Logical representation and analysis of protocols.

Security protocols

- A security protocol is a set of rules, adhered to by the communication parties in order to ensure achieving various security or privacy goals, such as establishing a common cryptographic key, achieving authentication, etc.
- We have discussed already several protocols, aiming at:
  - Key exchange;
  - Private electronic payments;
  - E-voting.

Correctness of protocols

- Are they correct at all?
- How do we establish correctness?
- We have used semi-formal arguments, like
  \textit{If a message is encrypted with the public key of Alice, then only a participant who knows private key of Alice (presumably Alice herself only) can decrypt it.}
- Typically we have considered possible attacks and argued using the reasoning as above, that attacks are impossible (under some reasonable assumptions).
- Is that enough? Are we sure that we have considered all possible situations of use?

Correctness of protocols. II

- Security protocols are designed to succeed even in the presence of a malicious agent, often called \textit{intruder} (adversary);
- Intruder may have complete or partial control over the communication network and may have different computational capabilities;
- The correctness of the protocols depends on the assumptions on capabilities of possible intruder;
- Assumptions are often left implicit;
- Typically in security we have to deal with numerous non-trivial assumptions.
The power of formal methods

- What should we do about establishing correctness of security protocols?
- Apply formal methods!
  - Make explicit all the assumptions involved in a protocol;
  - Make a formal model of the protocol (and its execution);
  - Apply formal reasoning, which would establish the correctness of the protocol.
- Two important aspects:
  - The correctness is established only for a particular formal model of the protocol;
  - and under explicit assumptions (about capabilities of participants, etc);

Logical representation

- Formal aspects of reasoning is an important part of logic;
- Logical representation and analysis of the security protocols is a particular successful approach for the protocols verification;
- Non-classical modal epistemic logics dealing with such notions as “belief” and “knowledge”, are more suitable here than classical logics dealing primarily with “truth”.

Protocol analysis using a logic

- Derive the specification of an idealized protocol in a logical language from the (usually informal) original specification;
- Specify the assumptions about the initial state;
- Attach logical formulae to statements of the protocol as assertions about the state of the system after each statement;
- Apply logical axioms and inference rules to derive beliefs held by parties in the protocols.

BAN logic

- M. Burrows, M. Abadi, R. Needham (1989): Logic of authentication, or BAN logic;
- Suitable for formal analysis of authentication protocols;
- A protocol is analysed from the point of view of each principal (participant) $P$.
- Each message received by $P$ is considered in relation to previous messages received by $P$ and sent by $P$;
- The question, one can address using BAN logic, is what a principal should believe, on the basis of the messages it has sent and received.
Formulae of BAN logic

- **P believes** X is a formula of BAN logic saying
  - P is entitled to conclude that X is true, or
  - P has a justification for X;
- **P sees** X
  - The principal P receives a message containing X. P might need to perform decryption to extract X. X can be a statement or a simple item of data. P does not necessarily believes X.

Formulae of BAN. II

- **P controls** X
  - P has jurisdiction over X, or P is trusted as an authority on X. For example an authentication server is trusted as an authority on statements about a key it has allocated.
- **P said** X
  - At some point in the past, P is known to have sent a message including X

Further notation

- If K is a key, then \{X\}_K means X encrypted with the key K.
- If X and Y are statements, then X \cdot Y means X and Y

Formulae of BAN logic. II

- **Fresh(X)**
  - X has not been sent earlier. It is a fresh value (nonce = number used once).
- **P \&\& Q**
  - K is a secret between P and Q and possibly other principals trusted by P and Q (such as authentication server).
Main assumption

- Trusted principals do not lie about their beliefs to other principals.
- That means if $P$ is trusted, and if a formula $X$ is received in a message (known to have been) sent by $P$ then it can be deduced that $P$ believes $X$.

Deduction rules

- Deduction rules (or postulates) of BAN logic have the following format

$$\frac{X, Y}{Z}$$

meaning $Z$ follows from a conjunction of statements $X$ and $Y$.

Main postulates of BAN logic

The message meaning rule:

\[
\begin{align*}
\text{P believes } P \rightarrow Q, P \text{ sees } \{X\}_K \\
\text{P believes } (Q \text{ said } X)
\end{align*}
\]

If $P$ believes that it shares a secret key $K$ with $Q$, and if $P$ receives a message containing $X$ encrypted with $K$ then $P$ believes that $Q$ once said $X$.

Main postulated of BAN logic

The nonce-verification rule

\[
\begin{align*}
P \text{ believes fresh}(X), P \text{ believes } (Q \text{ said } X) \\
P \text{ believes } (Q \text{ believes } X)
\end{align*}
\]

Nonce = number used once = fresh value.

If $P$ believes that $Q$ once said $X$, then $P$ believes that $Q$ once believed $X$ (by main assumption). If additionally $P$ believes $X$ is fresh then $P$ must believe that $Q$ currently believes $X$. 
## Main postulated of BAN logic

The jurisdiction rule:

\[
P \text{ believes } (Q \text{ controls } X), P \text{ believes } (Q \text{ believes } X) \\
\hline
P \text{ believes } X \\
\]

If \( P \) believes that \( Q \) has control over whether or not \( X \) true and if \( P \) believes that \( Q \) believes it to be true, then \( P \) must believe in it also. The reason is \( Q \) is an authority on the matter as far as \( P \) is concerned.

---

## Decomposition postulates

### \( P \) sees \((X,Y)\)

\[
\frac{P \text{ sees } (X,Y)}{P \text{ sees } X} \\
\hline
P \text{ believes fresh}(X) \\
\frac{P \text{ believes fresh}(X,Y)}{P \text{ believes } (Q \text{ believes } (X,Y))} \\
\frac{P \text{ believes } (Q \text{ believes } (X))}{P \text{ believes } (Q \text{ believes } (X,Y))} \\
\]

\( P \) sees \((X,Y)\) and \( P \) believes fresh\((X)\) leads to \( P \) believing that \( Q \) believes \((X,Y)\) and further that \( Q \) believes \((X)\).