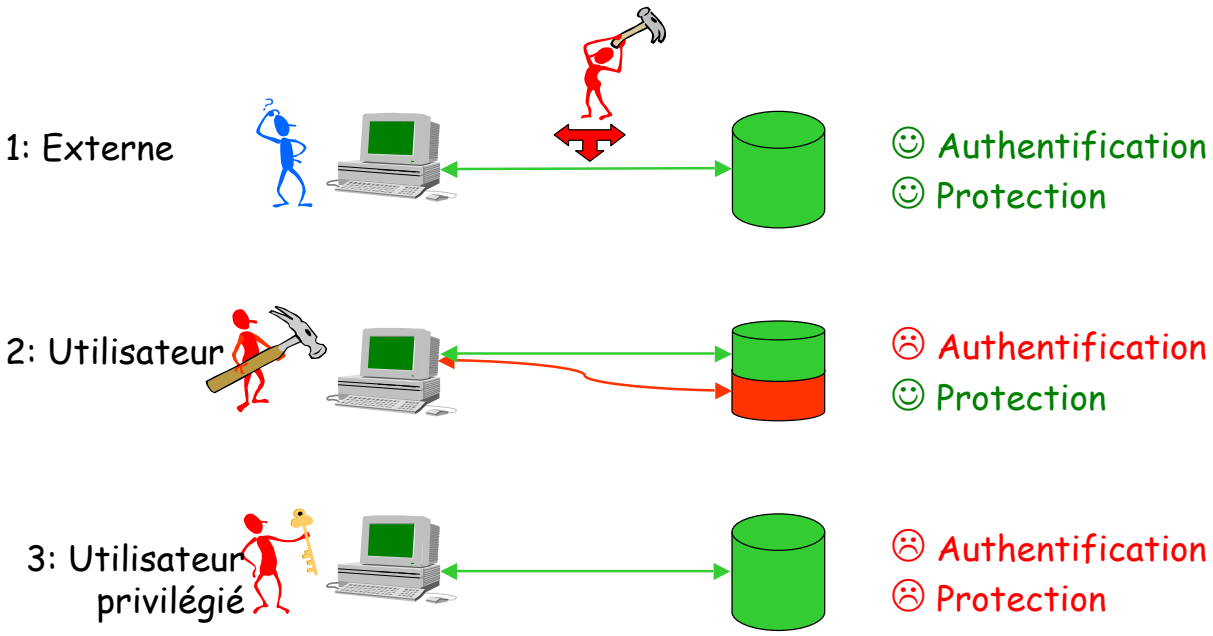
Protection dans Internet

Yves Deswarte
deswarte@laas.fr

Groupe
"Tolérance aux fautes et Sûreté de Fonctionnement Informatiques"

Qui sont les intrus?



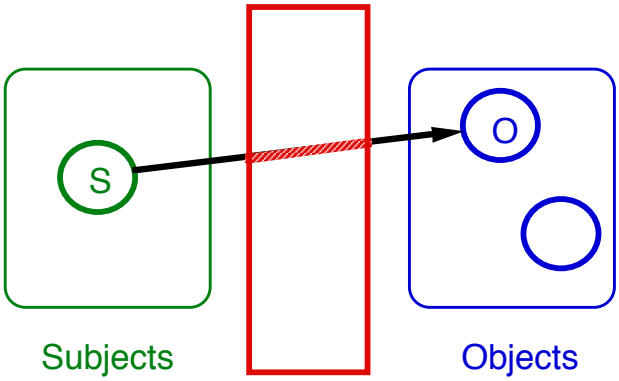
Intrus internes ou externes ?

- 01 Informatique 1998
  - 1200 entreprises dans 32 pays
  - 66% ont subi ≥1 fraude dans les 12 derniers mois
    - 85% par des employés de l'entreprise
- Information Week's security survey 1999

  http://www.informationweek.com/743/security.htm
  - 2700 spécialistes de sécurité dans 49 pays
  - 76% ont subi ≥1 violation de sécurité en 12 mois
    - 41 % par des utilisateurs autorisés (en 1998: 58 %)
    - 31 % par des fournisseurs de service (en 1998: 10 %)

Protection

- Vue classique : « Livre Orange »

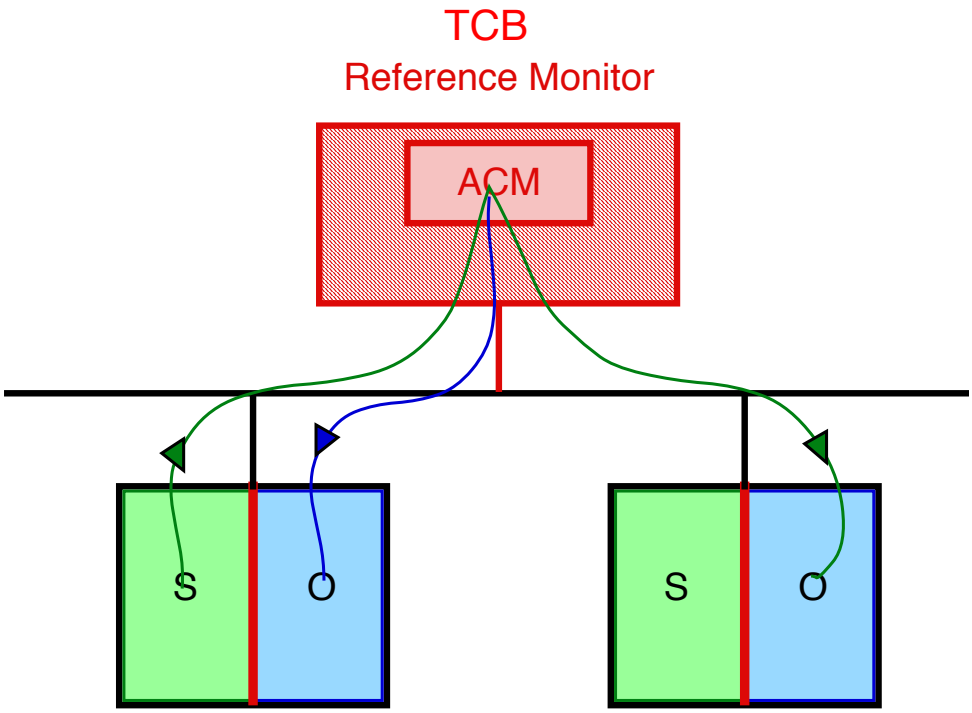


Subject (active)
≈ process

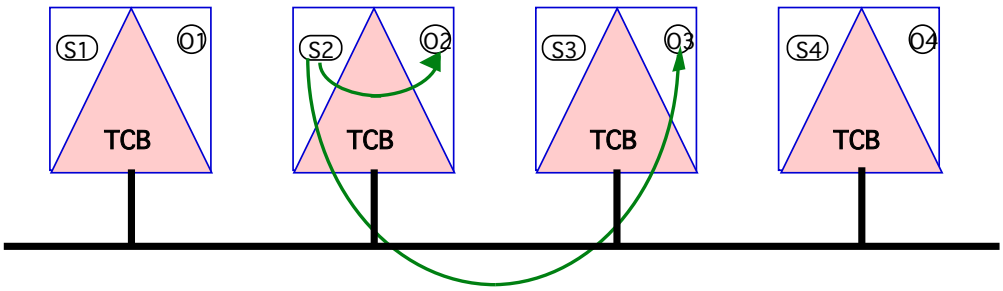
Object (passive)
≈ information containers

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

Protection d'un système réparti?



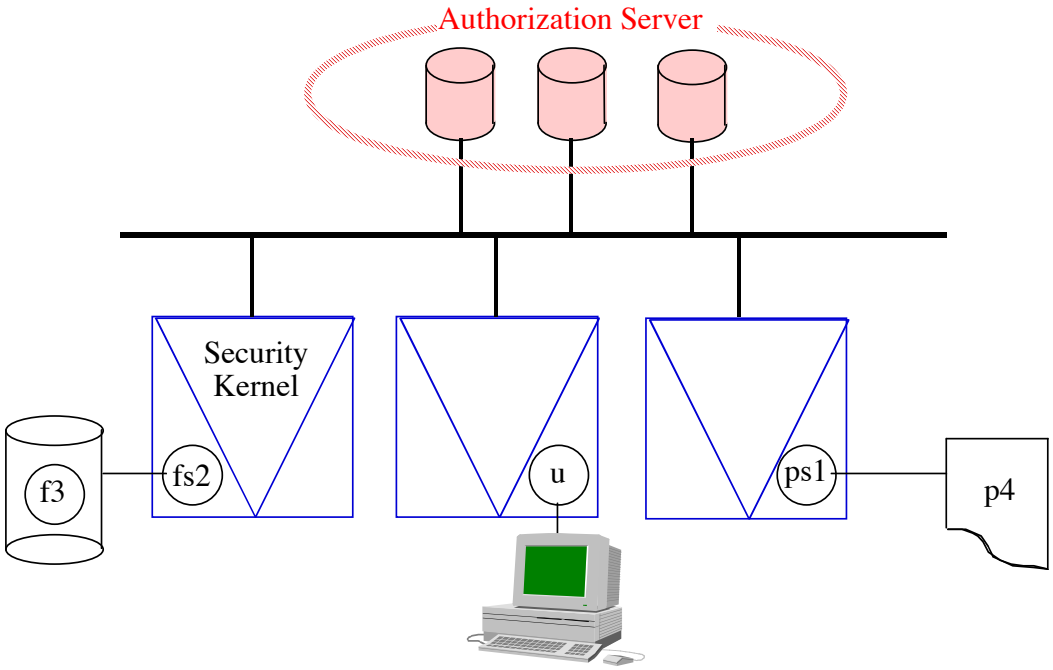
Vision classique (« Livre Rouge »)



☺ Pas de goulot d'étranglement,
pas de point unique de défaillance

☹ Confiance mutuelle entre TCBs, cohérence?

Notre proposition



Tolérance aux intrusions

Une intrusion dans une partie du système ne devrait donner accès qu'à des informations non significatives

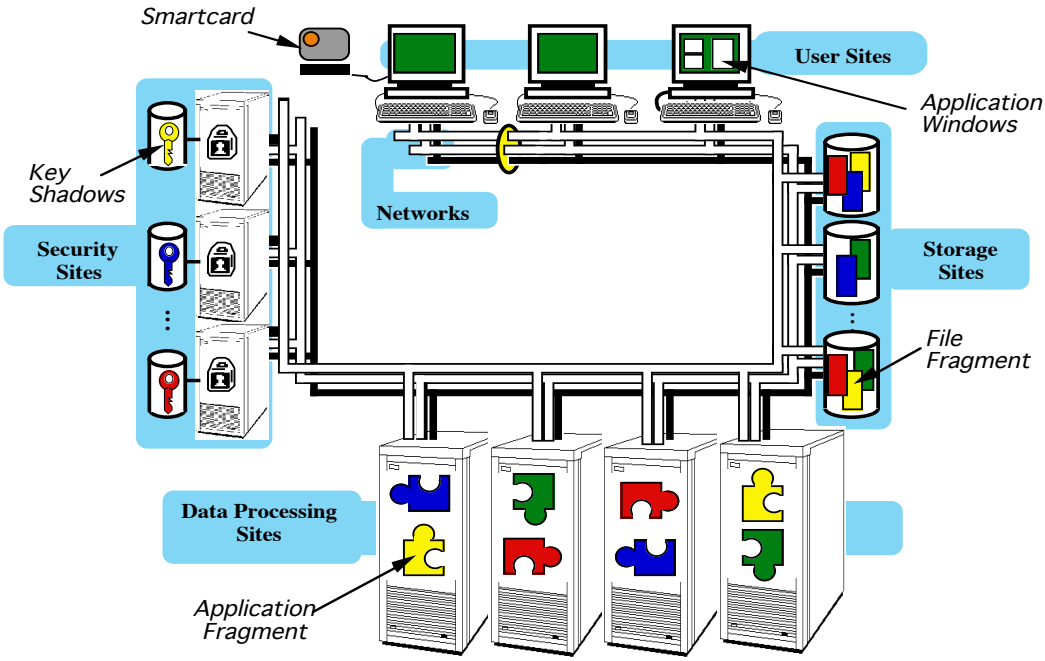
FRD: Fragmentation-Redondance-Dissémination

- Fragmentation: découper les information en fragments non significatifs: *confidentialité*
- Redondance: ajouter de la redondance aux fragments pour en tolérer la destruction et modification partielles: *intégrité + disponibilité*
- Dissémination: isoler les fragments individuels

Types de dissémination

- Espace : utiliser différents liens de communication et sites de stockage
- Temps : transmettre les fragments dans un ordre aléatoire, ou mélanger les fragments de différentes sources
- Fréquences : utiliser des porteuses de fréquences différentes (communication à large bande)
- Privilèges : exiger la coopération de différentes entités pour réaliser une opération (partage de secret, séparation des pouvoirs)

Prototype



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)	Peter Ryan, 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/