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

The messages

The messages M are one of

- atomic messages;
- keys (from $\mathbf{Key}$ or $\mathbf{PSK}$), nonces (from the set $\mathbf{Nonce}$);
- 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 φ, ψ are one of

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

The formulae (2/3)

- $\mathbf{e} \xrightarrow{K^+} P$, $\mathbf{s} \xrightarrow{K^+} P$, $P \xleftrightarrow{K} Q$ — the key K^+ is the public encryption/signature key of P or K is a symmetric key known only by P and Q;
- $M_1 = M2$, Vfy$(M_{\text{sig}}, K^+, M_{\text{txt}})$ — equality of messages and the correctness of a signature;
- $\varphi\,\mathcal{S}\,\psi$ and $\varphi\,\mathcal{U}\,\psi$ — the temporal connectives “since” and “until”;
  - $\Diamond\varphi$ and $\Box\varphi$ are defined in terms of $\mathcal{U}$.
  - $\blacklozenge\varphi$ and $\blacksquare\varphi$ are defined in terms of $\mathcal{S}$.
- A φ and E φ — φ holds in all possible futures / in at least one of them;
- $right_P$ — whenever the agent P has said φ, the formula φ has been correct;

The formulae (3/3)

- $\mathcal{K}_P\varphi$ — agent P *knows* that φ holds — in all worlds that P may consider himself to be (according to his knowledge), φ holds;
- $\mathcal{B}_P\varphi$ — agent P *believes* that φ holds — φ holds in all of the above worlds that P considers the most probable;
- $\mathcal{M}_P\varphi$ — P can make sure that φ holds.

The actions

An action is one of

- $Send_P(M, \mathcal{Q})$, where $\mathcal{Q} \subseteq \mathbf{Agent}$. The agent P has sent out a message M meant for principals in $\mathcal{Q}$.
  - M may not contain the statements $right_R$.
    - Otherwise the interpretation of formulae is not well-defined.
- $Recv_P(M)$. Denotes that P received the message M.
  - All sent messages are eventually received by their intended recipients.
- $Generate_P(M)$ 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.

$$\mathcal{R} = \mathbf{T} \to \mathcal{A}_\perp$$

Here $\mathbf{T}$ 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 $t \in \mathbf{T}$, 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 $r \in \mathcal{R}$, $t \in \mathbf{T}$, $\varphi \in \Phi$.

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

- $(r, t) \vDash said(P, M)$ 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.
- $(r, t) \vDash right_P$ if for all formulae φ that P has said at some time $t' \leq t$ (and has understood that he said that), $(r, t') \vDash \varphi$.

Semantics — knowing

- Suppose an agent P sees a set of messages $\mathbf{M}$. For some $M \in \mathbf{M}$, P does generally not see the structure of M “all the way through”, because he does not have all the necessary decryption keys.
- For $\mathbf{M}$ and $M \in \mathbf{M}$ corresponds a “message with holes” M'.
- P’s view is the set of Sends, Recvs and $\mathit{Generate}$s that P has done, together with their times, but the messages are replaced with corresponding messages with holes.
- $r \sim_P^t r'$, if the views of P in r and r' at time t are equal (up to α-conversion).
  - $\sim_P^t$ is an equivalence relation.
- $(r, t) \vDash \mathfrak{K}_P \varphi$ if $(r', t) \vDash \varphi_\alpha$ for all r' where $r \sim_P^t r'$.

Semantics — believing

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

- $\sim_P^t$ defines a partitioning of $\mathcal{R}$. Let $r/\!\sim_P^t$ be the part containing r.
- $(r,t) \vDash \mathfrak{B}_P\varphi$, if $(r',t) \vDash \varphi$ for the most likely elements r' of $r/\!\sim_P^t$.
- A partial order "more likely than" is defined on $r/\!\sim_P^t$.
- This order must be some refinement of the order $\supseteq$ on sets
$$\{T \in \mathbf{TTP} \,:\, (r',t) \vDash \mathit{right}_T\}$$
for $r' \in r/\!\sim_P^t$.
- We could also let the set $\mathbf{TTP}$ 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 φ to Q" is formalized as $\mathfrak{M}_P\Diamond\mathfrak{B}_Q\varphi$.

Semantics — being able to make sure

$(r, t) \vDash \mathfrak{M}_P \varphi$ 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 $t' \leq t$.
- $(r', t) \vDash \varphi$ for all $r' \in R$;
- if $\dot{r} =_t r$ and $\dot{r} \notin R$, then for all $r' \in R$:
  Let $t' \in \mathbf{T}$ 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 $\mathit{Generate}$ by P);
  - there exists $r'' \in R$, such that $\dot{r} =_{t'+\varepsilon} r''$.

Semantics — $\mathcal{S}$ and $\mathcal{U}$, A and E

- $(r,t) \models \varphi \mathcal{U} \psi$ if $(r,t') \models \psi$ for some $t' > t$ and for all t'', where $t < t'' < t'$, $(r,t'') \models \varphi$.
  - $(r,t) \models \varphi \mathcal{S} \psi$ is defined similarly.
- $\Diamond\varphi \equiv \mathsf{true}\,\mathcal{U}\,\varphi$.
- $\Box\varphi \equiv \neg\Diamond\neg\varphi$.
- $\blacklozenge\varphi \equiv \mathsf{true}\,\mathcal{S}\,\varphi$.
- $\blacksquare\varphi \equiv \neg\blacklozenge\neg\varphi$.
- $(r,t) \models \mathsf{A}\,\varphi$ if $(r',t) \models \varphi$ for all r', where $r =_t r'$.
- $\mathsf{E}\,\varphi \equiv \neg\,\mathsf{A}\,\neg\varphi$.

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.

Source: [Buldas, Lipmaa, Schoenmakers. Optimally Efficient Accountable Time-Stamping. Proc. PKI'2000].

Duties of agents

- 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 $P \in \mathbf{Agent}$ there is a formula D_P that is true iff P "has done everything he has to do" so far.
- We assume that $\neg D_P \to \mathsf{A}\Box\neg D_P$ holds for all agents P.

Formalizing fraud detection

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

- $D_P \to \mathfrak{M}_P(\neg D_Q \to \Diamond \mathfrak{B}_P \neg D_Q)$
- $D_P \wedge D_R \to \mathfrak{M}_P(\neg D_Q \to \Diamond \mathfrak{B}_R \neg D_Q)$

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”:

- $D_P \wedge D_Q \wedge \mathfrak{B}_Q \neg D_P \rightarrow \mathfrak{M}_P \Diamond \neg \mathfrak{B}_Q \neg D_P$
  - $D_P \wedge D_Q \wedge \mathfrak{B}_Q \neg D_P \rightarrow \mathfrak{M}_Q \Diamond \mathfrak{M}_P \Diamond \neg \mathfrak{B}_Q \neg D_P$
  - $D_P \wedge D_Q \wedge \mathfrak{B}_Q \neg D_P \rightarrow \mathfrak{M}_P \mathfrak{M}_Q \Diamond \mathfrak{M}_P \Diamond \neg \mathfrak{B}_Q \neg D_P$
- $D_Q \wedge \mathfrak{B}_Q \neg D_P \rightarrow \mathfrak{M}_Q \Diamond (D_P \rightarrow \mathfrak{M}_P \Diamond \neg \mathfrak{B}_Q \neg D_P)$

Some axioms

$$\mathsf{A}(\varphi \to \psi) \to (\mathfrak{M}_P\varphi \to \mathfrak{M}_P\psi)$$

$$\mathfrak{M}_P\varphi \to \mathfrak{M}_P\mathfrak{M}_P\varphi$$

$$\mathsf{A}\,\varphi \to \mathfrak{M}_P\varphi$$

$$\mathfrak{K}_P\Box\varphi \to \Box\mathfrak{K}_P\Box\varphi$$

$$sees(P, M) \to \mathfrak{M}_P\Diamond sees(Q, M)$$

$$said(P, \varphi) \wedge right_P \to \blacklozenge(said(P, \varphi) \wedge \varphi)$$

$$\ldots$$

What axioms or inference rules are there for deriving $\mathfrak{B}_P right_T$?

Some axioms

$$\mathcal{K}_P(\varphi \to \psi) \to (\mathcal{K}_P\varphi \to \mathcal{K}_P\psi) \qquad \mathcal{K}_P\varphi \to \mathsf{A}\,\varphi$$

$$\mathcal{K}_P\varphi \to \mathcal{K}_P\mathcal{K}_P\varphi \qquad \mathsf{A}\,\varphi \to \varphi$$

$$\neg\mathcal{K}_P\varphi \to \mathcal{K}_P\neg\mathcal{K}_P\varphi \qquad \mathcal{K}_P\varphi \to \mathcal{B}_P\varphi$$

$$\mathcal{B}_P(\varphi \to \psi) \to (\mathcal{B}_P\varphi \to \mathcal{B}_P\psi) \qquad \mathcal{B}_P\varphi \to \mathcal{K}_P\mathcal{B}_P\varphi$$

$$\mathsf{A}(\varphi \to \psi) \to (\mathsf{A}\,\varphi \to \mathsf{A}\,\psi) \qquad \neg\mathcal{B}_P\varphi \to \mathcal{K}_P\neg\mathcal{B}_P\varphi$$

$$\mathsf{A}\,\varphi \to \mathsf{A}\,\mathsf{A}\,\varphi \qquad \neg\,\mathsf{A}\,\varphi \to \mathsf{A}\,\neg\,\mathsf{A}\,\varphi$$

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.
- …