Epistemic and Temporal Epistemic Logics of Authentication

Sharar Ahmadi

University of York

12th Feb, 2019

Table of Contents

- The principals in a network need to be assured that they are communicating with the intended principals.
- Authentication protocols are some rules based on cryptography.
- Attacker capabilities (Dolev-Yao Definition):
  - An attacker can eavesdrop all communications.
  - It can drop messages.
  - It can change messages.
  - It can perform cryptographic operations using his known keys and messages.
  - It can replay messages.
  - It can impersonate authorized principals.
- Successful attacks on authentication ptotocols
- We abstract away cryptography algorithms and implemention
- Target: Logical behaviour
- Approach: Formal analysis of authentication protocols.

- Logics of Authentication
- Epistemic logic —- Modal logic

  axiom K: $(\phi \rightarrow \ \psi) \rightarrow (\Box\phi \rightarrow \ \Box\psi)$ *Necessitation* : $\dfrac{\phi}{\Box\phi}$

- The standard Kripke semantics results in logical omniscience.

  1. A *receives* $\{m\}_k \rightarrow$ *exists* m (intuitive axiom)
  2. $K_B(A$ *receives* $\{m\}_k \rightarrow$ *exists* $m)$ (1, Neccessitation)
  3. K_B A *receives* $\{m\}_k \rightarrow K_B$ *exists* m (2, Axiom K)
  4. K_B A *receives* $\{m\}_k$ (Assumption: Anonymity fails)
  5. K_B *exists* $\{m\}_k$ (3, 4, Modus ponens)

- Preventing logical omniscience:
  - Weakening Necessitation rule (Counterpart theory)
  - Providing explicit model for Knowledge (Algorithmic Knowledge)

- Epistemic and temporal epistemic logics have significantly improved the analysis of authentication protocols.

- An attack may be detected by an omniscience-free logic while it is ignored by another logic that is not omniscience-free.
- A protocol can be specified by a temporal epistemic logic while it cannot be specified by an epistemic logic.
- The expected properties:
  - Soundness
  - Compeleteness
  - Dealing with logical Omniscience
  - Temporal modalities
  - Knowledge modalities
  - Modeling Powerful attackers (Dolev-Yao Definitions)

NSPK protocol	**man-in-the-middle attack**
$A \rightarrow B : \{n_a.A\}_{pk(B)}$	1. $A \rightarrow I : \{n_a, A\}_{pk(I)}$
$B \rightarrow A : \{n_a.n_b\}_{pk(A)}$	$1'$. $I(A) \rightarrow B : \{n_a, A\}_{pk(B)}$
$A \rightarrow B : \{n_b\}_{pk(B)}$	$2'$. $B \rightarrow I(A) : \{n_a, n_b\}_{pk(A)}$
	2. $I \rightarrow A : \{n_a, n_b\}_{pk(A)}$
	3. $A \rightarrow I : \{n_b\}_{pk(I)}$
	$3'$. $I(A) \rightarrow B : \{n_b\}_{pk(B)}$

Example: A variant of a stream authentication protocol TESLA.
Mode: [(u,v),d], where $u, v, d \in N$ and $d \neq 0$.
Sequence of messages: $m_1,\ m_2,\ m_3, \ldots, m_i,\ m_{i+1}, \ldots$.
d: time interval between sending m_i and m_{i+1}.
send: t => receive: [t+u, t+v]
If $v \geq d$, the protocol is vulnerable to an attack.

$$
\begin{array}{ll}
\mathbf{P_{00}}: & R \rightarrow S : n_r \\
\mathbf{P_{01}}: & S \rightarrow R : \{f(k_1).n_r\}_{pr_s} \\
\mathbf{P_1}: & S \rightarrow R : \{m_1\}_{k_s}.f(k_2).mac\big(g(k_1), \{m_1\}_{k_s}.f(k_2)\big) \\
\mathbf{P_2}: & S \rightarrow R : \{m_2\}_{k_s}.f(k_3).k_1.mac\big(g(k_2), \{m_2\}_{k_s}.f(k_3).k_1\big) \\
\mathbf{P_3}: & S \rightarrow R : \{m_3\}_{k_s}.f(k_4).k_2.mac\big(g(k_3), \{m_3\}_{k_s}.f(k_4).k_2\big) \\
\vdots & \\
\mathbf{P_{i-1}}: & S \rightarrow R : \{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}.mac\big(g(k_{i-1}), \{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}\big) \\
\mathbf{P_i}: & S \rightarrow R : \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}.mac\big(g(k_i), \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}\big) \\
\mathbf{P_{i+1}}: & S \rightarrow R : \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i.mac\big(g(k_{i+1}), \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i\big) \\
\vdots &
\end{array}
$$

$\mathbf{h_1}$:

$\vdots$

$S\ snd\ \{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}.mac\big(g(k_{i-1}), \{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}\big),$

$R\ rcv\ \{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}.mac\big(g(k_{i-1}), \{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}\big),$

$S\ snd\ \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}.mac\big(g(k_i), \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}\big),$

$R\ rcv\ \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}.mac\big(g(k_i), \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}\big),$

$S\ snd\ \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i.mac\big(g(k_{i+1}), \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i\big),$

$R\ rcv\ \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i.mac\big(g(k_{i+1}), \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i\big),$

$\vdots$

$\mathbf{h_2}$:

$\vdots$

$S\ snd\ \{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}.mac\big(g(k_{i-1}),\{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}\big),$

$R\ rcv\ \{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}.mac\big(g(k_{i-1}),\{m_{i-1}\}_{k_s}.f(k_i).k_{i-2}\big),$

$S\ snd\ \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}.mac\big(g(k_i),\{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}\big),$

$C(R)\ rcv\ \{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}.mac\big(g(k_i),\{m_i\}_{k_s}.f(k_{i+1}).k_{i-1}\big),$

$S\ snd\ \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i.mac\big(g(k_{i+1}),\{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i\big),$

$C(R)\ rcv\ \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i.mac\big(g(k_{i+1}),\{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i\big),$

$C(S)\ snd\ \{m'_i\}_{k_c}.f(k_{i+1}).k_{i-1}.mac\big(g(k_i),\{m'_i\}_{k_c}.f(k_{i+1}).k_{i-1}\big),$

$R\ rcv\ \{m'_i\}_{k_c}.f(k_{i+1}).k_{i-1}.mac\big(g(k_i).\{m'_i\}_{k_c}.f(k_{i+1}).k_{i-1}\big),$

$C(S)\ snd\ \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i.mac\big(g(k_{i+1}),\{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i\big),$

$R\ rcv\ \{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i.mac\big(g(k_{i+1}),\{m_{i+1}\}_{k_s}.f(k_{i+2}).k_i\big),$

$\vdots$

- The model of a protocol: The set of all possible runs of that protocol
- We formalize the authentication goal as follows:
  $R\ rcvd\ P_i \rightarrow K_R\ S\ snt\ P_i$

Proof (According to standard Kripke semantics):

- $h_1 \models R\ rcvd\ P_i \rightarrow K_R\ S\ snt\ P_i$
- Assume that $h_1 \models R\ rcvd\ P_i$, We need to prove $h_1 \models K_R\ S\ snt\ P_i$.
- $h_1 \models K_R\ S\ snt\ P_i$ iff for every h which is indistinguishable from h_1 in $R's$ view, $h \models S\ snt\ P_i$
- Let $h = h2$ ($\{m_i\}_{k_s}$ is indistinguishable from $\{m'_i\}_{k_c}$ with respect to $R's$ view because R does not know the keys k_c and k_s.)
- $h_2 \not\models S\ snt\ P_i$
- $h_1 \not\models R\ rcvd\ P_i \rightarrow K_R\ S\ snt\ P_i$

Proof (According to Counterpart theory):

- $h_1 \models K_R\ S\ snt\ P_i$ iff for every h which is indistinguishable from h_1 in $R's$ view, $h \models S\ snt\ \rho(P_i)$
- $h2$ cannot be a counter example ($\rho(\{m_i\}_{k_s}) = \{m'_i\}_{k_c}$).

- The formal analysis of a protocol using epistemic logics depends on the knowledge gained by the principals executing that protocol.
- The propositional knowledge is implicit and does not care about the details of computation.
- A principal i knows a formula ϕ implicitly ($K_i\phi$), if i knows that ϕ is true.
- Alternative: Algorithmic knowledge
- If a principal has some bit strings, he can apply cryptographic operators to compute more strings using some predefined algorithms.
- A trust theory for a protocol
- A model that respects the Dolev-Yao indistinguishability relation.
- Two messages are Dolev-Yao indistinguishable if any test - based on a limited set of operations on messages - gives the same result about the configuration of those messages. => computational soundness

- A proof system X consists of some axioms and rules.
- The axioms are valid with respect to the semantics.
- The rules preserve validity.
- X is logically sound if every derivable formula ϕ in X is valid.
- X is complete if every valid formula ϕ is provable in X.
- Logical soundness is based on formal models.
- Computational soundness: If a message can be derived formally, it can also be computed in the computational model.
- Logical soundness and completeness => A strong intuition that the formal semantics is working as expected.

- Fusion:
  - Epistemic and Temporal modalities appear in each other's scope
  - $K_A \bigcirc B \ rcvd \ \{m\}_k$ *vs.* $\bigcirc K_A \ B \ rcvd \ \{m\}_k$
  - There can be Interactions between time and knowledge (axioms and rules).

- Temporalization:
  - Temporal modalities are not allowed to appear in the scope of Epistemic modalities.

- Fibring:
  - Epistemic and Temporal modalities appear in each other's scope.
  - There are no interactions between time and knowledge (axioms and rules).
  - Soundness and Completeness of the fibred logic can be proven based on soundness and completeness of the constituent logics.

Logic	Order	Operators	Proof system/tool	S	C	O-f	Attacke
BAN (1989)	PR	E	proof system	–	–	×	Implicit
GNY (1990)	PR	E	proof system	–	–	×	Implicit
AT (1991)	PR	E	proof system	✓	×	×	Implicit
T-BAN (1993)	PR	E/T	proof system	✓	×	×	Implicit
VO (1993)	PR	E	proof system	–	–	×	Implicit
SVO (1993)	PR	E	proof system	✓	×	×	Implicit
L_n^{KX} (2003)	PR	E/A	knowledge algorithm	–	–	EXP	Explicit
KL_n (2004)	FO	E/T	resolution	–	–	×	Explicit
TML+ (2004)	FO	E/T	tableau	✓	✓	×	Implicit
WS5 (2005)	PR	E	proof system	✓	✓	✓	Implict
TDL (2006)	FO	E/A/T	proof system	✓	✓	EXP	Explicit
FL (2006)	FO	E/T	KEM prover	✓	✓	×	Implicit
FWS5 (2007)	FO	E	proof system	✓	✓	✓	Implicit
$ECKL_n$ (2009)	FO	E/T	MCTK	–	–	×	Explicit
CTLK (2009)	FO	E/T	MCMAS	–	–	×	Explicit
CTLS5 (2010)	FO	E/T	MCMAS	–	–	×	Explicit
CTLKR (2012)	FO	E/T	MCMAS-E	–	–	×	Explicit
TBL (2012)	FO	E/T	proof system	✓	✓	×	Implicit
ICTLK (2016)	FO	E/T	MCMAS-S	–	–	×	Explicit
TWS5 (2017)	PR	E/T	proof system	✓	✓	✓	Implicit

- Soundness
- Computational Soundness
- Attacker model
- Explicit Knowledge and Implicit Knowledge
- Completeness
- Logical Omniscience
- Expressiveness
- Provers and Model checkers
- Decidability
- Complexity

- I. Boureanu, M. Cohen, and A. Lomuscio. Automatic verification of temporal epistemic properties of cryptographic protocols. Journal of Applied Non-Classical Logics, 19(4): 463-487, Taylor & Francis, 2009.
- A. Lomuscio and B. Wozna. A complete and decidable security-specialized logic and its applications to the TESLA protocol. In Proceedings of the 5th international joint conference on Autonomous agents and multiagent systems, pages 145-152. ACM, 2006.
- S. Ahmadi and M.S.Fallah. An omniscience-free temporal logic of knowledge for verifying authentication protocols. Bulletin of the Iranian Mathematical Society, pages 1-23, Springer, 2018.
- S. Ahmadi, M.S. Fallah and M. Pourmahdian. On the properties of Epistemic and Temporal Epistemic Logics of Authentication. Informatica: An International Journal of Computing and Informatics (To appear).