With MAFTIA's Authorization...

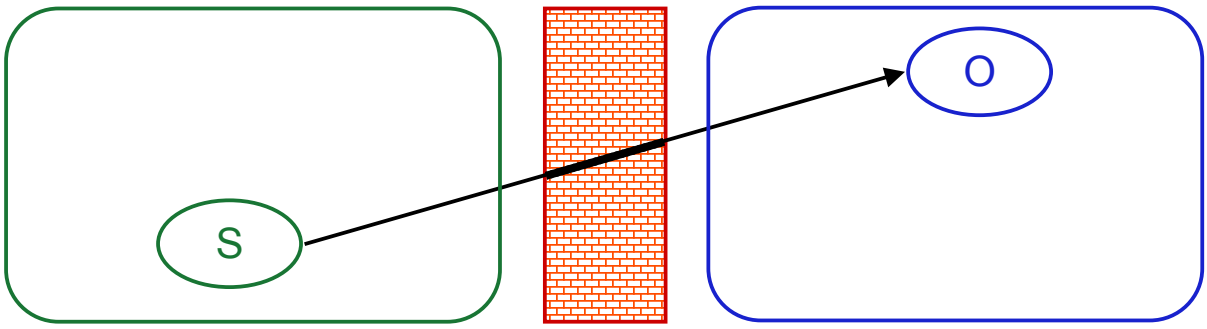
Yves Deswarte
deswarte@laas.fr

LAAS-CNRS
Toulouse, France

Authorization

- Contributes to protection:
  - Error detection/confinement
  - Intrusion prevention/confinement
- For Internet applications:
  - More flexible than "client-server" paradigm
  - Contributes to privacy:
    personal information is disclosed only on a "need-to-know" basis

Authorization: reference monitor

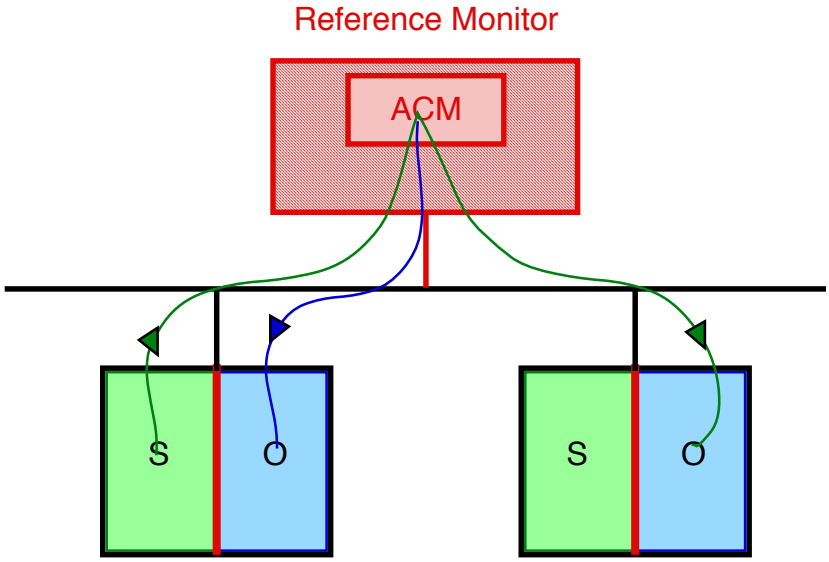


Subjects
=
Active Entities
(e.g., process, user, …)

Reference
Monitor
=
Tamperproof
Always Invoked
Verified Correct

Objects
=
Information Containers
(e.g., file, display, …)

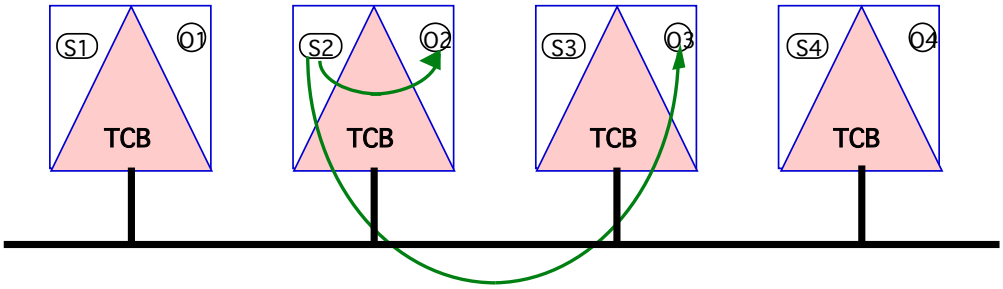
Distributed Authorization ? (1)



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

Distributed Authorisation ? (2)

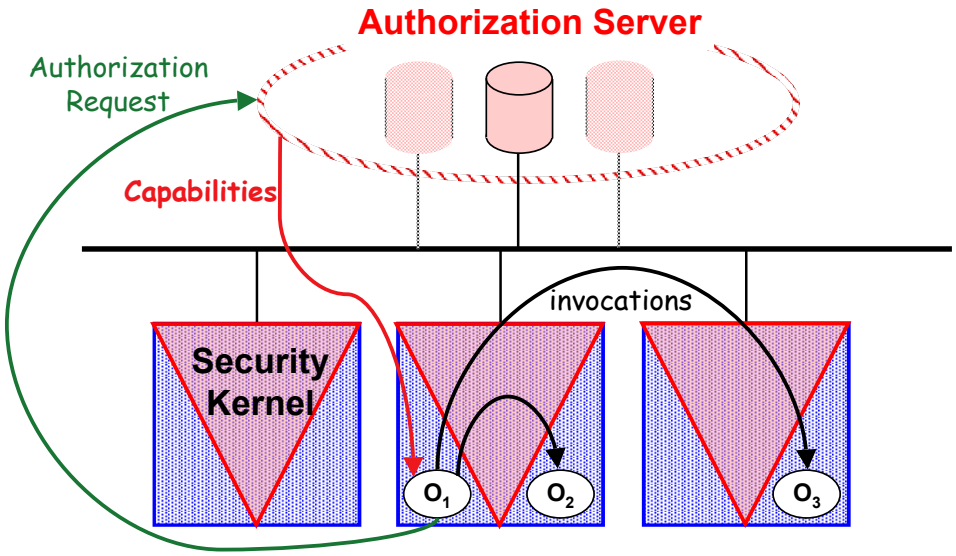
Red Book (TNI)



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

Authorization Scheme for DOOS

[Nicomette & Deswarte, 1997]



Characteristics

- High-level operations:
  - Correspond to coordinated invocations of several objects, e.g. to print a file
  - Facilitate security management:
    - Automatic generation of capabilities
    - Automatic name resolution
- Vouchers:
  - New delegation scheme satisfying the least-privilege principle

Authorisation Scheme

Access Matrix :

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

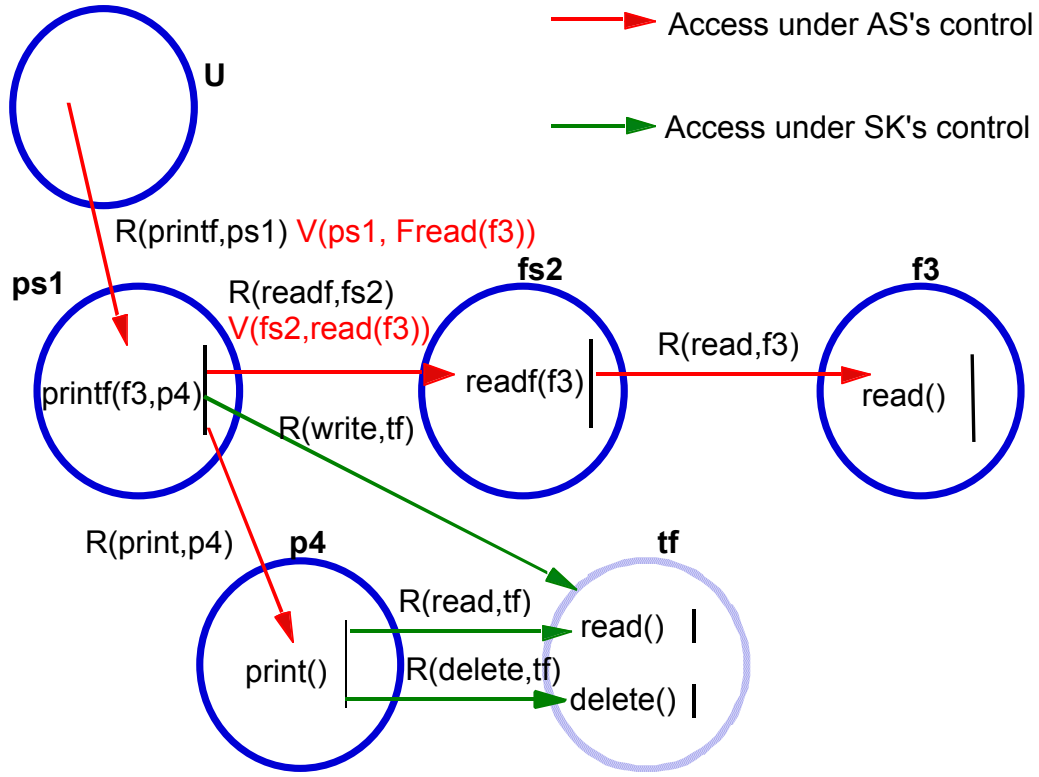
Symbolic rights: corresponding to the authorisation for an object to execute high level operations

	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)



In the context of MAFTIA

- 2 typical scenarios have been analyzed:
  - French healthcare network
  - Web auctions
- Added requirements:
  - Separation of duty
  - Degradable capabilities
- Intrusion-tolerant authorization servers?
- Local protection?

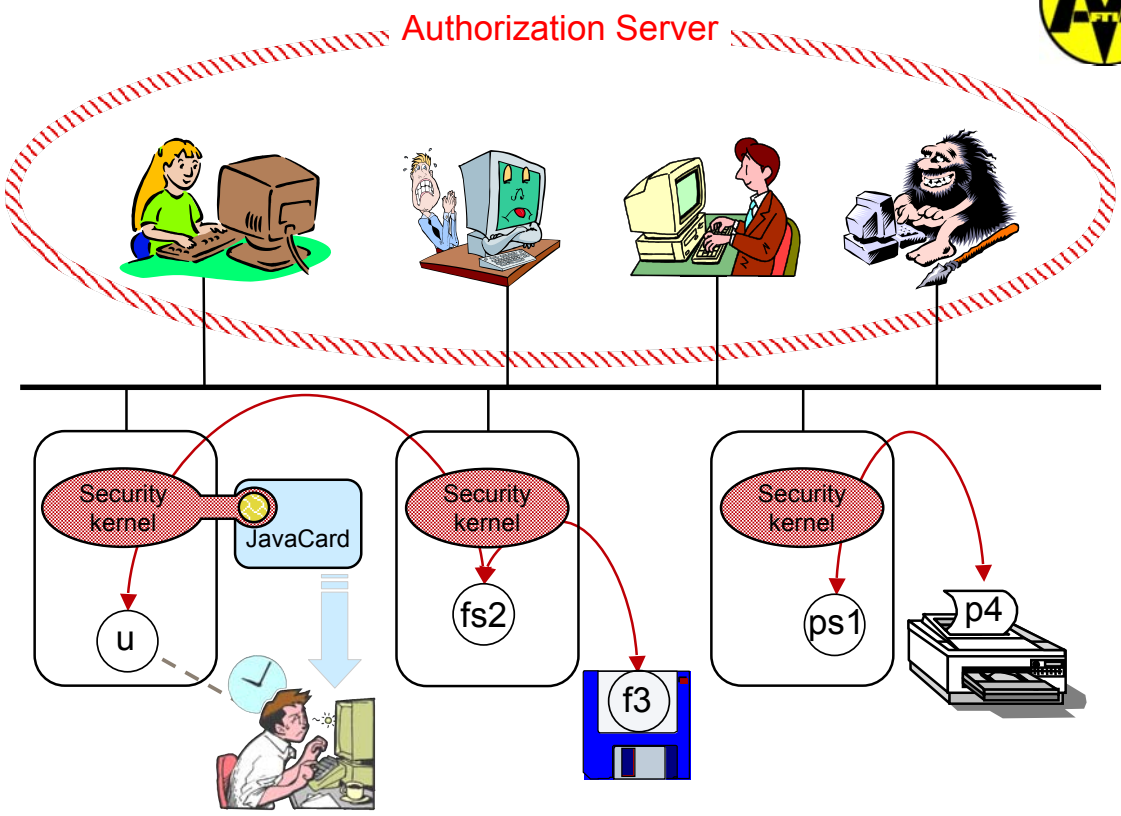
IT Authorization Servers

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)

Local protection

- Internet applications => no modification of user workstations
- No security kernel, but JVM (?)
- Capabilities/vouchers -> applets
- In-lined Reference Monitors?
- Possibly enforced by JavaCards … useful for authentication



References

- N. Abghour, Y. Deswarte, V. Nicomette and D. Powell
  Specification of Authorisation Services
  MAFTIA Deliverable D27, Jan. 2001
  LAAS Report 01.001

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