With MAFTIA's Authorization...

Yves Deswarte
deswarte@laas.fr

LAAS-CNRS
Toulouse, France

MAFTIA

IST Dependability Initiative
Cross Program Action 2
Dependability in services and technologies

- Malicious- and Accidental-Fault Tolerance for Internet Applications

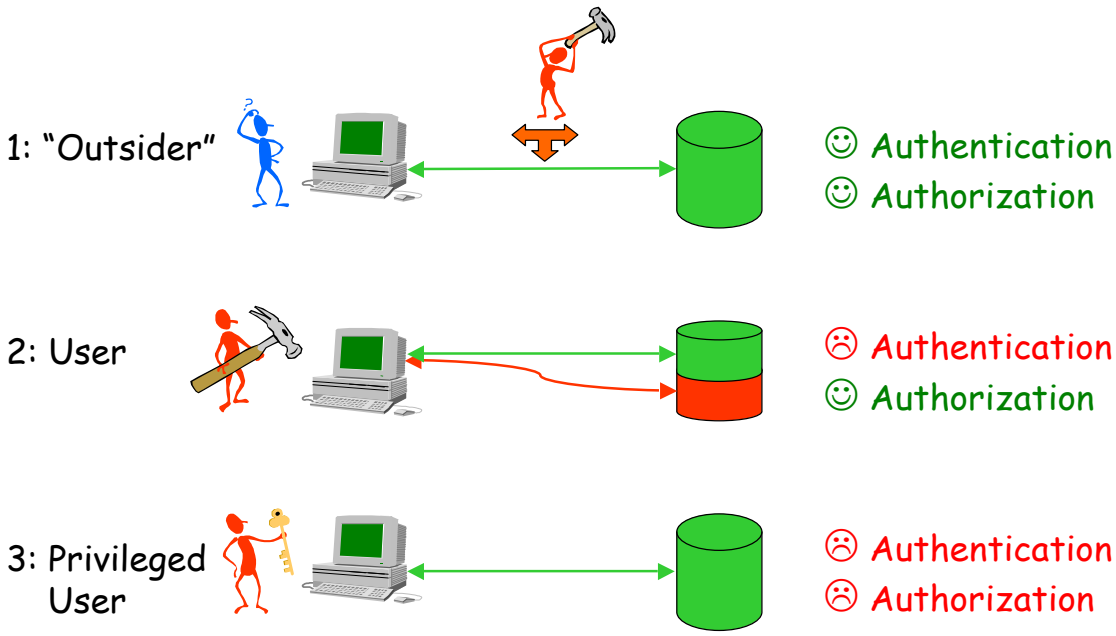
University of Newcastle (UK) — Brian Randell, Robert Stroud
University of Lisbon (P) — Paulo Verissimo
DERA, Malvern (UK) — Tom McCutcheon, Colin O'Halloran
University of Saarland (D) — Birgit Pfitzmann
LAAS-CNRS, Toulouse (F) — Yves Deswarte, David Powell
IBM Research, Zurich (CH) — Marc Dacier, Michael Waidner

c. 45 man-years, c. 2.5M euro
http://www.research.ec.org/maftia/

MAFTIA Workplan

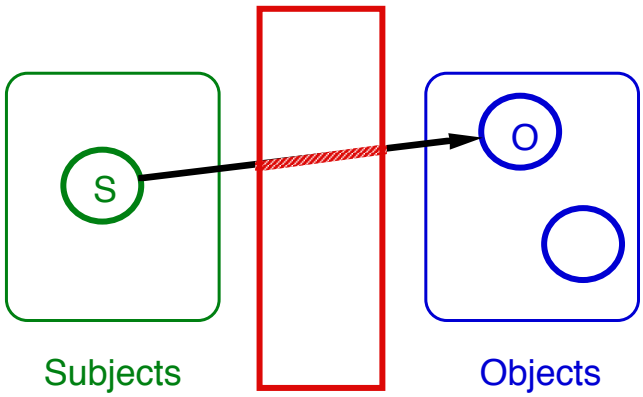
- WP1: Conceptual model and architecture
- WP2: Dependable middleware
- WP3: Intrusion detection
- WP4: Dependable trusted third parties
- WP5: Distributed authorization
- WP6: Assessment

Who are the intruders?



because the "least privilege principle" is not implemented

Authorization: reference monitor

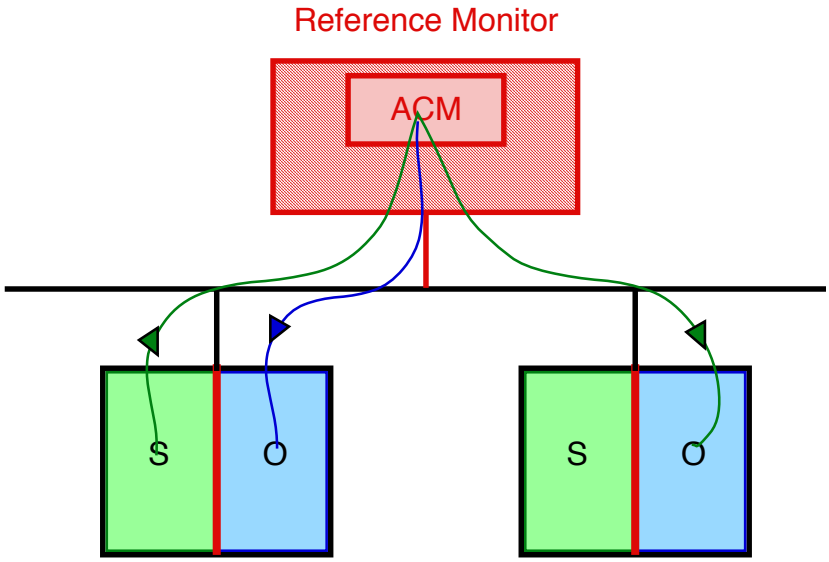


Subject (active)
≈ process

Object (passive)
≈ information containers

Reference Monitor:
- tamperproof
- always invoked
- verifiable as correct

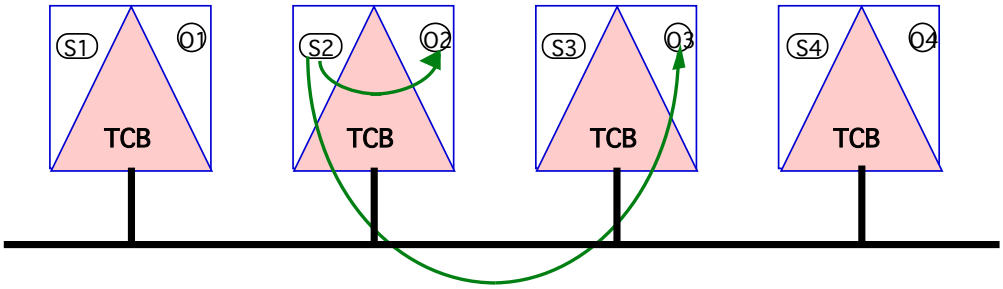
Distributed Authorization ? (1)



☺ small trusted area, easy administration
☹ bottleneck, single-point-of-failure

Distributed Authorisation ? (2)

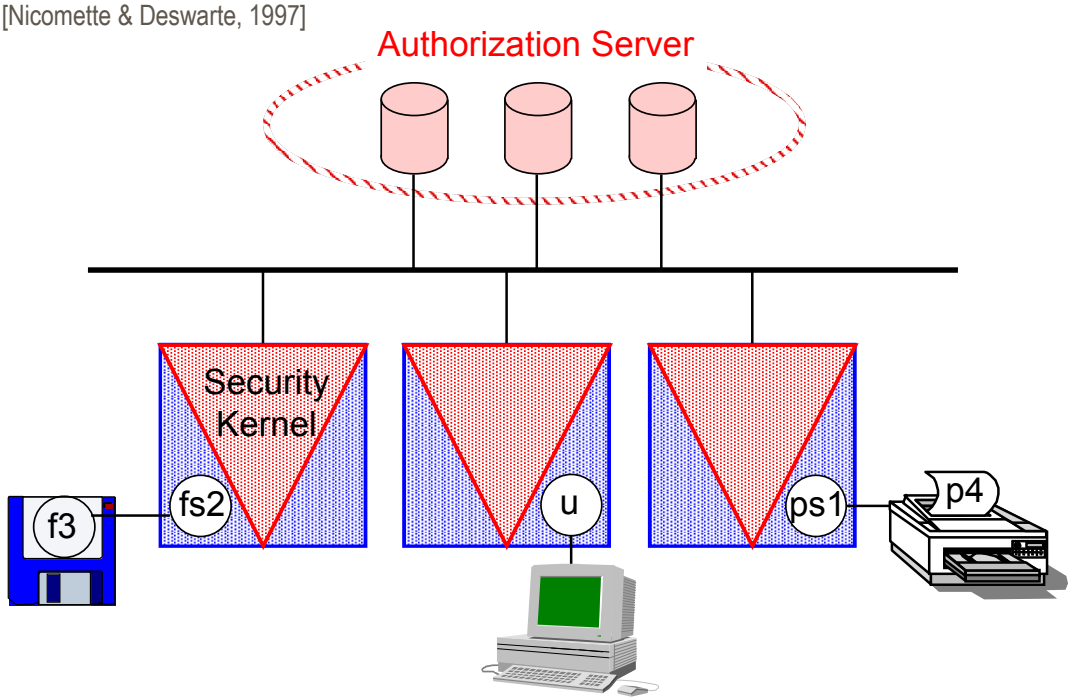
Red Book (TNI)



☺ No bottleneck, no single-point-of-failure
☹ Mutual trust between TCBs, consistency?

Authorisation Scheme for DOOS

[Nicomette & Deswarte, 1997]



Authorisation Scheme

Access Matrix :

Method rights: corresponding to the authorisation for an object to call another object methods

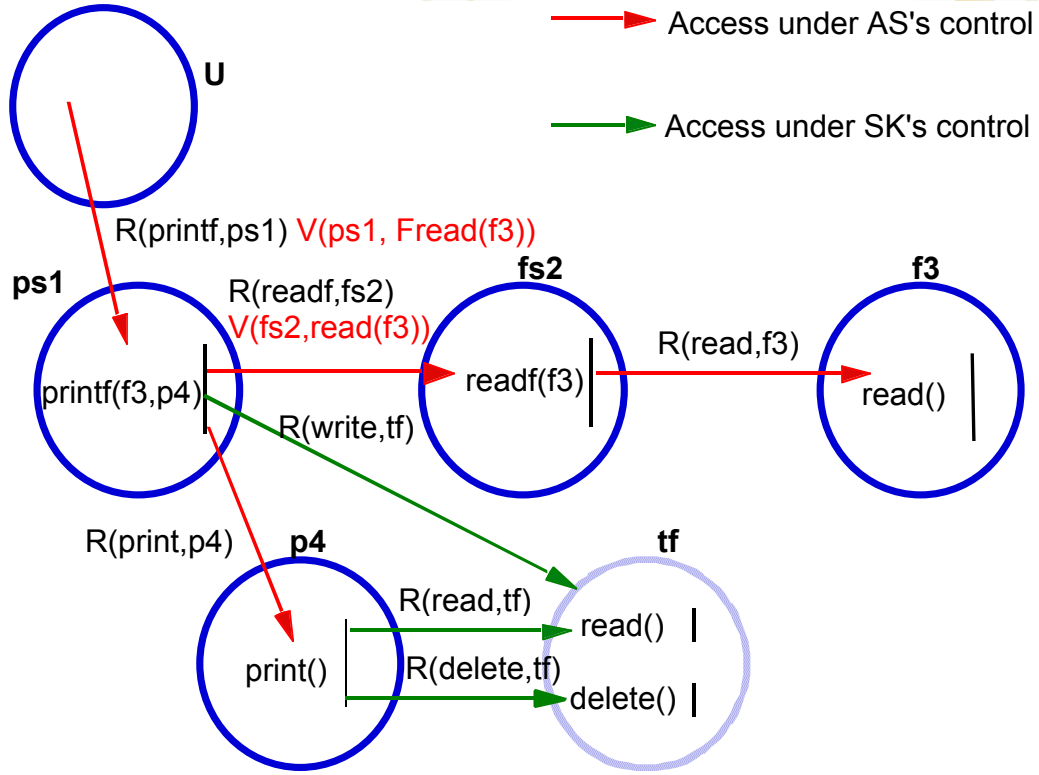
Symbolic rights: corresponding to the authorisation for an object to execute high level operations

	ps1	fs2	f 3	p 4
u			`PF(this,PRINTER)`	`PF(FILE,this)`
ps1				print
fs2				

Symbolic right rules: to check authorisation for high level operations

Capability creation rules: to grant capabilities and *vouchers* to enable high level operations

Example: u:: PF(f3,P4)



MAFTIA Authorization

- Intrusion tolerant authorization servers
- Multi-party transactions
  (not simple client-server relations)
- Local protection

IT Authorization Servers

Like Delta-4 Security servers [Deswarte et al., 1991]:
Fragmentation-Redundancy-Scattering

- Non-confidential information is replicated
- Confidential information is fragmented
  (threshold crypto)
- Global consensus
  (majority voting or Byzantine agreement?)
- Distribution of capabilities/vouchers
  (threshold crypto)

Multi-party transactions

Based on DOOS Authorization Scheme, but…

- Implementing "separation of duty" (transactions initiated jointly by several users)

Local protection

- Internet applications => no modification of user workstations
- No security kernel, but JVM (?)
- Capabilities/vouchers -> applets
- Possibly enforced by smartcards (e.g., JavaCards) … which are already necessary for authentication
- In-line Reference Monitors?

Use cases / Scenarios

- Medical:
  French Healthcare Professional Network
  - Patient smartcard Vitale
  - Professional smartcard CPS
  - Electronic prescriptions
  - Network, PKI, anonymisation, delegation, …
- Electronic Commerce:
  Auction services, privacy enforced payment,…

References

- Yves Deswarte, Laurent Blain and Jean-Charles Fabre
  "Intrusion Tolerance in Distributed Systems"
  IEEE Symposium on Research in Security and Privacy
  Oakland, CA, USA, May 1991, pp.110-121.
- Vincent Nicomette and Yves Deswarte
  "An Authorization Scheme for Distributed Object Systems"
  IEEE Symposium on Security and Privacy
  Oakland, CA, USA , May 1997, pp. 21-30.

http://www.research.ec.org/maftia/