	2.15	0.51	1.84	-
	secrecy	sec_c_T3	NO	2.17	0.50	1.83	-
	secrecy	sec_s_KC_Sremote	NO	2.21	0.52	6.75	-

continued on next page

Legend :

YES	a known attack has been found
$\boxed{\text{YES}}$	a new attack has been found
NO	the protocol is safe under the analysed scenario
†	the analysis is inconclusive
-	the problem is not supported by the back-end
MO	memory out
TO	time-out

continued from previous page

Problem			Atk	Backends			
Protocol	**property**	**on**		**ofmc**	**cl-atse**	**satmc**	**ta4sp**
	secrecy	sec_s_T3	NO	2.15	0.52	6.87	-
	secrecy	sec_tl_KC_TGSlocal	NO	2.20	0.52	6.74	-
	secrecy	sec_tl_KC_TGSremote	NO	2.23	0.53	6.77	-
	secrecy	sec_tr_KC_Sremote	NO	2.20	0.50	6.69	-
	secrecy	sec_tr_KC_TGSremote	NO	2.21	0.51	6.75	-
	wauth	t1	NO	2.24	0.51	6.83	-
	wauth	t1r	NO	2.23	0.50	6.67	-
Kerb-Ticket-Cache	auth	n1	NO	0.61	0.09	31.25	-
	auth	n2	NO	0.60	0.08	40.07	-
	auth	t1	NO	0.59	0.08	7.37	-
	auth	t2a	NO	0.58	0.09	39.07	-
	auth	t2b	NO	0.62	0.10	32.44	-
	secrecy	sec_c_Kcg	NO	0.57	0.06	7.31	-
	secrecy	sec_c_Kcs	NO	0.57	0.08	7.35	-
	secrecy	sec_k_Kcg	NO	0.64	0.07	37.50	-
	secrecy	sec_s_Kcs	NO	0.61	0.08	37.18	-
	secrecy	sec_t_Kcg	NO	0.60	0.07	42.84	-
	secrecy	sec_t_Kcs	NO	0.58	0.08	35.52	-
Kerb-Forwardable	auth	n1	NO	7.36	0.14	TO	-
	auth	n2	NO	7.39	0.18	TO	-
	auth	t1	NO	7.02	0.16	TO	-
	auth	t2a	NO	6.96	0.17	TO	-
	auth	t2b	NO	7.53	0.16	TO	-
	secrecy	sec_a_Kcg	NO	7.24	0.17	TO	-
	secrecy	sec_c_Kcg1	NO	6.98	0.15	TO	-
	secrecy	sec_c_Kcg2	NO	6.71	0.15	TO	-
	secrecy	sec_c_Kcs	NO	6.82	0.20	TO	-
	secrecy	sec_s_Kcs	NO	7.05	0.16	TO	-

continued on next page

Legend :

YES	a known attack has been found
$\boxed{\text{YES}}$	a new attack has been found
NO	the protocol is safe under the analysed scenario
†	the analysis is inconclusive
-	the problem is not supported by the back-end
MO	memory out
TO	time-out

continued from previous page

Problem			Atk	Backends			
Protocol	**property**	**on**		**ofmc**	**cl-atse**	**satmc**	**ta4sp**
	secrecy	sec_t_Kcg	NO	7.20	0.16	TO	-
	secrecy	sec_t_Kcs	NO	7.15	0.16	TO	-
Kerb-preauth	auth	n1	NO	0.41	0.12	27.52	-
	auth	n2	NO	0.41	0.11	28.64	-
	auth	t0	NO	0.39	0.14	4.68	-
	auth	t1	NO	0.37	0.12	4.69	-
	auth	t2a	NO	0.40	0.11	28.64	-
	auth	t2b	NO	0.37	0.13	34.25	-
	secrecy	sec_a_Kcg	NO	0.38	0.11	26.33	-
	secrecy	sec_c_Kcg	NO	0.37	0.09	4.70	-
	secrecy	sec_c_Kcs	NO	0.38	0.10	4.77	-
	secrecy	sec_s_Kcs	NO	0.37	0.11	28.28	-
	secrecy	sec_t_Kcg	NO	0.38	0.14	26.01	-
	secrecy	sec_t_Kcs	NO	0.39	0.11	28.02	-
Kerb-PKINIT	auth	n1	NO	0.47	0.05	34.76	-
	auth	n2	NO	0.46	0.05	34.41	-
	auth	t0	NO	0.46	0.05	14.07	-
	auth	t1	NO	0.47	0.06	14.18	-
	auth	t2a	NO	0.47	0.08	33.44	-
	auth	t2b	NO	0.48	0.06	33.01	-
	secrecy	sec_a_Kcg	NO	0.51	0.08	33.39	-
	secrecy	sec_c_Kcg	NO	0.47	0.05	14.25	-
	secrecy	sec_c_Kcs	NO	0.44	0.06	14.20	-
	secrecy	sec_s_Kcs	NO	0.45	0.05	33.60	-
	secrecy	sec_t_Kcg	NO	0.48	0.08	33.66	-
	secrecy	sec_t_Kcs	NO	0.46	0.06	33.51	-
CRAM-MD5	auth	auth	NO	0.21	0.06	0.28	-
	secrecy	sec_SK	NO	0.24	0.02	0.06	0.97

continued on next page

Legend :

YES	a known attack has been found
$\boxed{\text{YES}}$	a new attack has been found
NO	the protocol is safe under the analysed scenario
†	the analysis is inconclusive
-	the problem is not supported by the back-end
MO	memory out
TO	time-out

continued from previous page							
Problem			**Atk**	**Backends**			
Protocol	**property**	**on**		**ofmc**	**cl-atse**	**satmc**	**ta4sp**
PBK	auth	msg	YES	0.34	0.01	0.25	-
PBK-fix	auth	msg	YES	0.14	0.03	0.09	-
PBK-fix-weak-auth	wauth	msg	NO	3.47	0.49	0.33	-
hip	auth	initiator_responder_r2	NO	0.23	0.08	-	-
	secrecy	hash_dh	NO	0.22	0.09	-	-
DHCP-delayed-auth	auth	sig	NO	0.06	0.02	0.13	-
	secrecy	sec_k	NO	0.05	0.02	0.10	6.84
lipkey-spkm-known-initiator	auth	k	NO	0.17	0.10	-	-
	auth	ktrgtint	NO	0.16	0.03	-	-
	secrecy	sec_i_Log	NO	0.17	0.05	-	-
	secrecy	sec_i_Pwd	NO	0.16	0.05	-	-
	secrecy	sec_t_Log	NO	0.19	0.08	-	-
	secrecy	sec_t_Pwd	NO	0.16	0.05	-	-
lipkey-spkm-unknown-initiator	auth	k	NO	4.69	0.24	-	-
	secrecy	sec_i_Log	NO	4.59	0.10	-	-
	secrecy	sec_i_Pwd	NO	4.62	0.12	-	-
	secrecy	sec_t_Log	NO	5.34	0.12	-	-
	secrecy	sec_t_Pwd	NO	4.35	0.03	-	-
TSIG	wauth	client_server_k_ba	NO	0.19	0.08	0.37	-
	wauth	server_client_k_ab	NO	0.18	0.02	0.39	-
ASW	auth	no	NO	0.36	0.11	TO	-
	auth	nr	NO	0.36	0.09	TO	-
	secrecy	no_secret	NO	0.34	0.10	TO	-
ASW-abort	auth	no	NO	2.29	0.22	75.83	-
	auth	nr	NO	2.17	0.19	75.38	-
	secrecy	no_secret	NO	2.05	0.21	74.99	-
	secrecy	secret_ref	$\boxed{\text{YES}}$	1.39	0.19	36.79	-
FairZG	wauth	alice_bob_nrr	NO	8.85	0.16	0.29	-
							continued on next page

Legend :

YES	a known attack has been found
$\boxed{\text{YES}}$	a new attack has been found
NO	the protocol is safe under the analysed scenario
†	the analysis is inconclusive
-	the problem is not supported by the back-end
MO	memory out
TO	time-out

continued from previous page

Problem			Atk	Backends			
Protocol	**property**	**on**		**ofmc**	**cl-atse**	**satmc**	**ta4sp**
	wauth	alice_server_con	NO	8.71	0.13	0.27	-
	wauth	bob_alice_nro	NO	8.88	0.97	0.29	-
	wauth	bob_alice_sub	NO	8.68	0.33	0.28	-
	wauth	bob_server_con	NO	8.68	0.25	0.26	-
SET-purchase	auth	deal	MO	MO	TO	TO	-
	secrecy	order	MO	MO	69.90	TO	-
	secrecy	payment	$\boxed{\text{YES}}$	0.94	0.13	TO	-
	wauth	deal	$\boxed{\text{YES}}$	1.53	0.96	TO	-
SET-purchase-hon.-payment-gateway	auth	deal	NO	0.87	1.85	TO	-
	secrecy	order	NO	0.80	0.09	TO	-
	secrecy	payment	NO	0.75	0.08	TO	-
	wauth	deal	NO	0.88	0.43	TO	-
AAAMobileIP	secrecy	secFAHA	NO	0.14	0.02	0.04	753.40
	secrecy	secFAMN	NO	0.15	0.03	0.05	754.19
	secrecy	secMNHA	NO	0.13	0.02	0.06	754.73
	wauth	k_faha1	NO	0.13	0.03	0.14	-
	wauth	k_faha2	NO	0.13	0.03	0.14	-
	wauth	k_mnfa1	NO	0.14	0.03	0.14	-
	wauth	k_mnfa2	NO	0.15	0.03	0.14	-
	wauth	k_mnha1	NO	0.14	0.03	0.14	-
	wauth	k_mnha2	NO	0.13	0.01	0.15	-
h.530	auth	key	TO	TO	TO	-	-
	auth	key1	$\boxed{\text{YES}}$	0.69	TO	-	-
	secrecy	sec_m_Key	TO	TO	TO	-	-
	secrecy	sec_v_Key	$\boxed{\text{YES}}$	0.71	TO	-	-
h.530-fix	auth	key	NO	1395.69	TO	-	-
	auth	key1	NO	1391.94	TO	-	-
	secrecy	sec_m_Key	NO	1391.44	TO	-	-

continued on next page

Legend :

YES	a known attack has been found
$\boxed{\text{YES}}$	a new attack has been found
NO	the protocol is safe under the analysed scenario
†	the analysis is inconclusive
-	the problem is not supported by the back-end
MO	memory out
TO	time-out

continued from previous page							
Problem			**Atk**	**Backends**			
Protocol	**property**	**on**		**ofmc**	**cl-atse**	**satmc**	**ta4sp**
	secrecy	sec_v_Key	NO	1387.55	TO	-	-
Simple	secrecy	presenceinfo	NO	78.87	12.86	0.48	-
	wauth	ps_wr_user	NO	80.68	12.59	0.48	-
	wauth	wr_ps_presenceinfo	NO	75.96	275.05	0.53	-
CTP-non_predictive-fix	auth	npaa_pac_nnpaa	NO	0.21	0.05	TO	-
	auth	ppaa_pac_ip_pac	NO	0.26	0.05	TO	-
	secrecy	mac_key	NO	0.21	0.07	TO	-
geopriv	auth	lr_mu_n_lr	NO	0.28	0.06	0.16	-
	secrecy	filtered_loc	NO	0.24	0.03	0.05	-
	secrecy	k_psi	NO	0.23	0.05	0.05	-
	secrecy	psi	NO	0.25	0.02	0.02	-
	wauth	ls_mu_psi	NO	0.26	0.04	0.13	-
pervasive	auth	lbs_t_n_lbs	NO	30.94	67.71	4.77	-
	secrecy	loc	NO	30.10	27.63	3.22	TO
two_pseudonyms	auth	lr_t_n_lr	NO	0.35	0.06	0.16	-
	secrecy	filtered_loc	NO	0.27	0.04	0.05	-
	secrecy	loc	NO	0.30	0.07	0.04	-
	secrecy	psi_lr	NO	0.30	0.06	0.05	-
	secrecy	psi_t	NO	0.29	0.06	0.04	-
QoS-NSLP	wauth	router_server_clientid	NO	15.76	42.87	0.20	-
	wauth	server_client_service	NO	16.26	21.44	0.23	-
sip	auth	y	NO	1.86	0.05	810.01	-

Legend :

NO	the protocol is safe under the analysed scenario
-	the problem is not supported by the back-end
TO	time-out

When using the untyped model (see Table 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.

Table 10: Effectiveness of the AVISPA Tool v.3 on the UNTY&B scenario

Problem			Atk	Backends	
Protocol	**property**	**on**		**ofmc**	**cl-atse**
UMTS_AKA	auth	r1	NO	0.05	0.01
	auth	r2	NO	0.01	0.00
	secrecy	sseq1	NO	0.04	0.04
	secrecy	sseq2	NO	0.04	0.03
ISO1	auth	na	YES	0.02	0.01
ISO2	auth	ra	NO	0.07	Y 0.01
ISO3	wauth	na	$\boxed{\text{YES}}$	0.03	0.01
	wauth	nb	$\boxed{\text{YES}}$	0.03	0.03
ISO4	auth	na	NO	0.64	Y 0.04
	auth	nb	NO	0.62	Y 0.04
CHAPv2	auth	na	NO	0.29	0.02
	auth	nb	NO	0.28	0.02
	secrecy	sec_kab1	NO	0.28	0.04
	secrecy	sec_kab2	NO	0.23	0.01
EKE	auth	na	YES	0.08	0.03
	auth	nb	YES	0.05	0.05
	secrecy	sec_k1	NO	0.14	0.03
	secrecy	sec_k2	NO	0.14	0.05
SRP	auth	k1	NO	0.06	0.01
	auth	k2	NO	0.10	0.06
	secrecy	sec_i_K	NO	0.09	0.02
	secrecy	sec_r_K	NO	0.07	0.02
EKE2	auth	mk_a	NO	0.04	0.02
	auth	mk_b	NO	0.03	0.01
	secrecy	sec_i_MK_A	NO	0.07	0.01
	secrecy	sec_r_MK_B	NO	0.03	0.02

continued on next page

Legend:

YES	a known attack has been found
$\boxed{\text{YES}}$	a new 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
MO	memory out
TO	time-out

Problem			Atk	Backends		
Protocol	**property**	**on**		**ofmc**		**cl-atse**
SPEKE	auth	ca	NO	1.65		0.07
	auth	cb	NO	1.56		0.08
	secrecy	sec_i_Ca	NO	1.55		0.07
	secrecy	sec_i_Cb	NO	1.45		0.09
	secrecy	sec_r_Ca	NO	1.46		0.08
	secrecy	sec_r_Cb	NO	1.47		0.07
IKEv2-CHILD	auth	ni	NO	0.44		0.05
	auth	nr	NO	0.43		0.10
	secrecy	sec_a_CSK	NO	0.41		0.09
	secrecy	sec_b_CSK	NO	0.42		0.05
IKEv2-DS	auth	sk1	NO	3.39	Y	0.17
	auth	sk2	$\boxed{\text{YES}}$	0.13		0.02
	secrecy	sec_a_SK	NO	3.22	Y	0.21
	secrecy	sec_b_SK	NO	3.35	Y	0.02
IKEv2-DSx	auth	sk1	NO	23.40	Y	4.40
	auth	sk2	NO	23.53	Y	0.07
	secrecy	sec_a_SK	NO	23.65	Y	0.25
	secrecy	sec_b_SK	NO	23.93	Y	0.04
IKEv2-MAC	auth	sk1	NO	3.28		0.25
	auth	sk2	NO	3.34	Y	0.06
	secrecy	sec_a_SK	NO	3.12		0.26
	secrecy	sec_b_SK	NO	3.25	Y	0.04
IKEv2-MACx	auth	sk1	NO	22.45	Y	0.08
	auth	sk2	NO	22.21		9.05
	secrecy	sec_a_SK	NO	21.68		10.02
	secrecy	sec_b_SK	NO	22.20	Y	0.12
TLS	auth	na_nb1	NO	0.27		0.06
	auth	na_nb2	NO	0.27		0.06
	secrecy	sec_clientk	NO	0.25		0.08

continued on next page

Legend:

YES	a known attack has been found
$\boxed{\text{YES}}$	a new 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
MO	memory out
TO	time-out

Problem			Atk	Backends	
Protocol	property	on		ofmc	cl-atse
	secrecy	sec_serverk	NO	0.27	0.07
LPD-MSR	secrecy	secx	YES	0.02	0.02
	wauth	x	YES	0.03	0.01
LPD-IMSR	secrecy	secx	NO	0.05	0.03
	wauth	x	NO	0.05	0.03
Kerb-basic	secrecy	sec_a_K_CG	NO	0.58	0.34
	secrecy	sec_c_K_CG	NO	0.59	0.35
	secrecy	sec_c_K_CS	NO	0.58	0.36
	secrecy	sec_g_K_CG	NO	0.58	0.35
	secrecy	sec_g_K_CS	NO	0.60	0.37
	secrecy	sec_s_K_CS	NO	0.59	0.34
	wauth	k_cg	NO	0.65	Y 0.06
	wauth	k_cs	NO	0.66	Y 0.05
	wauth	t1	NO	0.61	0.38
	wauth	t2a	NO	0.55	0.41
Kerb-Cross-Realm	auth	n1	NO	2.00	Y 0.06
	auth	n1r	NO	2.07	Y 0.08
	auth	n2	NO	1.93	Y 0.09
	auth	t2a	NO	1.92	10.55
	auth	t2b	NO	2.00	9.29
	secrecy	sec_a_KC_TGSlocal	NO	1.96	9.13
	secrecy	sec_c_KC_Sremote	NO	1.88	9.13
	secrecy	sec_c_KC_TGSlocal	NO	1.91	9.33
	secrecy	sec_c_KC_TGSremote	NO	1.85	9.28
	secrecy	sec_c_T3	NO	1.89	9.23
	secrecy	sec_s_KC_Sremote	NO	1.90	9.24
	secrecy	sec_s_T3	NO	1.92	9.16
	secrecy	sec_tl_KC_TGSlocal	NO	1.91	9.15
	secrecy	sec_tl_KC_TGSremote	NO	1.92	9.21

continued on next page

Legend:

YES	a known attack has been found
$\boxed{\text{YES}}$	a new 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
MO	memory out
TO	time-out

Problem			Atk	Backends		
Protocol	property	on		ofmc		cl-atse
	secrecy	sec_tr_KC_Sremote	NO	1.94		9.17
	secrecy	sec_tr_KC_TGSremote	NO	1.88		9.15
	wauth	t1	NO	1.96		9.16
	wauth	t1r	NO	1.97		9.15
Kerb-Ticket-Cache	auth	n1	NO	0.56	Y	0.05
	auth	n2	NO	0.56	Y	0.30
	auth	t1	NO	0.51		MO
	auth	t2a	NO	0.52		MO
	auth	t2b	NO	0.54	Y	0.28
	secrecy	sec_c_Kcg	NO	0.53		MO
	secrecy	sec_c_Kcs	NO	0.52		MO
	secrecy	sec_k_Kcg	NO	0.55		MO
	secrecy	sec_s_Kcs	NO	0.51	Y	0.34
	secrecy	sec_t_Kcg	NO	0.52	Y	0.05
	secrecy	sec_t_Kcs	NO	0.50	Y	0.05
Kerb-Forwardable	auth	n1	NO	10.23	Y	0.11
	auth	n2	NO	10.24		MO
	auth	t1	NO	9.50		MO
	auth	t2a	NO	9.71		MO
	auth	t2b	NO	10.57	Y	2.29
	secrecy	sec_a_Kcg	NO	9.78		MO
	secrecy	sec_c_Kcg1	NO	9.34		MO
	secrecy	sec_c_Kcg2	NO	8.99		MO
	secrecy	sec_c_Kcs	NO	9.35		MO
	secrecy	sec_s_Kcs	NO	9.59	Y	2.26
	secrecy	sec_t_Kcg	NO	9.81	Y	0.11
	secrecy	sec_t_Kcs	NO	9.81	Y	0.09
Kerb-preauth	auth	n1	NO	0.54	Y	0.04
	auth	n2	NO	0.56	Y	0.33

continued on next page

Legend:

YES	a known attack has been found
$\boxed{\text{YES}}$	a new 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
MO	memory out
TO	time-out

Problem			Atk	Backends	
Protocol	property	on		ofmc	cl-atse
	auth	t0	NO	0.51	MO
	auth	t1	NO	0.54	MO
	auth	t2a	NO	0.55	Y 0.34
	auth	t2b	NO	0.55	MO
	secrecy	sec_a_Kcg	NO	0.57	MO
	secrecy	sec_c_Kcg	NO	0.54	MO
	secrecy	sec_c_Kcs	NO	0.52	MO
	secrecy	sec_s_Kcs	NO	0.53	Y 0.33
	secrecy	sec_t_Kcg	NO	0.54	Y 0.07
	secrecy	sec_t_Kcs	NO	0.55	Y 0.07
Kerb-PKINIT	auth	n1	NO	0.40	0.18
	auth	n2	NO	0.41	Y 0.05
	auth	t0	NO	0.37	0.19
	auth	t1	NO	0.39	0.18
	auth	t2a	NO	0.39	0.22
	auth	t2b	NO	0.41	0.16
	secrecy	sec_a_Kcg	NO	0.39	0.20
	secrecy	sec_c_Kcg	NO	0.41	0.17
	secrecy	sec_c_Kcs	NO	0.39	0.18
	secrecy	sec_s_Kcs	NO	0.36	0.16
	secrecy	sec_t_Kcg	NO	0.38	0.16
	secrecy	sec_t_Kcs	NO	0.40	0.18
CRAM-MD5	auth	auth	NO	0.87	0.10
	secrecy	sec_SK	NO	0.78	0.04
PBK	auth	msg	YES	0.35	0.01
PBK-fix	auth	msg	YES	0.12	0.03
PBK-fix-weak-auth	wauth	msg	NO	4.26	0.50
hip	auth	initiator_responder_r2	NO	0.64	0.17
	secrecy	hash_dh	NO	0.61	0.20

continued on next page

Legend:

YES	a known attack has been found
$\boxed{\text{YES}}$	a new 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
MO	memory out
TO	time-out

Problem			Atk	Backends	
Protocol	property	on		ofmc	cl-atse
DHCP-delayed-auth	auth	sig	NO	0.07	0.02
	secrecy	sec_k	NO	0.06	0.02
lipkey-spkm-known-initiator	auth	k	NO	0.16	0.11
	auth	ktrgtint	NO	0.15	0.05
	secrecy	sec_i_Log	NO	0.14	0.05
	secrecy	sec_i_Pwd	NO	0.13	0.05
	secrecy	sec_t_Log	NO	0.14	0.06
	secrecy	sec_t_Pwd	NO	0.14	0.04
lipkey-spkm-unknown-initiator	auth	k	NO	3.87	0.71
	secrecy	sec_i_Log	NO	3.64	0.23
	secrecy	sec_i_Pwd	NO	3.71	0.24
	secrecy	sec_t_Log	NO	4.22	0.24
	secrecy	sec_t_Pwd	NO	3.45	0.02
TSIG	wauth	client_server_k_ba	NO	0.17	0.06
	wauth	server_client_k_ab	NO	0.16	0.02
ASW	auth	no	NO	0.43	1.06
	auth	nr	NO	0.43	1.23
	secrecy	no_secret	NO	0.46	1.01
ASW-abort	auth	no	NO	5.74	3.62
	auth	nr	NO	5.29	3.69
	secrecy	no_secret	NO	5.11	3.88
	secrecy	secret_ref	YES	3.54	19.86
FairZG	wauth	alice_bob_nrr	NO	8.02	0.15
	wauth	alice_server_con	NO	7.88	0.14
	wauth	bob_alice_nro	NO	8.02	0.90
	wauth	bob_alice_sub	NO	7.98	0.32
	wauth	bob_server_con	NO	7.93	0.21
SET-purchase	auth	deal		TO	Y 26.23
	secrecy	order		TO	MO
continued on next page					

Legend:

YES	a known attack has been found
$\boxed{\text{YES}}$	a new 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
MO	memory out
TO	time-out

Problem			Atk	Backends	
Protocol	**property**	**on**		**ofmc**	**cl-atse**
	secrecy	payment	$\boxed{\text{YES}}$	0.99	0.30
	wauth	deal	$\boxed{\text{YES}}$	1.90	246.97
SET-P-honest-payment-gateway	auth	deal	NO	0.98	TO
	secrecy	order	NO	0.88	TO
	secrecy	payment	NO	0.89	TO
	wauth	deal	NO	0.99	TO
AAAMobileIP	secrecy	secFAHA	NO	0.14	0.02
	secrecy	secFAMN	NO	0.16	0.03
	secrecy	secMNHA	NO	0.16	0.03
	wauth	k_faha1	NO	0.17	0.03
	wauth	k_faha2	NO	0.15	0.02
	wauth	k_mnfa1	NO	0.14	0.04
	wauth	k_mnfa2	YES	0.03	0.02
	wauth	k_mnha1	NO	0.17	0.02
	wauth	k_mnha2	YES	0.05	0.04
h.530	auth	key		TO	Y 93.73
	auth	key1	$\boxed{\text{YES}}$	0.63	TO
	secrecy	sec_m_Key		TO	Y 93.12
	secrecy	sec_v_Key	$\boxed{\text{YES}}$	0.61	TO
h.530-fix	auth	key	NO	1293.86	TO
	auth	key1	NO	1293.67	TO
	secrecy	sec_m_Key	NO	1290.70	TO
	secrecy	sec_v_Key	NO	1287.34	TO
Simple	secrecy	presenceinfo	NO	83.48	13.10
	wauth	ps_wr_user	NO	84.01	12.90
	wauth	wr_ps_presenceinfo	NO	85.23	280.85
CTP-non_predictive-fix	auth	npaa_pac_nnpaa	NO	0.21	Y 0.03
	auth	ppaa_pac_ip_pac	NO	0.22	0.06
	secrecy	mac_key	NO	0.21	Y 0.07

continued on next page

Legend:

YES	a known attack has been found
$\boxed{\text{YES}}$	a new 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
MO	memory out
TO	time-out

Problem			Atk	Backends	
Protocol	**property**	**on**		**ofmc**	**cl-atse**
geopriv	auth	lr_mu_n_lr	NO	0.30	Y 0.04
	secrecy	filtered_loc	NO	0.30	0.09
	secrecy	k_psi	NO	0.27	0.05
	secrecy	psi	NO	0.29	0.04
	wauth	ls_mu_psi	NO	0.28	0.04
pervasive	auth	lbs_t_n_lbs	NO	67.63	127.76
	secrecy	loc	NO	66.87	56.62
two_pseudonyms	auth	lr_t_n_lr	NO	0.41	4.08
	secrecy	filtered_loc	NO	0.40	4.06
	secrecy	loc	NO	0.36	4.12
	secrecy	psi_lr	NO	0.38	4.07
	secrecy	psi_t	NO	0.39	4.04
QoS-NSLP	wauth	router_server_clientid	NO	47.71	79.09
	wauth	server_client_service	NO	49.46	42.00
sip	auth	y	NO	4.05	0.07

Legend:

YES	a known attack has been found
$\boxed{\text{YES}}$	a new 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
MO	memory out
TO	time-out

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] N. Asokan, V. Shoup, and M. Waidner. Asynchronous protocols for optimistic fair exchange. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 86–99, 1998.

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

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

[6] AVISPA. Deliverable 6.2: Specification of the Problems in the High Level Protocol Specification Language. Available at `http://www.avispa-project.org/publications.html`, 2004.

[7] AVISPA. Deliverable 7.3: Assessment of the AVISPA tool v.2. Available at `http://www.avispa-project.org`, 2004.

[8] 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`.

[9] G. Bella, F. Massacci, and L. C. Paulson. Verifying the SET Purchase Protocols. Technical Report 524, University of Cambridge, November 2001. URL: `http://www.cl.cam.ac.uk/Research/Reports/TR524-lcp-purchase.pdf`.

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

[11] 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.

[12] J. Bournelle, M. Laurent-Maknavicius, H. Tschofenig, and Y. E. Mghazli. Handover-aware access control mechanism: Ctp for pana. In *ECUMN*, pages 430–439, 2004.

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

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

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

[16] J. Cuellar, J. Morris, D. Mulligan, J. Peterson, and J.Polk. RFC 3693: Geopriv requirements, 2004. `http://www.faqs.org/rfcs/rfc3693.html`.

[17] S. V. den Bosch, G. Karagiannis, and A. McDonald. NSLP for Quality-of-Service signalling, Feb. 2005. `http://www.ietf.org/internet-drafts/draft-ietf-nsis-qos-nslp-06.txt`, Work in Progress.

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

[19] 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.

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

[21] D. Eastlake 3rd. RFC 2137: Secure Domain Name System Dynamic Update, Apr. 1997. Status: Proposed Standard.

[22] D. Eastlake 3rd. RFC 2930: Secret Key Establishment for DNS (TKEY RR), Sept. 2000. Status: Proposed Standard.

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

[24] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, and L. Stewart. RFC 2617: HTTP Authentication: Basic and Digest Access Authentication, June 1999. Status: Draft Standard.

[25] M. Garcia-Martin, M. Belinchon, M. Pallares-Lopez, C. Canales, and K. Tammi. Diameter Session Initiation Protocol (SIP) Application, Mar. 2005. Work in Progress.

[26] P. Hankes Drielsma and S. Mödersheim. The ASW protocol revisited: A unified view. In *Proceedings of the IJCAR04 Workshop ARSPA*, 2004. To appear in ENTCS, available at `http://www.avispa-project.org`.

[27] 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.

[28] 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.

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

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

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

[32] 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.

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

[34] C. Jennings, J. Peterson, and M. Watson. RFC 3325: Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks, Nov. 2002. Status: Informational.

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

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

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

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

[39] Mastercard and VISA. SET Secure Electronic Transaction Specification, May 1977.

[40] 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.

[41] 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.

[42] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson. Host Identity Protocol, June 2005. Work in Progress.

[43] 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-clarific%ations-07.txt`, Work in Progress.

[44] A. B. Roach. RFC 3265: Session Initiation Protocol (SIP)-Specific Event Notification, June 2002. Status: Proposed Standard.

[45] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. RFC 3261: SIP: Session Initiation Protocol, June 2002. Status: Proposed Standard.

[46] V. Shmatikov and J. C. Mitchell. Analysis of a fair exchange protocol. In *Proceedings of the 1999 FLoC Workshop on Formal Methods and Security Protocols*, Trento, Italy, 1999.

[47] V. Shmatikov and J. C. Mitchell. Finite-state analysis of two contract signing protocols. *Theoretical Computer Science*, 283(2):419–450, 2002.

[48] 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.

[49] P. Vixie, O. Gudmundsson, D. Eastlake 3rd, and B. Wellington. RFC 2845: Secret Key Transaction Authentication for DNS (TSIG), May 2000. Status: Proposed Standard.

[50] B. Wellington. RFC 3007: Secure Domain Name System (DNS) Dynamic Update, Nov. 2000. Status: Proposed Standard.

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

[52] J. Zhou and D. Gollmann. A fair non-repudiation protocol. In *Proc. of the 15th IEEE Symposium on Security and Privacy*, pages 55–61. IEEE Computer Society Press, 1996.

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