Authorization and Privacy of Internet Applications

or: Facing Good Security, We Need Better Privacy

Yves Deswarte
deswarte@laas.fr

LAAS-CNRS, France

SRI International, USA

Network security is improving

- Laws on digital signatures -> PKIs
- IP-Sec -> IPv6
- Deployment of Intrusion Detection Systems

… but threats are growing

- DDoS (distributed denial of services)
- e-Commerce fraud
- Transnational e-criminality

…thus we need more security

- e.g., ingress traffic filtering by ISPs
- more audits, more records, …
  - Example: each time a software is run, it sends (serial # + IP @ + …) to the software publisher (Adobe, Totally Hip Software, Eudora, Microsoft…): check new versions, anti-piracy…

… which undermines privacy

- It is more and more practical and easy to collect private information
- Laws on the protection of personal data are inefficient: good will of Information Systems owners

In privacy area, research is weak

- There is no economic pressure for privacy
- Historically,research on security has been funded by defense agencies, and later by financial organizations

State-of-the art: client-server

- The server grants or denies privileges to the client, according to client's identity
- Thus, personal data can/must be recorded, can be correlated…

This paradigm is obsolete

- Internet transactions involve more than 2 parties (e.g., customer, merchant, credit card company, banks, delivery company, …)

- The parties have different, competing interests
  => mutually suspicious

Need-to-know principle

- A merchant does not need to know the real identity of a customer, only the validity of the money order
- The customer's bank does not need to know the identity of the merchant, only the reference of his bank account
- Etc.

… of course

- Real identities would be disclosed to a judge in case of dispute, or on request by judicial authorities (to prevent money laundering, for instance)

MAFTIA project

- Malicious- and Accidental-Fault Tolerance in Internet Applications

- European project IST-1999-11583
  http://www.research.ec.org/maftia/

- Jan.2000 - Dec.2002
  5.5 M€, 45 person.years

MAFTIA authorization scheme