The meanings of knowing, believing and ability of checking in protocols for e-commerce

Peeter Laud
peeter_l@ut.ee

Tartu Ülikool
Cybernetica AS
Non-repudiation

If Alice said $M$ to Bob, then

- Bob can convince himself that it really was Alice who said $M$.
- Bob is able to convince other people (for example, the judge) that Alice said $M$. 
Integrity and Checkability

Integrity:
- A party wants to be sure the other party cannot do anything bad.
- More generally, the party wants to be sure that no unacceptable set of circumstances can occur.

Checkability:
- The party wants to be sure, that if an unacceptable set of circumstances occurs, then
  - he is able to recognize that it occurred;
  - he can convince others that it occurred;
  - he can show that there was someone else who did not fulfill his obligations.
State of the art

The existing protocol logics allow to express,
- what the parties see, say, receive, generate, know;
- which keys are good keys;
- what one party can prove to another party.

They do not allow to express
- the beliefs of parties;
- the checkability of arbitrary formulae and the convincing communicability of the results of these checks.
Structure of the talk

- Messages and formulae.
- The set of protocol runs.
- Semantics of some constructs.
- Expressing some nice protocol properties.
- Some axioms.
- Conclusions and future work.
Protocols — the necessary sets

We have

- The set of parties Agent.
- The set of symmetric keys Key.
- The set of asymmetric keys (for both encryption and signing) PSK.
  - We denote the key pair by $K$, public and secret parts by $K^+$ and $K^-$, respectively.
- The set of messages $M$.
- The set of formulae $\Phi$.
- The set of actions $A$.
- The set of protocol runs $R$. 
The messages $M$ are one of

- atomic messages;
- keys (from Key or PSK), nonces (from the set Nonce);
- pairs $(M_1, M_2)$;
- encryptions $\{M\}_K$ or $\{M\}_{K^+}$;
- signed messages $[M]_{K^-}$;
  - we assume that $M$ can be found from $[M]_{K^-}$
- message digests $H(M)$;
- formulae $\varphi \in \Phi$. 
The formulae (1/3)

The formulae $\varphi, \psi$ are one of

- the atomic formulae;
- $\neg \varphi, \varphi \land \psi, \varphi \lor \psi, \varphi \rightarrow \psi$, false, true;
- $\text{said}(P, M) — \text{agent } P \text{ has sent a message containing } M \text{ and } P \text{ was aware that it contained } M$;
- $\text{sees}(P, M) — \text{agent } P \text{ can construct the message } M \text{ from the messages it has generated or received}$;
- $\text{received}(P, M) — \text{agent } P \text{ has received the message } M \text{ or some supermessage of it}$;
- $\text{sees}(P, M) \land \neg \text{received}(P, M) \text{ means that } P \text{ has generated } M \text{ himself.}$
The formulae (2/3)

- \( e^{K^+} P, s^{K^+} P, P \leftrightarrow^K Q \) — the key \( K^+ \) is the public encryption/signature key of \( P \) or \( K \) is a symmetric key known only by \( P \) and \( Q \);

- \( M_1 = M_2, \ Vfy(M_{\text{sig}}, K^+, M_{\text{txt}}) \) — equality of messages and the correctness of a signature;

- \( \varphi S \psi \) and \( \varphi U \psi \) — the temporal connectives “since” and “until”;
  - \( \lozenge \varphi \) and \( \square \varphi \) are defined in terms of \( U \).
  - \( \lozenge \varphi \) and \( \square \varphi \) are defined in terms of \( S \).

- \( A \varphi \) and \( E \varphi \) — \( \varphi \) holds in all possible futures / in at least one of them;

- \( \text{right}_P \) — whenever the agent \( P \) has said \( \varphi \), the formula \( \varphi \) has been correct;
The formulae (3/3)

- $\mathcal{K}_P\varphi$ — agent $P$ knows that $\varphi$ holds — in all worlds that $P$ may consider himself to be (according to his knowledge), $\varphi$ holds;

- $\mathcal{B}_P\varphi$ — agent $P$ believes that $\varphi$ holds — $\varphi$ holds in all of the above worlds that $P$ considers the most probable;

- $\mathcal{M}_P\varphi$ — $P$ can make sure that $\varphi$ holds.
The actions

An action is one of

- \[ \text{Send}_P(M, Q), \text{ where } Q \subseteq \text{Agent}. \text{ The agent } P \text{ has sent out a message } M \text{ meant for principals in } Q. \]
  - \[ M \] may not contain the statements \[ \text{right}_R. \]
  - Otherwise the interpretation of formulae is not well-defined.

- \[ \text{Recv}_P(M). \text{ Denotes that } P \text{ received the message } M. \]
  - All sent messages are eventually received by their intended recipients.

- \[ \text{Generate}_P(M) \] denotes that \[ P \] generated a new message \[ M \] (either a key(pair) or a nonce).
The protocol runs

The protocol runs are mappings from time moments to (sets of) actions.

$$\mathcal{R} = \mathbb{T} \rightarrow \mathcal{A}_{\perp}$$

Here $\mathbb{T}$ is the set of time moments. We identify it with the set of positive real numbers. $\perp$ means that no action occurs.

Moreover, for a run $r \in \mathcal{R}$:

- for all $t \in \mathbb{T}$, the set of moments $t' \leq t$, where $r(t') \neq \perp$, is finite;
- if an agent $P$ sends a message $M$ at a certain moment, then he must see that message at that moment.
Semantics

We define the relation

$$(r, t) \models \varphi$$

where \( r \in \mathcal{R}, t \in \mathcal{T}, \varphi \in \Phi. \)
Semantics — seeing

- $P$ can see the messages it has generated or received (or knows at the beginning of time).

- Generally, $P$ can see the submessages of a message. But
  - to see the submessage $M$ of $\{M\}_K$, $P$ has to see $K$;
  - to see $M$ in $\{M\}_{K^+}$, $P$ has to see $K^-$;
  - from just $H(M)$, $P$ cannot find $M$.

- $P$ can construct new messages from the ones it sees.

This defines, whether $(r, t) \models sees(P, M)$ holds.

$(r, t) \models received(P, M)$, if $P$ can see $M$ as a submessage of a message that it has received.
Semantics — saying and being right

$(r, t) \models said(P, M)$ if $P$ has sent out a message $M'$ at a
time moment $t' \leq t$ and $P$ could see that $M$ was a
submessage of $M'$ at that time.

$(r, t) \models right_P$ if for all formulae $\varphi$ that $P$ has said at
some time $t' \leq t$ (and has understood that he said that),
$(r, t') \models \varphi$. 
Suppose an agent $P$ sees a set of messages $\mathcal{M}$. For some $M \in \mathcal{M}$, $P$ does generally not see the structure of $M$ “all the way through”, because he does not have all the necessary decryption keys.

For $\mathcal{M}$ and $M \in \mathcal{M}$ corresponds a “message with holes” $M'$.

$P$’s view is the set of $\text{Sends}$, $\text{Recvs}$ and $\text{Generates}$ that $P$ has done, together with their times, but the messages are replaced with corresponding messages with holes.

$r \sim^t_P r'$, if the views of $P$ in $r$ and $r'$ at time $t$ are equal (up to $\alpha$-conversion).

$\sim^t_P$ is an equivalence relation.

$(r, t) \models \mathcal{K}_P \varphi$ if $(r', t) \models \varphi_\alpha$ for all $r'$ where $r \sim^t_P r'$. 
Semantics — believing

Let $\text{TTP} \subseteq \text{Agent}$ be the set of trusted parties.

- $\sim^t_P$ defines a partitioning of $\mathcal{R}$. Let $r/\sim^t_P$ be the part containing $r$.

- $(r, t) \models \mathcal{B}_P \varphi$, if $(r', t) \models \varphi$ for the most likely elements $r'$ of $r/\sim^t_P$.

- A partial order “more likely than” is defined on $r/\sim^t_P$.

- This order must be some refinement of the order $\supseteq$ on sets

$$\{ T \in \text{TTP} : (r', t) \models \text{right}_T \}$$

for $r' \in r/\sim^t_P$.

- We could also let the set $\text{TTP}$ be different for different agents, and let the agent change it over time.
What you know and what you believe

- An agent can know only statements that describe only his own circumstances or are derivable from them.
  - For example, what he sees.
  - If $P$ has sent $M$ to $Q$ then $P$ knows that $Q$ sees or eventually will see $M$.

- If an agent uses statements said by others to infer something, then the agent can only believe that.
  - For example, everything derived from statements made by trusted third parties is only believed in, not known.

- Most statements that we are interested in can only be believed, not known.

- “$P$ can prove $\varphi$ to $Q$” is formalized as $M_P \diamond B_Q \varphi$. 
Semantics — being able to make sure

\((r, t) \models M_P \varphi\) if there exists \(R \subseteq \mathcal{R}\), such that

- \(R \neq \emptyset\);
- \(r =_t r'\) for all \(r' \in R\);
- \(r =_t r'\) means that \(r(t') = r'(t')\) for all \(t' \leq t\).
- \((r', t) \models \varphi\) for all \(r' \in R\);
- if \(\dot{r} =_t r\) and \(\dot{r} \notin R\), then for all \(r' \in R\):
  
  Let \(t' \in T\) be minimal such, that \(r' \neq_t \dot{r}\). Then at least one of the following holds:
  - at least one of \(r'(t')\) and \(\dot{r}(t')\) is an action of the agent \(P\) (i.e. a Send or a Generate by \(P\));
  - there exists \(r'' \in R\), such that \(\dot{r} =_t r''\).
Semantics — $S$ and $U$, $A$ and $E$

1. $(r, t) \models \varphi U \psi$ if $(r, t') \models \psi$ for some $t' > t$ and for all $t''$, where $t < t'' < t'$, $(r, t'') \models \varphi$.

2. $(r, t) \models \varphi S \psi$ is defined similarly.

3. $\Diamond \varphi \equiv \text{true} U \varphi$.

4. $\Box \varphi \equiv \neg \Diamond \neg \varphi$.

5. $\Diamond \varphi \equiv \text{true} S \varphi$.

6. $\Box \varphi \equiv \neg \Diamond \neg \varphi$.

7. $(r, t) \models A \varphi$ if $(r', t) \models \varphi$ for all $r'$, where $r =_t r'$.

8. $E \varphi \equiv \neg A \neg \varphi$. 

Teooriapäevad Pedasel, 03-05.10.2003 – p.20/28
Some desirable protocol properties

**Fraud detection** Any interested party can detect and prove (to another party), whether a trusted party has committed any frauds.

**Anti-framing** An honest trusted party can explicitly disavow any false accusations against her.

The previous slide contained phrases
- ... party has committed any frauds ...
- ... an honest ... party ...

Generally, only parties that have done everything they have to do can expect to be covered by these statements on the previous slide.

How to model “have done everything they have to do”?

In general, we could just say that for each $P \in \text{Agent}$ there is a formula $D_P$ that is true iff $P$ “has done everything he has to do” so far.

We assume that $\neg D_P \rightarrow A \Box \neg D_P$ holds for all agents $P$. 

Teooriapäevad Pedasel, 03-05.10.2003 – p.22/28
Formalizing fraud detection

Possible formalizations of “if $Q$ has not fulfilled his duties, then $P$ can find that out / prove that to $R$”:

- $D_P \rightarrow \mathcal{M}_P(\neg D_Q \rightarrow \Box \mathcal{B}_P \neg D_Q)$
- $D_P \land D_R \rightarrow \mathcal{M}_P(\neg D_Q \rightarrow \Box \mathcal{B}_R \neg D_Q)$
Formalizing anti-framing

Possible formalizations of “if $Q$ thinks $P$ has not fulfilled his duties, but $P$ has, then $P$ can make $Q$ change his mind”:

\[
D_P \land D_Q \land B_Q \neg D_P \rightarrow M_P \Diamond \neg B_Q \neg D_P \\
D_P \land D_Q \land B_Q \neg D_P \rightarrow M_Q \Diamond M_P \Diamond \neg B_Q \neg D_P \\
D_P \land D_Q \land B_Q \neg D_P \rightarrow M_P M_Q \Diamond M_P \Diamond \neg B_Q \neg D_P \\
D_Q \land B_Q \neg D_P \rightarrow M_Q \Diamond (D_P \rightarrow M_P \Diamond \neg B_Q \neg D_P)
\]
Some axioms

\[ A(\varphi \rightarrow \psi) \rightarrow (\mathcal{M}_P \varphi \rightarrow \mathcal{M}_P \psi) \]

\[ \mathcal{M}_P \varphi \rightarrow \mathcal{M}_P \mathcal{M}_P \varphi \]

\[ A \varphi \rightarrow \mathcal{M}_P \varphi \]

\[ \mathcal{K}_P \Box \varphi \rightarrow \Box \mathcal{K}_P \Box \varphi \]

\[ sees(P, M) \rightarrow \mathcal{M}_P \Diamond sees(Q, M) \]

\[ said(P, \varphi) \land \text{right}_P \rightarrow \Diamond (said(P, \varphi) \land \varphi) \]

\[ \ldots \]

What axioms or inference rules are there for deriving \( B_{P \text{right}_T} \)?
Some axioms

\[ K_P(\varphi \rightarrow \psi) \rightarrow (K_P \varphi \rightarrow K_P \psi) \quad K_P \varphi \rightarrow A \varphi \]

\[ K_P \varphi \rightarrow K_P K_P \varphi \quad A \varphi \rightarrow \varphi \]

\[ \neg K_P \varphi \rightarrow K_P \neg K_P \varphi \quad K_P \varphi \rightarrow B_P \varphi \]

\[ B_P(\varphi \rightarrow \psi) \rightarrow (B_P \varphi \rightarrow B_P \psi) \quad B_P \varphi \rightarrow K_P B_P \varphi \]

\[ A(\varphi \rightarrow \psi) \rightarrow (A \varphi \rightarrow A \psi) \quad \neg B_P \varphi \rightarrow K_P \neg B_P \varphi \]

\[ A \varphi \rightarrow A A \varphi \quad \neg A \varphi \rightarrow A \neg A \varphi \]

etc.
Conclusions

- We have defined some quite expressive notions.
- We should try to model some real protocols with them.
  - There are quite a lot of premises to be modelled.
    - Agents do not lose their secret keys.
    - Servers are responsive.
- This may give us an “intuitively complete” set of axioms.
Future work

The explicit checking of the formulae should be added.

Currently, when an agent sees several messages, it is supposed to see right away, in what kind of relationship(s) they are.

There are protocols where some agent does not have to determine these relationships, although he is able to.

The “being able to make sure” should be extended to “knowing how to make sure”.

Tree-shaped semantical structures?

Timings.

...