An Authentication Logic Supporting Synchronization, Revocation, and Recency

Stuart Stubblebine
Rebecca Wright

AT&T Research

CCS ’96
15 March, 1996
MOTIVATION

- Distributed systems involve dynamic changes to security attributes.

- Participants must act on beliefs that may or may not be currently true.

- There may be a wide range of policies for extension and revocation of beliefs.

- Such policies are dependent on timing and synchronization.
AUTHENTICATION LOGICS

- Published cryptographic protocols are often wrong.

- Authentication logics ([BAN], [AT], [GNY], [Syv], [SvO], ...) can be helpful for analyzing cryptographic protocols.

- Existing logics have limited ability to reason about time and about revocation of beliefs.
OUR LOGIC

• allows for arbitrary granularity of time.

• allows revocation of keys, jurisdictions, and beliefs.

• is very strict about extending beliefs from one time to another

  beliefs are extended according to specified policies

• analyzes a protocol together with belief-extension policies.
MESSAGES

- all public keys, private keys, shared keys, times, principals, and constants

- all formulas

- \{X\}_K, \ [X]_K, \ (X_1, \ldots, X_k)
FORMULAS

• primitive propositions

• $\neg \varphi$ and $\varphi \land \psi$

• $t_1 \leq t_2$ and $t_1 \geq t_2$

• $(\exists t \geq t')\varphi$ and $(\exists t \leq t')\varphi$

• $(\forall t \geq t')\varphi$ and $(\forall t \leq t')\varphi$
• $P \text{ believes}_t \varphi$
  $P \text{ believes}_{[t_1,t_2]} \varphi$
  $P \text{ believes}_{\langle t_1,t_2 \rangle} \varphi$
  $P \text{ believes}_{t,Q} \varphi$
  $P \text{ believes}_{[t_1,t_2],Q} \varphi$
  $P \text{ believes}_{\langle t_1,t_2 \rangle,Q} \varphi$

• $P \text{ controls}_t \varphi$
  $P \text{ received}_t X$
  $P \text{ said}_t X$
  $P \text{ says}_t X$
  $P \text{ has}_t K$
  $fresh_{t,P} X$

• $P \xleftarrow{K} t Q$
  $\xrightarrow{K} t P$
  $\xrightarrow{K} t P$

• $\text{sync}_{t,e} (P, Q)$

• $\varphi \text{ at}_P t$
AXIOMS

- monotonicity of time
  \[ P \text{ said}_t X \land t' \geq t \supset P \text{ said}_{t'} X \]

- synchronization between principals
  \[ \varphi \text{ at}_P t \land \text{ sync}_{t,\epsilon} (P, Q) \supset \varphi \text{ at}_Q (t - \epsilon, t + \epsilon) \]

- originator identification
  \[ K \Rightarrow_{t, P} Q \land P \text{ received}_t [X]_{K-1} \supset Q \text{ said}_{t, P} X \land Q \text{ said}_{t, P} [X]_{K-1} \land Q \text{ has}_{t, P} K^{-1} \]

- nonce verification
  \[ \text{fresh}_{t_1, P} X \land P \text{ said}_{t_2} X \supset P \text{ says}_{\langle t_1, t_2 \rangle} X \]
BELIEF-EXTENSION POLICIES

• Stable beliefs

$$P \text{ believes}_t \varphi \land (t \leq t') \supset P \text{ believes}_{t'} \varphi$$

• Believe if recent

$$P \text{ believes}_t \varphi \text{ at}_P t' \land (t' \leq t \leq \hat{t} \leq \delta + t'') \supset P \text{ still-believes}_{\tilde{t}} \varphi \text{ at}_P \hat{t}$$

• Believe until revoked

$$P \text{ believes}_t \varphi \text{ at}_P t' \land (t' \leq t \leq t'') \land$$
$$(\forall \hat{t} : t' \leq \hat{t} \leq t'') \neg(P \text{ believes}_{t''} ((\neg \varphi) \text{ at}_P \hat{t})) \supset$$
$$P \text{ still-believes}_{t''} \varphi \text{ at}_P t''$$
INFERENCE RULES

- Modus Ponens

  From $\varphi$ and $\varphi \supset \psi$ infer $\psi$.

- Necessitation

  From any theorem $\varphi$, infer $P \ believes_t \ \varphi.$
ANALYSIS

- idealize the protocol

- list initial assumptions, including policy assumptions

- use Modus Ponens and Necessitation to infer goals
AN EXAMPLE

PROTOCOL

Message 1 \[ S \rightarrow P : [Q, K_Q, s_Q, t_b, t_e, t_s]_{K_S^{-1}} \]

Message 2 \[ S \rightarrow P : [t, s_Q]_{K_S^{-1}} \]

IDEALIZATION

Message 1 \[ S \rightarrow_{t_1} P : [S \text{ says}_{t_s} K_Q [t_b, t_e], S Q]_{K_S^{-1}} \]

Message 2 \[ S \rightarrow_{t_2} P : [S \text{ says}_t K_Q [t_b, t_e], S Q]_{K_S^{-1}} \]
Assuming a believe-until-revoked policy, logic allows us to deduce:

\[ P \text{ believes}_{t_1} \xrightarrow{K_Q} [t_b,t_c],S \ Q \ at_P \ [t_s - \epsilon,t_s + \epsilon] \]

but not:

\[ P \text{ believes}_{t_3} \xrightarrow{K_Q} [t_b,t_c],S \ Q \ at_P \ t_3 \]
SEMANTICS

- We provide a semantics for our logic. closely based on semantics of [Abadi, Tuttle] and [Syverson, van Oorschot]

- Our logic is sound with respect to this semantics.
CONCLUSIONS

• Our logic supports reasoning about synchronization, recency, and revocation.

• Additional complexity is justified by increase in ability to analyze practical systems.

• The ability to reason about the conjunction of policies and protocols will be important as public and private key infrastructures are deployed and new, unanticipated policies are put into use.