The Dolev-Yao Intruder is the most Powerful Attacker

Iliano Cervesato iliano@itd.nrl.navy.mil

ITT Industries, Inc @ NRL - Washington DC

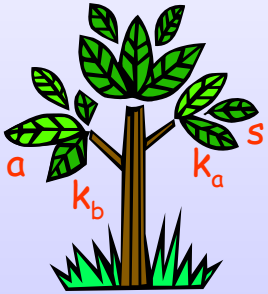
http://www.cs.stanford.edu/~iliano/

The Dolev-Yao Model of Security

- Symbolic data
  - No bits

- Black-box cryptography
  - No guessing of keys

- Partially abstract data access
  - Knowledge soup



- Found in most protocol analysis tools
  - Tractability

The Dolev-Yao Intruder

- Intercept / emit messages
- Decrypt / encrypt with known key
- Split / form pairs
- Look up public information
- Generate fresh data

- Found in most protocol analysis tools

Completeness unproved

Theorem

The Dolev-Yao intruder can emulate any attacker within the Dolev-Yao model of security.

The Medium

MSR: strongly-typed multiset rewriting with existentials and constraints

- Intruder specified as any other role
- Access control
  - Fine grained, protocol specific description of Dolev-Yao model

- Other frameworks could be used

The Proof

- Given the spec. of an arbitrary attacker
- Construct an equivalent sequence of actions for the Dolev-Yao intruder
- By induction on the structure of an AC derivation

Access Control & the DY Intruder