Tolérance aux intrusions sur Internet

Yves Deswarte & David Powell
LAAS-CNRS, Toulouse, France

Utilisateurs Internet

Utilisations :
B2B, B2C, C2A, e-government, associations, communautés virtuelles, usage privé…

Buts :
commerce, administration, démocratie, société, culture, loisirs, …

On ne doit pas exclure une catégorie d'utilisateurs au bénéfice d'une autre

Différents besoins ⇒ différents niveaux de sécurité

État de fait

1. Il y a des machines mal administrées qui peuvent être exploitées par des attaquants pour accroître leurs capacités et cacher leurs traces
2. Il y a des centaines de millions d'utilisateurs d'Internet dont une très petite proportion sont des attaquants potentiels

Attaquants sur Internet

Catégories:
Adolescents perturbés, groupes de hackers, délinquants, organisations criminelles, terroristes, états …

Motivations:
curiosité, sport, vanité, vandalisme, vengeance, appât du gain, idéologie, …

Degrés variés de ténacité

Niveaux de ressources variés

- **Vulnérabilités des réseaux** (écoute, brouillage, destruction, insertion, falsification ou rejeu de messages, falsification d'adresse, …)
- **Vulnérabilités des OS et applications** (débordements buffers/pile, …)

Sécurité :
disponibilité, confidentialité, intégrité

Internet

Techniques classiques de la sécurité

Authentification

- Identifier les utilisateurs
- Les tenir responsables (audit)

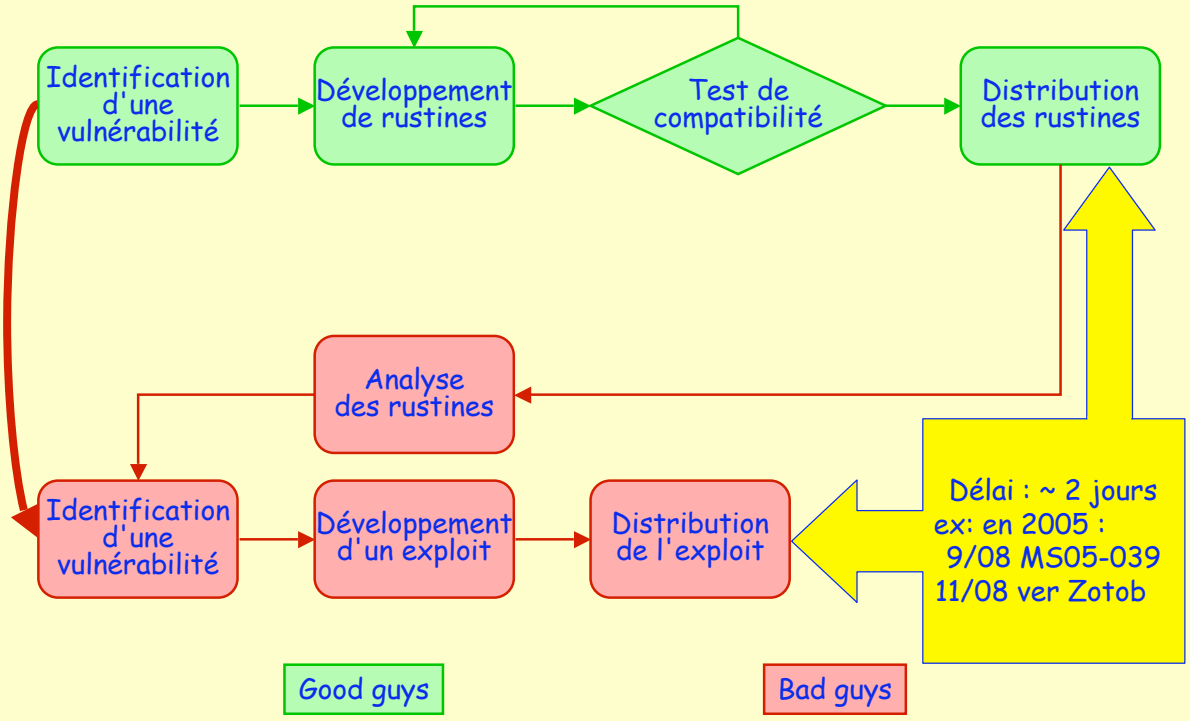
Autorisation

- Empêcher les actions illégitimes
- Principe du moindre privilège
  légitime ⇔ nécessaire

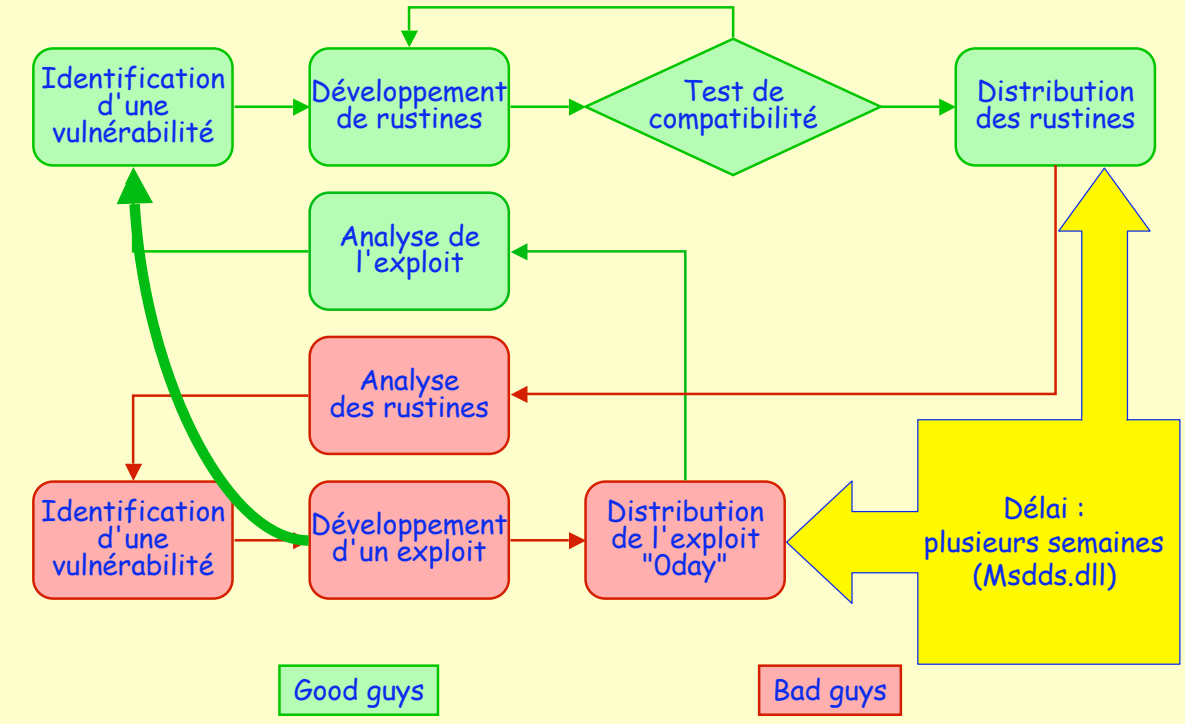
Dissuasion ⇐ Punition ⇐ Détection

➢ Inefficace dans le contexte Internet :
- o Authentification forte infaisable pour les sites publics
- o Applications et OS sur étagères :
  - nombreuses failles
  - rustines non appliquées : manque de temps ou de compétence, crainte de perdre des fonctionnalités nécessaires
- o Les protocoles Internet sont vulnérables (héritage Arpanet)
- o La pression économique ne favorise pas (encore) des défenses connues :
  - filtrage d'entrée (ingress filtering), capacité de traçage, …

Cycle de vie des patches



Cycle de vie des exploits



Approche tolérance?

Sûreté de fonctionnement (Dependability) : concept générique
[Laprie 1985]

Système de fichiers tolérant les intrusions
[Fraga & Powell 1985]

Secure systems from insecure components
[Dobson & Randell 1986]

Approche de tolérance pour les virus informatiques
[Joseph & Avizienis 1988]

Serveur de sécurité tolérant les intrusions
[Deswarte, Blain & Fabre 1991]

Traitement de données tolérant les intrusions
[Fabre, Deswarte & Randell 1994]

MAFTIA **OASIS**

Concepts de base de la SdF

Intrusion

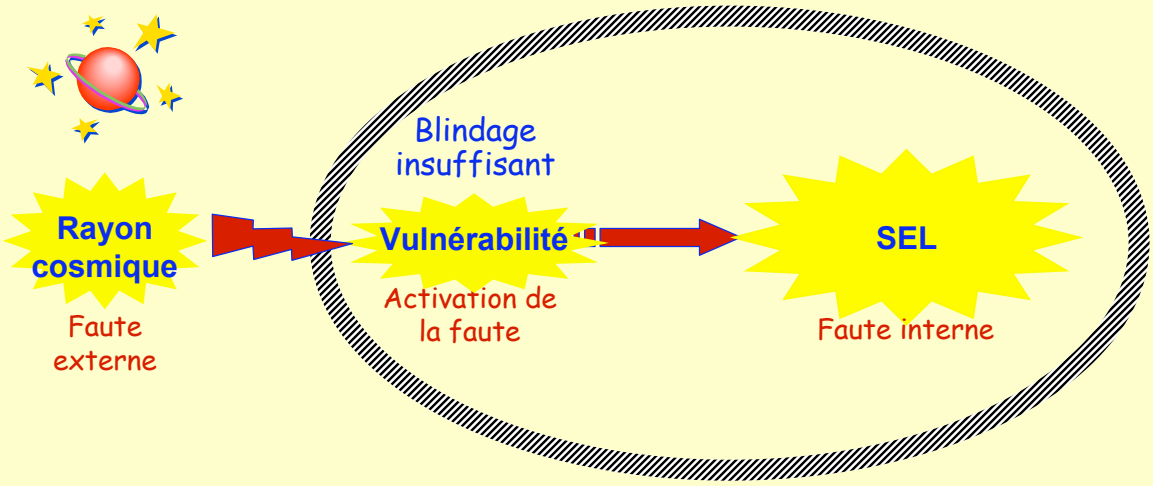
Cause (supposée ou reconnue) d'une erreur

Erreur *partie de l'état du système qui est différente de ce qu'elle devrait être*

Défaillance *survient lorsque le service dévie de sa fonction*

Exemple: Single Event Latch-up

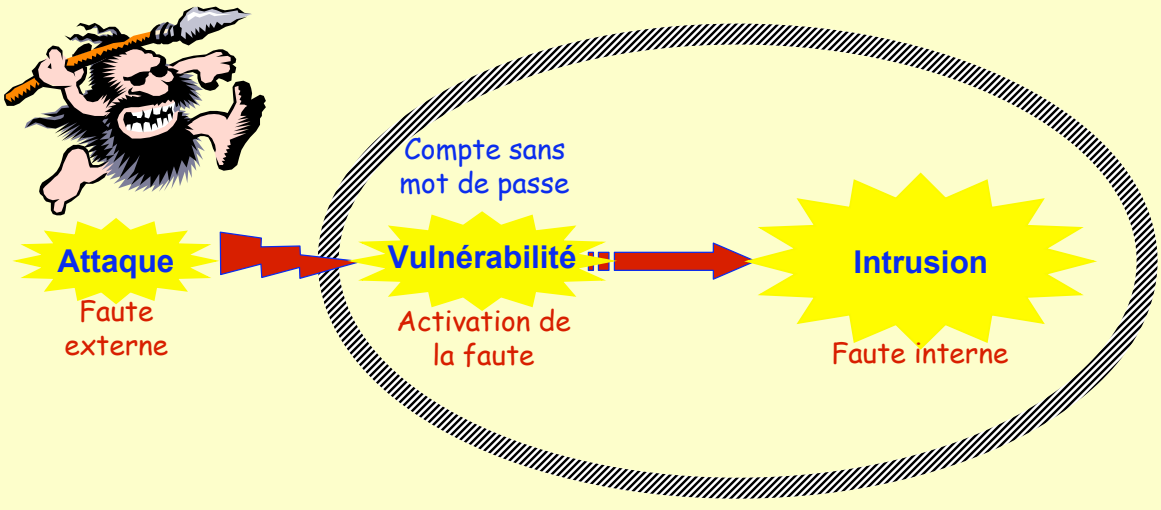
Les SELs sont des collages réversibles
(ex. rayons cosmiques, ions lourds)



Calculateur embarqué dans un engin spatial

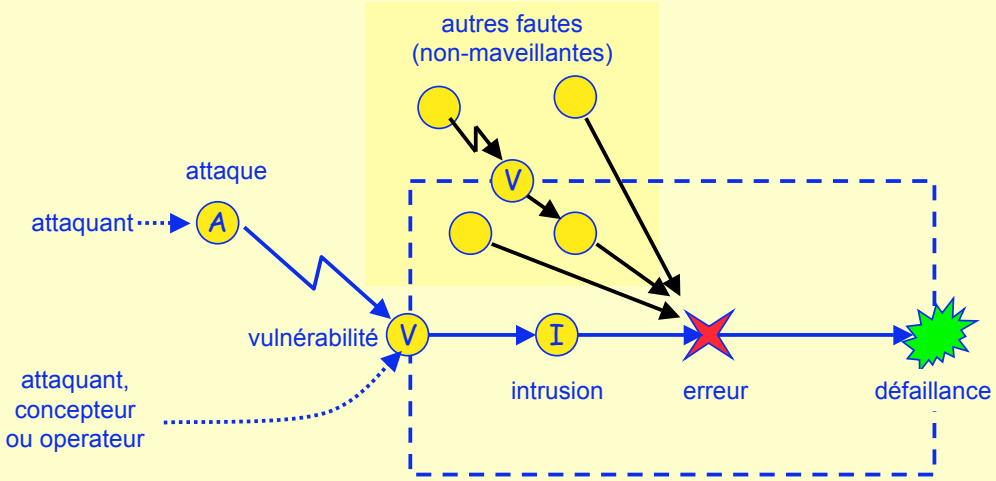
Intrusions

Les intrusions résultent d'attaques
réussies (au moins partiellement)



Système informatique

Modèle de faute



- **attaque** - activité malveillante externe visant à violer une ou plusieurs propriétés de sécurité; une tentative d'*intrusion*
- **vulnérabilité** - faute (par malveillance ou maladresse), dans les spécifications, la conception, la réalisation, l'installation ou la configuration du système, ou dans la façon de l'utiliser, qui peut être exploitée pour produire une *intrusion*
- **intrusion** - faute (malveillante) résultant d'une *attaque* qui a réussi à exploiter une *vulnérabilité*

Méthodes de sûreté de fonctionnement

FOURNITURE

Prévention des fautes - comment empêcher que des *fautes* surviennent ou soient introduites

Tolérance aux fautes - comment fournir un service conforme à la fonction en dépit des *fautes*

VALIDATION

Élimination des fautes - comment réduire la présence (en nombre ou en gravité) des *fautes*

Prévision des fautes - comment estimer la présence, la création et les conséquences des *fautes*

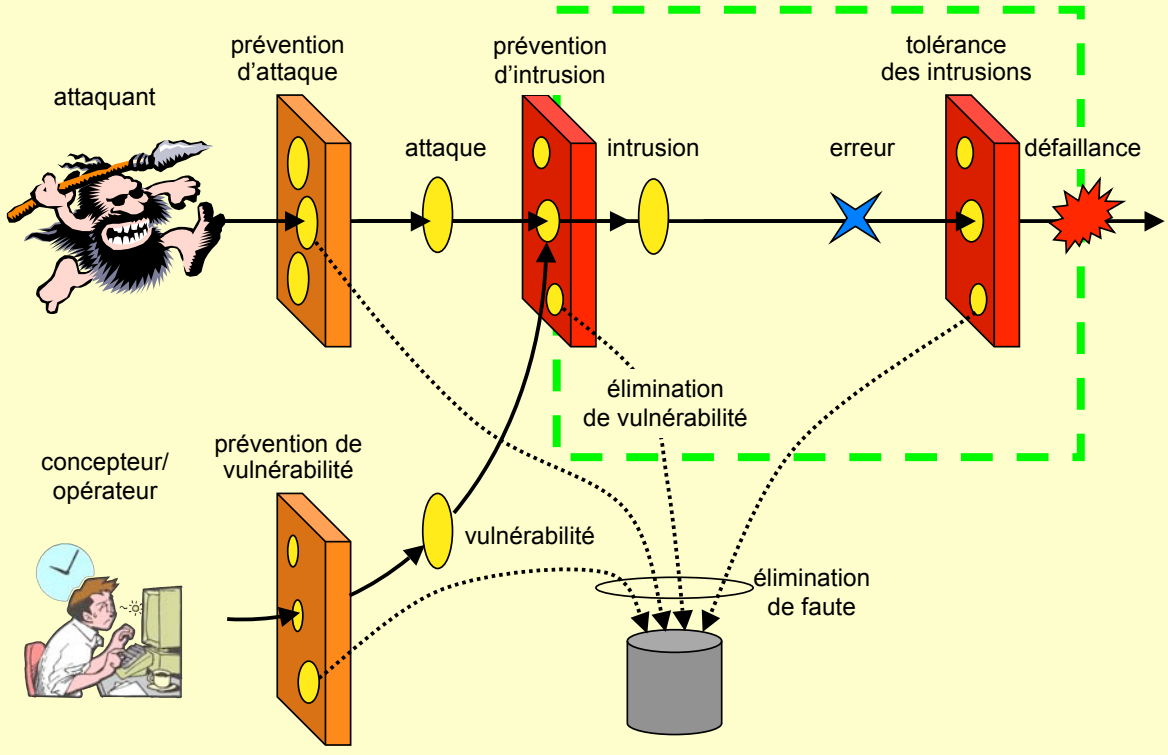
Éviter les fautes

Accepter les fautes

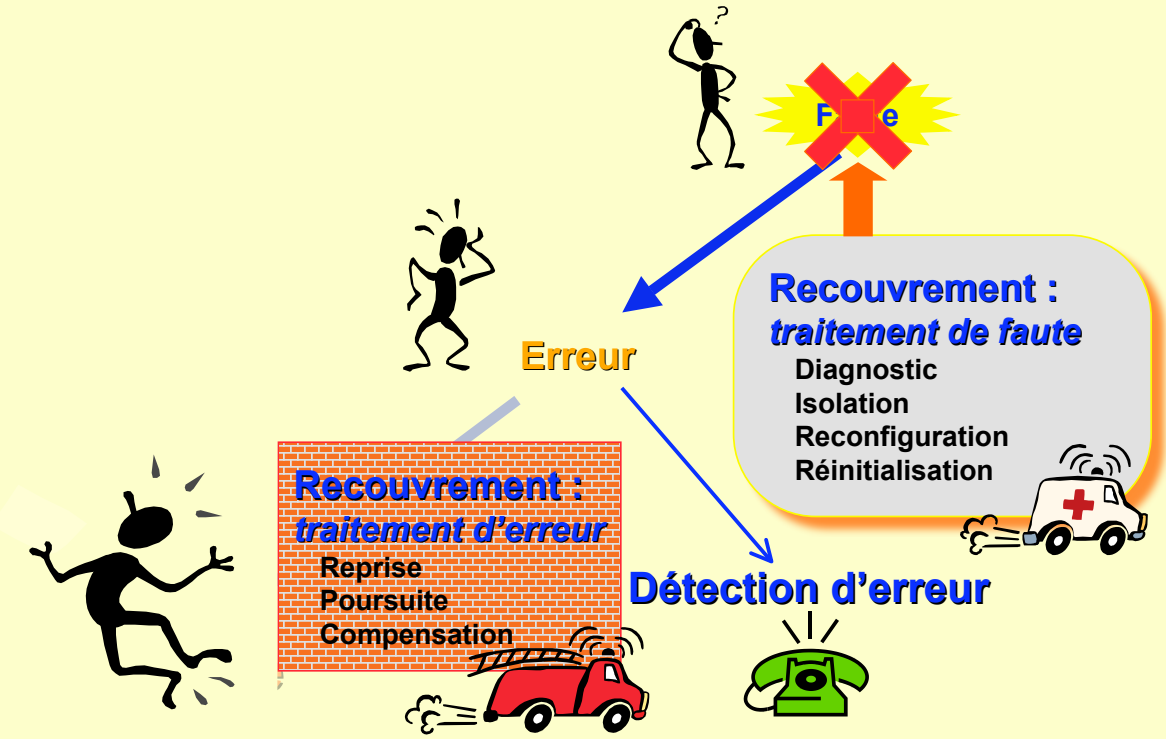
Méthodes de sécurité

Faute	Attaque (au sens humain)	Attaque (sens technique)	Vulnérabilité	Intrusion
Prévention (comment empêcher que des *fautes* surviennent …)	dissuasion, législation, pression sociale, surveillance, …	pare-feux, authentification, autorisation…	spécification semi-formelle ou formelle, conception rigoureuse, …	= prévention et élimination des attaques et des vulnérabilités
Tolérance (comment fournir un service conforme …)	= prévention et élimination des vulnérabilités tolérance aux intrusions		= prévention et élimination des attaques tolérance aux intrusions	détection et correction d'erreur, masquage de faute, détection d'intrusion & réaction, traitement de faute
Élimination (comment réduire le nombre ou la gravité …)	contre-mesures physiques, capture de l'attaquant	maintenance préventive et corrective pour éliminer les agents d'attaque (c-à-d, logique malicieuse)	1.preuve formelle, vérification de modèle, inspection, test… 2. maintenance préventive et corrective, dont patches de sécurité	⊆ élimination des attaques et vulnérabilités
Prévision (comment estimer la présence, la création …)	renseignement, estimation des menaces…	estimation de la présence d'agents d'attaques dormants et des conséquences éventuelles de leur activation	estimation de la présence de vulnérabilités, de la difficulté à les exploiter, des conséquences éventuelles…	= prévision des attaques et vulnérabilités

Prévention, tolérance et élimination



Tolérance aux fautes



Détection d'erreur

Vérification de propriétés

L'état du système ou ses transitions vérifient des propriétés (ou des règles)

- instructions/commandes inexistantes ou interdites
- adresses inexistantes
- mode d'accès interdit
- chiens de garde
- contrôle de vraisemblance
- codes détecteur d'erreur
- vérification de modèle à l'exécution
- …

Faible coût en redondance

Vérification par comparaison

En absence de faute, plusieurs exécutions en parallèle ou en série doivent donner un même résultat

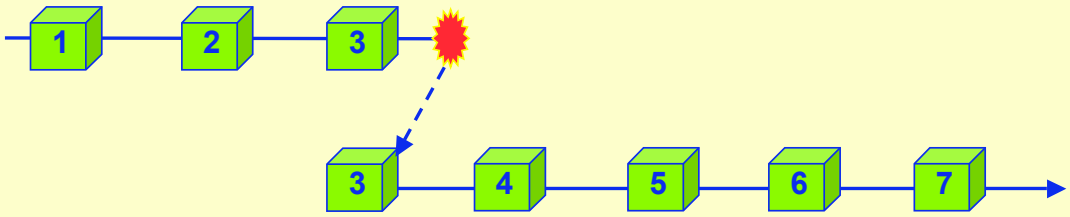
- nécessite des exécutions déterministes et des entrées équivalentes
- suppose une indépendance de fautes entre les exécutions

  - ✦fautes matérielles ⇒ exemplaires identiques
  - ✦fautes externes ⇒ dissimilarité
  - ✦fautes de conception ⇒ diversification

Coût élevé en redondance

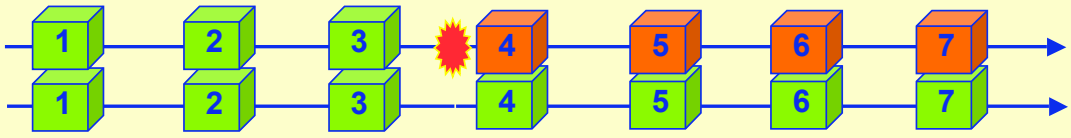
Traitement d'erreur

Reprise



Poursuite

Compensation (masquage)



Tolérance aux intrusions

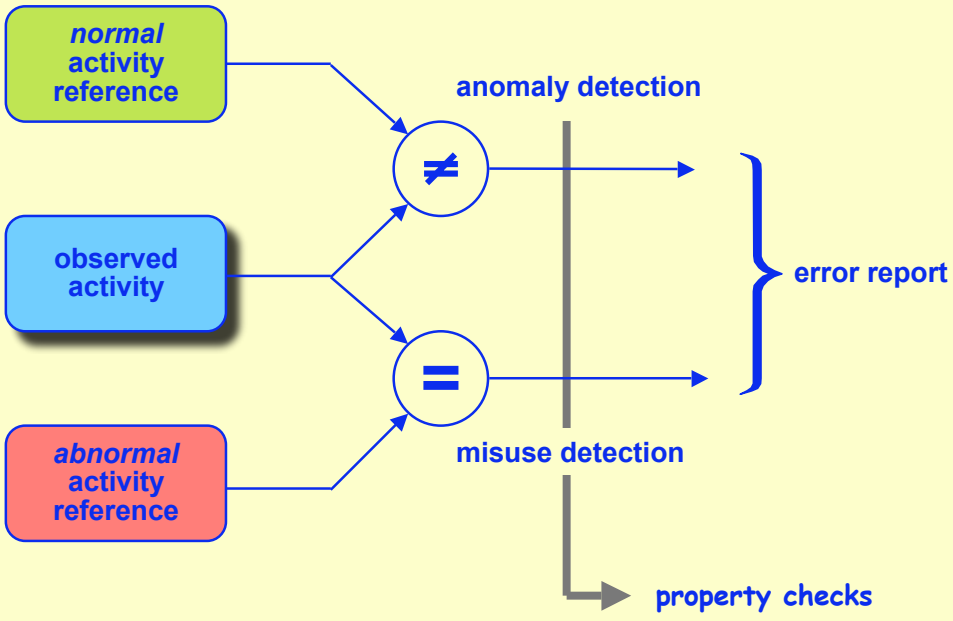
- Les intrusions sont des fautes
- Les fautes peuvent être tolérées

- Mais:
  - on ne peut pas se reposer sur la faible probabilité d'attaques presque simultanées sur différentes parties du système !
- Il faut donc s'assurer que :
  - chaque partie est suffisamment protégée (pas d'attaque triviale)
  - l'intrusion d'une partie ne facilite pas l'intrusion d'autres parties
    - ↪ une intrusion ne doit pas révéler des données confidentielles

Détection et traitement d'erreur préemptifs

- Rechercher des erreurs latentes et des fautes dormantes
- Pour les fautes accidentelles
  - test périodique (auto-test intégré)
  - balayage mémoire, …
- Interprétation vis-à-vis des malveillances
  - tests de vulnérabilités
  - vérification de configuration
  - procédures de rafraîchissement de clés, …

Détection d'intrusion et détection d'erreur



Recouvrement pour tolérer les intrusions

Traitement d'erreur

- **Reprise**
  - restauration depuis sauvegarde
  - reset des connexions TCP/IP
- **Poursuite**
  - reconstituer un état « sûr »
    - reboots du système
    - ré-installation du système
  - commuter sur un mode « sain »
- **Compensation**
  - mécanismes de vote
  - corrélation de capteurs d'IDS
  - fragmentation-redondance-dissémination

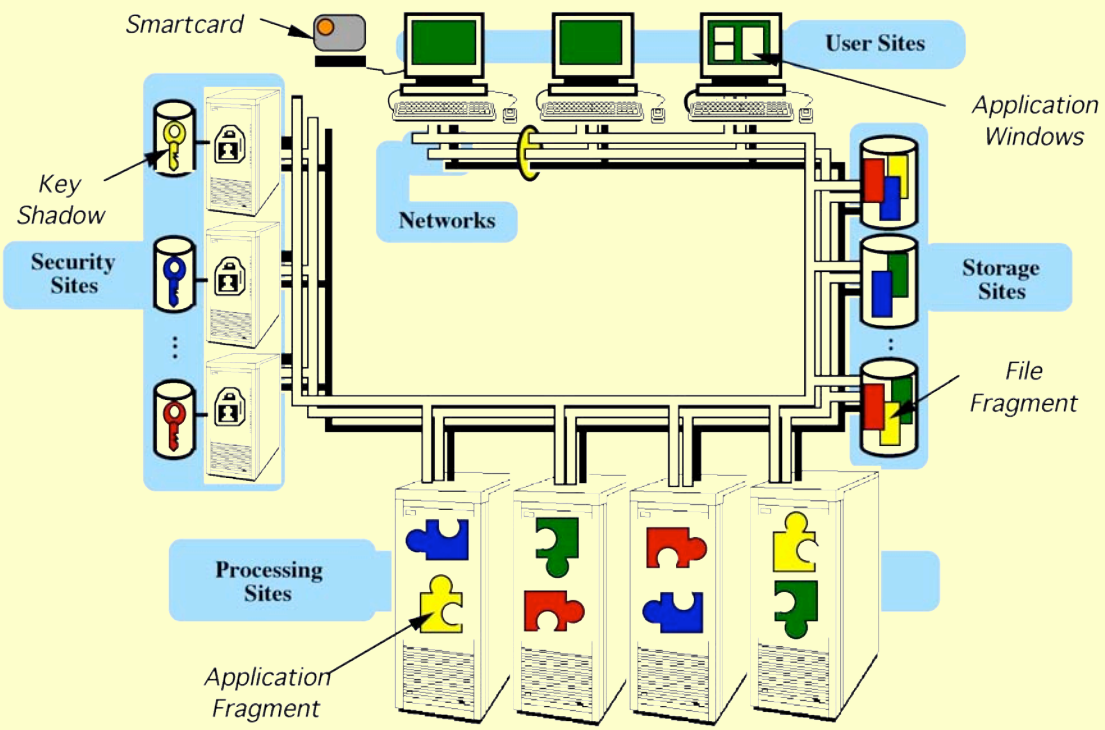
Traitement de faute

- **Diagnostic**
  - intrusions, vulnérabilités et attaques
- **Isolation**
  - zones corrompues
  - logiciels vulnérables
- **Reconfiguration**
  - mise à jour des logiciels ou retour à des versions anciennes
  - ajustement du seuil de vote

Masquage d'intrusion

- **Une intrusion dans une partie du système ne doit donner accès qu'à des informations non-significatives**
- **FRD : Fragmentation-Redondance-Dissémination**
  - Fragmentation: fragmenter l'information de telle sorte qu'un fragment isolé ne contienne pas d'info sensible : confidentialité
  - Redondance : ajouter de la redondance de telle sorte que la modification ou destruction de fragments n'empêche pas les accès légitimes : intégrité + disponibilité
  - Dissémination : isoler les fragments individuels
    - topologie/fréquences
    - temps
    - privilèges

Fragmentation-Redondance-Dissémination



Projet MAFTIA

FP5 IST Dependability Initiative
Cross Program Action
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
DSTL + QinetiQ (ex-DERA) (UK)	Tom McCutcheon, Sadie Creese
University of Saarland (D)	Birgit Pfitzmann
LAAS-CNRS, Toulouse (F)	Yves Deswarte, David Powell
IBM Research, Zurich (CH)	Marc Dacier, Michael Waidner

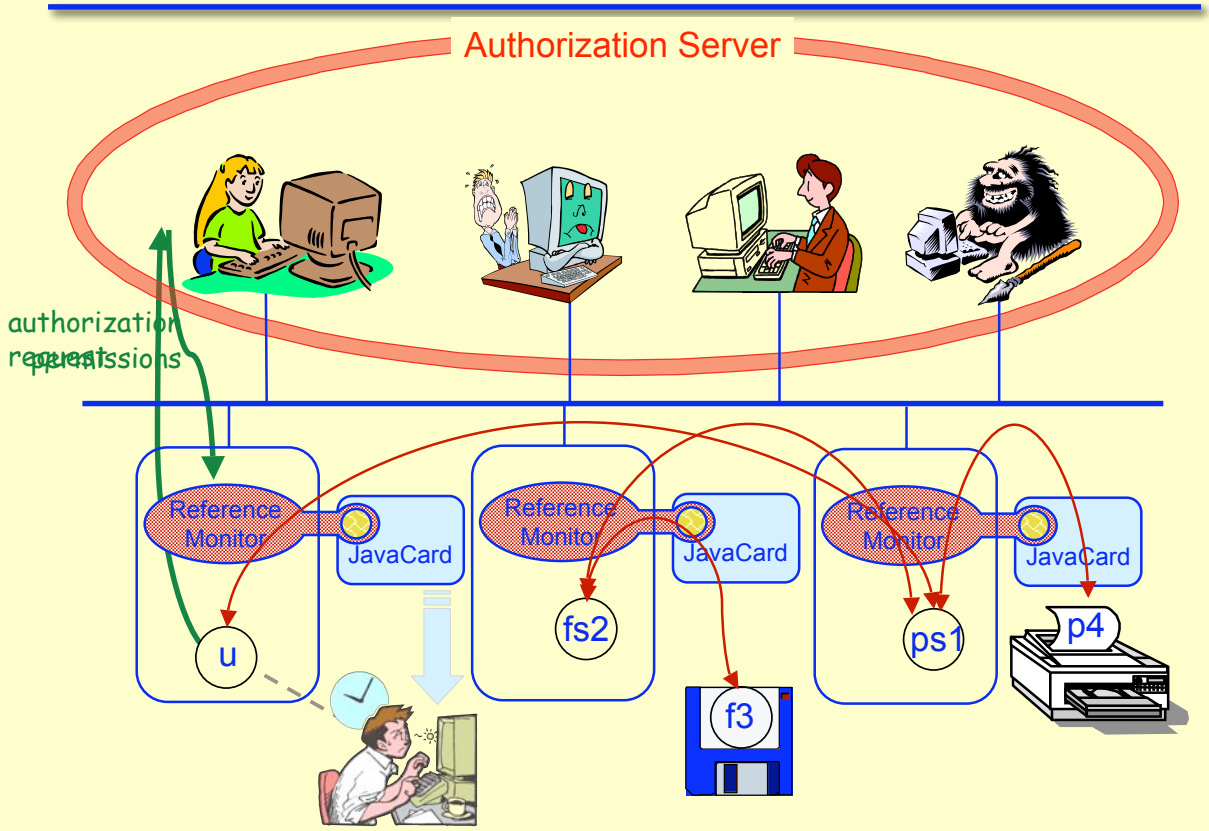
~ 55 personnes-ans, finacement CE ~2.5M€
Jan. 2000 -> Déc. 2002 (Fév. 2003)

Résultats obtenus par MAFTIA

- Cadre conceptuel et modèle d'architecture
- Mécanismes et protocoles :
  - **Intergiciel (*middleware*) pour la tolérance aux intrusions**
    - communications multicast (ordre causal, temps-réel) sécurisées
  - **Système de détection d'intrusion à large échelle**
  - **Tierces parties de confiance tolérant les intrusions**
  - **Mécanismes d'autorisation distribuée (TAI)**
- Validation et évaluation

http://www.maftia.org/

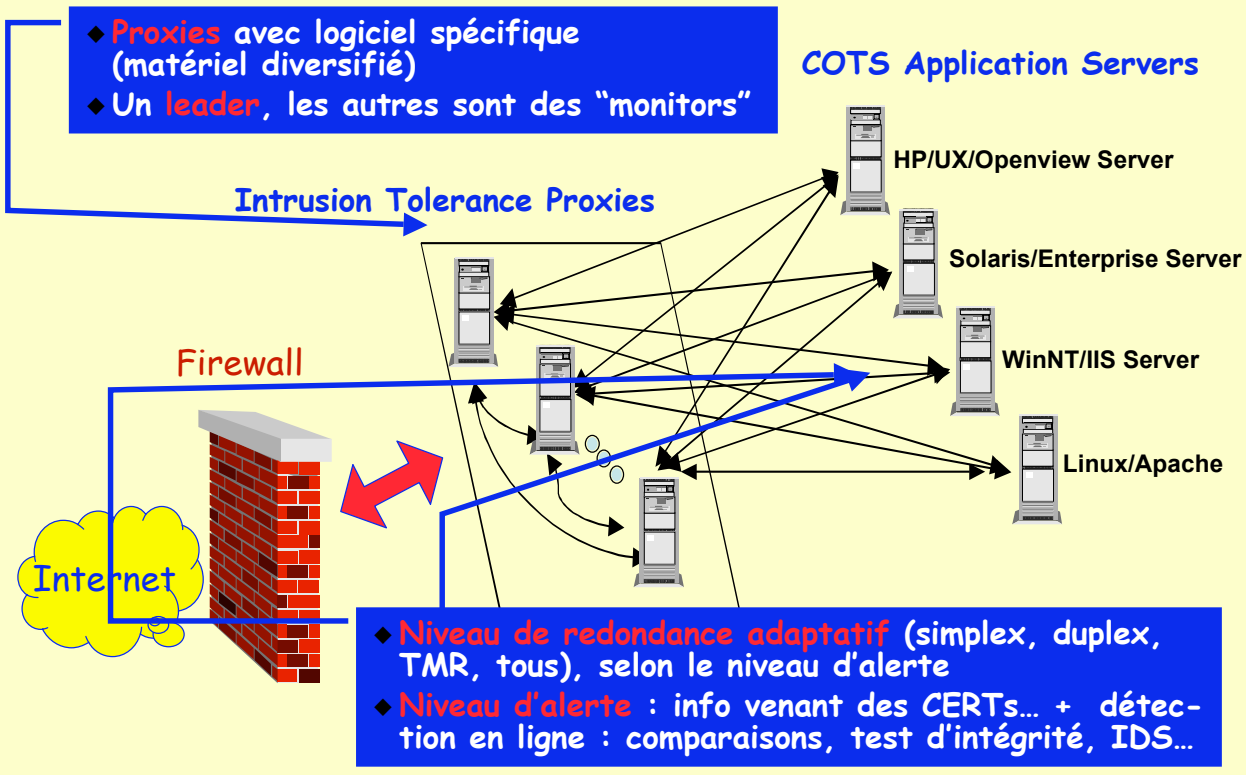
Schéma d 'autorisation MAFTIA



Projet DIT

- DIT = Dependable Intrusion Tolerance
- Programme DARPA OASIS (Organically Assured and Survivable Information Systems)
- En partie sous-contracté au LAAS par SRI-International
- Conception et réalisation d'un serveur Web tolérant les intrusions

Architecture DIT



Conclusion (1)

- Étant donnés
  - le taux d'attaques actuel sur Internet
  - le grand nombre de vulnérabilités des systèmes courants
- la tolérance aux intrusions est une technique prometteuse
  - compatible avec les systèmes classiques (COTS)
  - avec une redondance matérielle modérée et peu de logiciel spécifique
- mais coûteuse
  - support de plateformes multiples et diversifiées
    ⇒ indépendance de vulnérabilité
  - opérateurs/administrateurs indépendants
    ⇒ tolérance des attaques internes
- Est-ce le prix de la sécurité dans un monde ouvert et incertain?

Conclusion (2)

- Ca marche pour les systèmes d'entreprises (serveurs, B2B, web services, …)
- Quid des machines personnelles ?
  - Nombreuses vulnérabilités
  - Vers, virus, chevaux de Troie, portes dérobées, phishing… -> zombies
  - Spyware :
    80% des PC des entreprises ont au moins un spyware (en moyenne : 25)
- Quelle solution?
  - Responsabilité des fournisseurs (OS, FAI)
  - Difficile d'implémenter une solution TAI "massive"
  - Privilégier les outils de prévention/détection/recouvrement (reprise-poursuite)

Conclusion (3)

- **Systèmes critiques : safety/security**
  - Ex: Transport (aérien, ferroviaire, …), nucléaire, production chimique, …
- **Jusqu'à présent : safety**
  - Développement sûr : éliminer les fautes de conceeption
  - Tolérance aux défaillances de composants
  - Tolérance aux maladresses
  - ---> tolérance aux malveillances

Bibliographie

- Ludovic Mé & Yves Deswarte (sous la direction de)
  Sécurité des réseaux et des systèmes répartis (Tome 2)
  Traité IC2 série Réseaux, Hermès (éd.)
  parution prévue fin 2005