Demarcation of Security in Entity Authentication Protocols

Naveed Ahmed & Christian D. Jensen

DTU Informatics, Denmark

July 6, 2011

Entity Authentication Protocols

- Basis of Security in Distributed Environments
- Examples
  - Log in on a Computer Terminal
  - Log in on a Netbanking Portal
  - RFID Scanning of Goods in a Warehouse
  - Kerberos

Goals of Authentication Protocols

- End Results of Protocols may be Different !
- What is Authentication ?

Correctness and Security

- Conceptually Different
- Operationally Different?
- “authentication is, what an authentication protocol does” !

Our Proposal: Security Requirement

- Binding Sequence
  "a sequence of protocol messages, s.t., the sequence preserves its integrity"
- Sufficient and Necessary

Our Proposal: Correctness Requirements

- Fine Level Authentication Goals (FLAGs)
- Derivable from Binding Sequence
- List of FLAGs (1/2)
  - Recognition
  - (Anonymous) Identification
  - Operativeness
  - Willingness

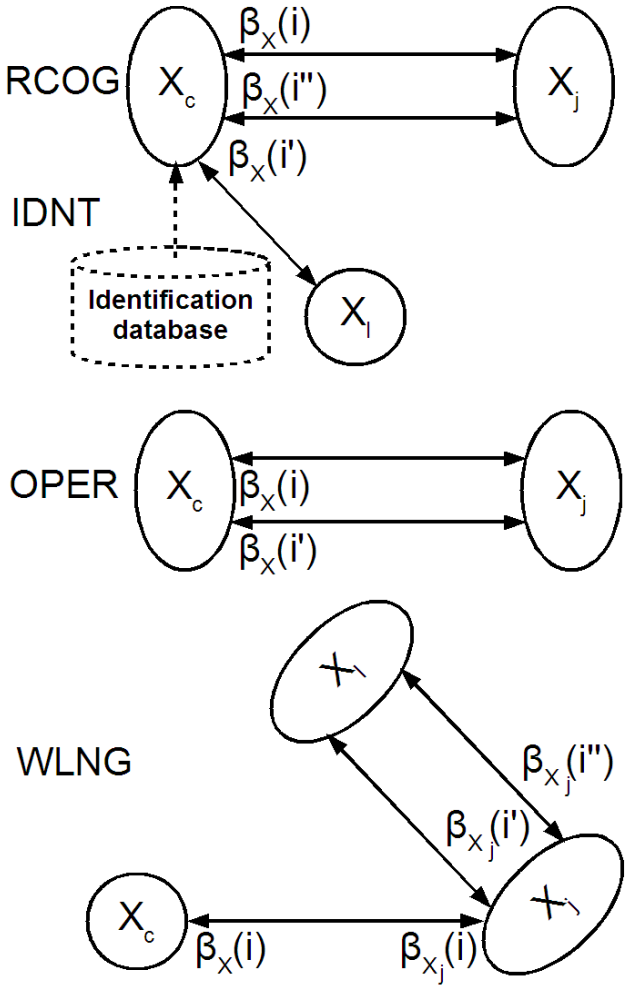
FLAGs (2/2)

- Single Sided Authentication
- Confirmation
- Strong Single-sided Authentication
- Mutual Authentication

How to Operationalize a FLAG?

- A Concrete Procedure / Algorithm / Method
- Example: Left-Right Indistinguishability

How to Operationalize FLAGs?



Final Words

- Separating Security and Correctness is important in System Design
- Relaxed Security / Soft Security / Adaptable Security

Final Words

- Separating Security and Correctness is important in System Design
- Relaxed Security / Soft Security / Adaptable Security

THANK YOU

naah@imm.dtu.dk
DTU-Informatik
Technical University of Denmark