Extending Dolev-Yao with Assertions

Formal Methods Update Meeting
IIT Kharagpur
July 28–30, 2014

Outline

In the beginning, there was nothing

- Then, Danny Dolev and Andrew Yao said "Let there be an abstract model for security protocols".
- Since then, lots of research on the Dolev-Yao model and various extensions.
- Treats terms as tokens - agents 'own' terms that they receive.

The need for assertions

- Protocols often use certification - if A receives a proof from B it may not then send the same to C in its own name.
- Frequently seen in voting protocols:
  - A sends an encrypted vote $\{v\}_{pk(A)}$ to B.
  - A also sends a (zero-knowledge) proof to B that v takes on one of a predetermined set of values.
  - Constructing such a proof needs the sender to have access to v.
  - Thus, B cannot forward this to other agents in its own name.
- We shall call such certificates 'assertions'.

The What and the Why

- We propose an extension to the Dolev-Yao model where agents explicitly send and receive assertions.
- The Dolev-Yao model can express such certification in many ways, depending on the situation.
  - Conventions of the framework: certifying the goodness of keys by servers, freshness of nonces etc.
  - Cryptographic devices: bit commitment, zero-knowledge proofs etc.
  - Protocol-specific ad hoc methods: tagging origin by pairing the sender's name with the message.
- Our extension, thus, adds no expressive power.

BUT!

- Increases flexibility for reasoning about protocols.
- Syntactic separation allows us to structure protocols better.

Examples

Assertion Language

$$\alpha ::= m \prec t \mid t = t' \mid \alpha_1 \vee \alpha_2 \mid \alpha_1 \wedge \alpha_2 \mid A \textit{ says } \alpha$$

The perfect assertion assumption

Intruder capabilities

The derivability problem

The safety-checking problem

Thank you!