University of Freiburg, Germany
Department of Computer Science

Distributed Systems

Chapter 2 System Models

Christian Schindelhauer

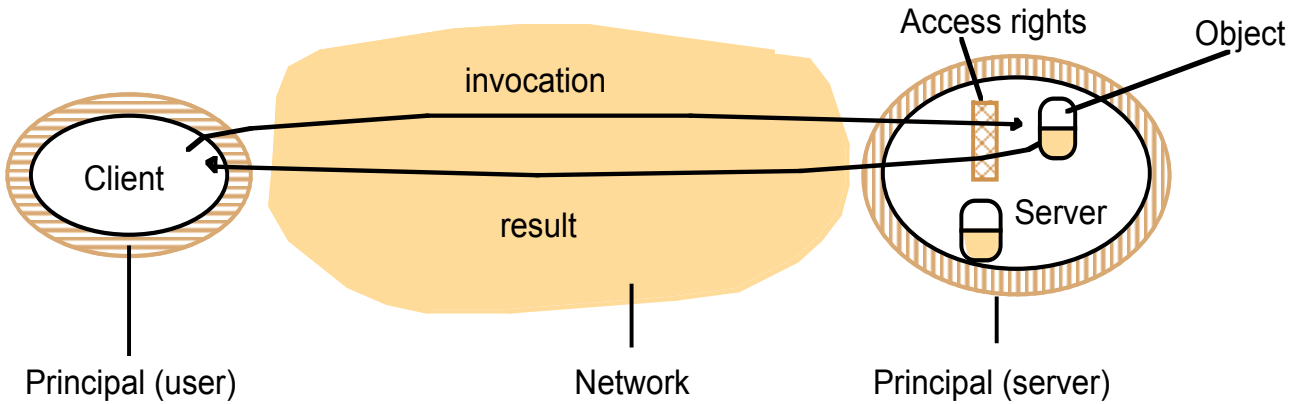
07. May 2014

2.3.3: Security Model

The security of a distributed system

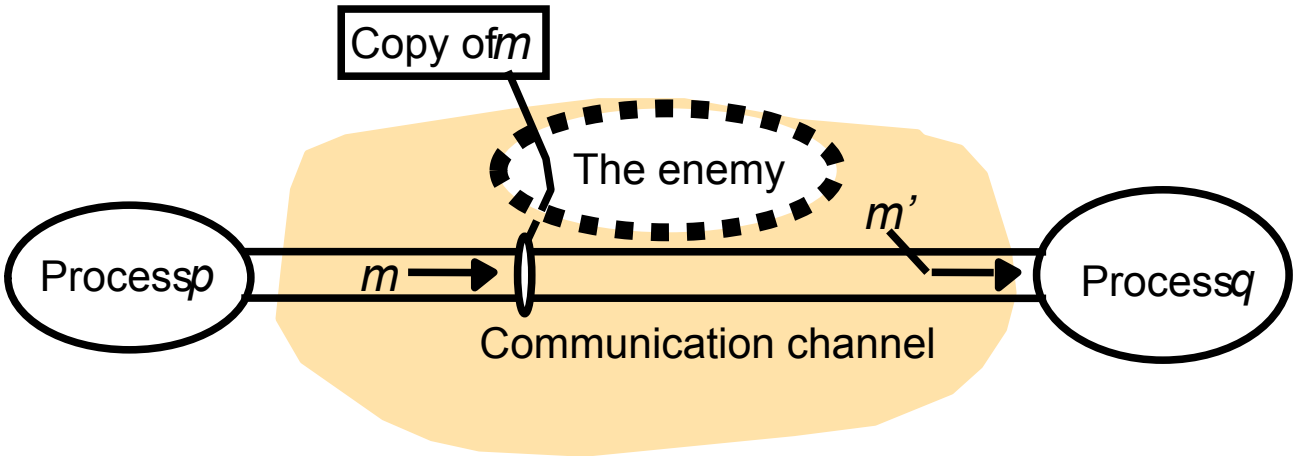
can be achieved by securing the processes and the interaction channels and by protecting the objects they encapsulate against unauthorized access.

- Protecting objects
  - access rights
  - an authority (user or process), called *principal*, grants the access to the objects
- securing processes and interactions
  - messages are exposed to attacks
  - processes expose their interfaces
  - enable invocations



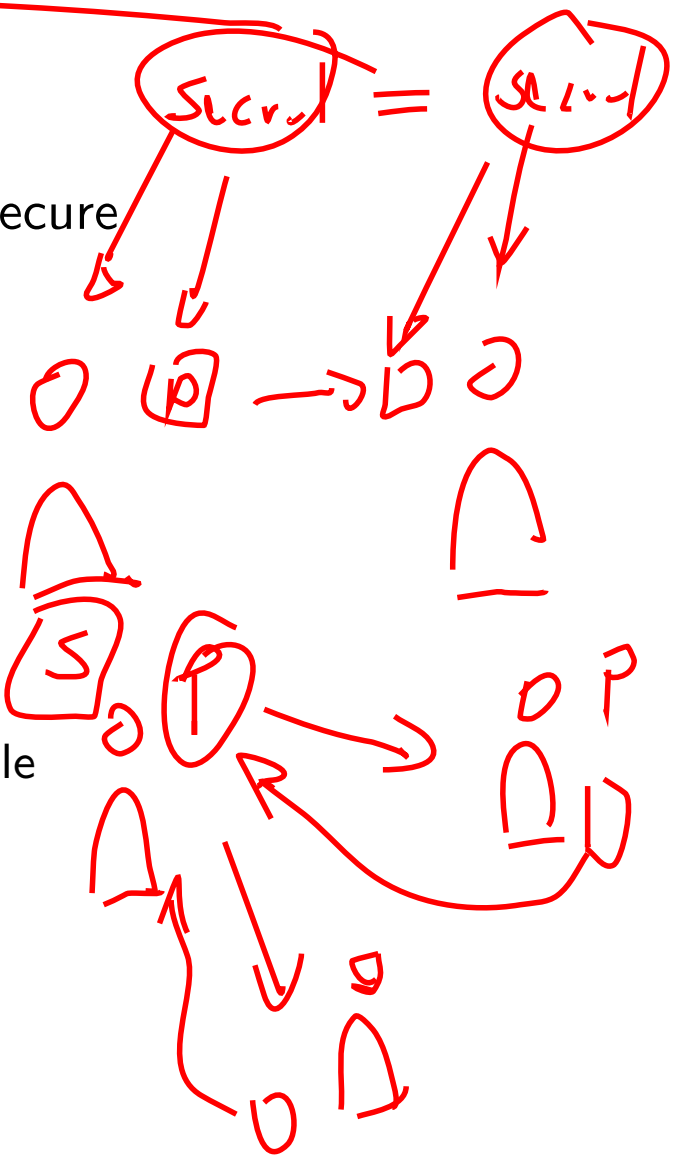
2.3.3: Security Model: The enemy

- threats to processes
  e.g. IP lacks the reliable knowledge of the source of messages
  - Servers, e.g. mail-server delivers e-mail to attacker
  - Clients, e.g. fake GSM radio station captures secret phone calls
- threats to communication channels
  - enemy copies, alters, injects messages
  - enemy saves copies of messages and replays them later
  - such attacks can be defeated by the use of secure channels
- denial of service



from *Distributed Systems – Concepts and Design*, Coulouris, Dollimore, Kindberg

2.3.3: Security Model: Defeating Security Threats



- Cryptography: the science of keeping messages secure
  - symmetric encryption
  - public-key encryption
  - challenge-response protocols
- Authentication
  - shared secrets
  - public-key encryption
- Secure channels
  - process know reliably the identity of the principle
  - ensure privacy and integrity of the data
  - include physical or logical time stamps
- Other threats: denial of service and mobile code

End of Section 2