École Nationale Supérieure
des Télécommunications de Bretagne

ENST Bretagne

CRIM : un module de corrélation d'alertes et de réaction aux attaques

get

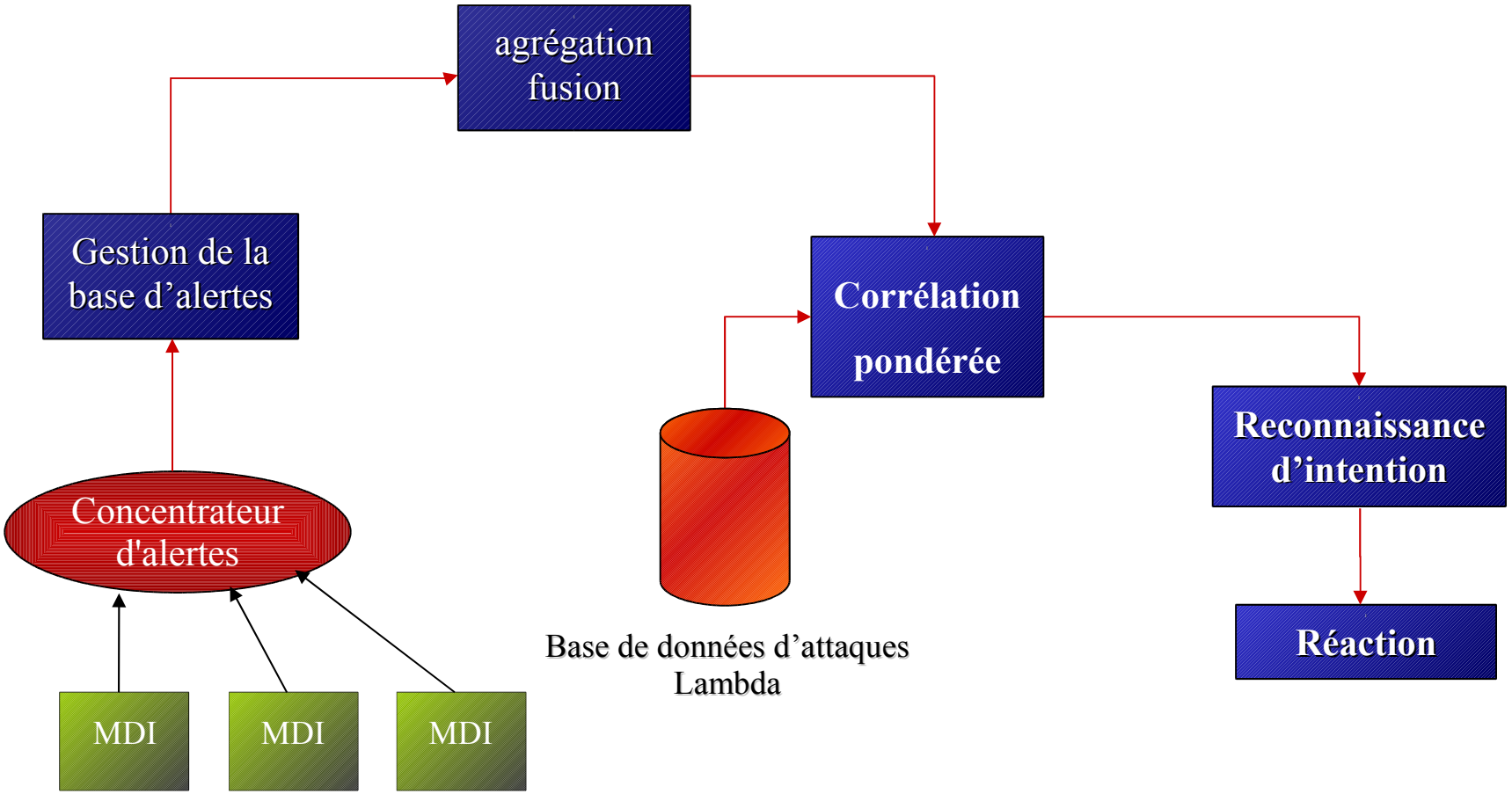
Contexte

- Détection d'intrusion
- Environnement coopératif: plusieurs MDIs coopèrent
- L'attaquant peut planifier son intrusion
  - Scénario d'intrusion

Objectifs de CRIM:

- Vision globale de l'attaque
- Anticiper les intentions de l'attaquant
- Réagir à une attaque achevée ou en cours

Architecture

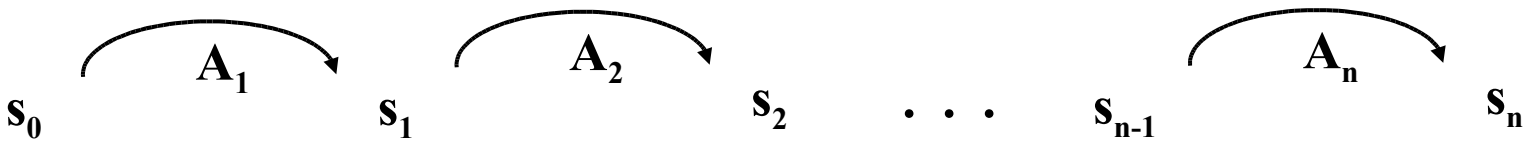


Agrégation/fusion d'alertes

- Objectifs
  - Regrouper les alertes redondantes
    - Plusieurs SDIs peuvent détecter le même événement
  - Regrouper les alertes similaires
    - Certaines attaques génèrent des paquets d'alertes
  - Obtenir une alerte globale a partir d'un ensemble d'alertes élémentaires en fusionnant les informations
- Approche de CRIM
  - Fonctions de similarité entre attributs
  - Pondération des valeurs de similarité en fonction de l'attaque

Corrélation d'alertes

- Modélisation de l'intrusion
  - Le processus d'intrusion: planification
    - L'attaquant a à sa disposition un ensemble d'actions
    - Il recherche un sous-ensemble d'actions lui permettant d'atteindre son objectif d'intrusion

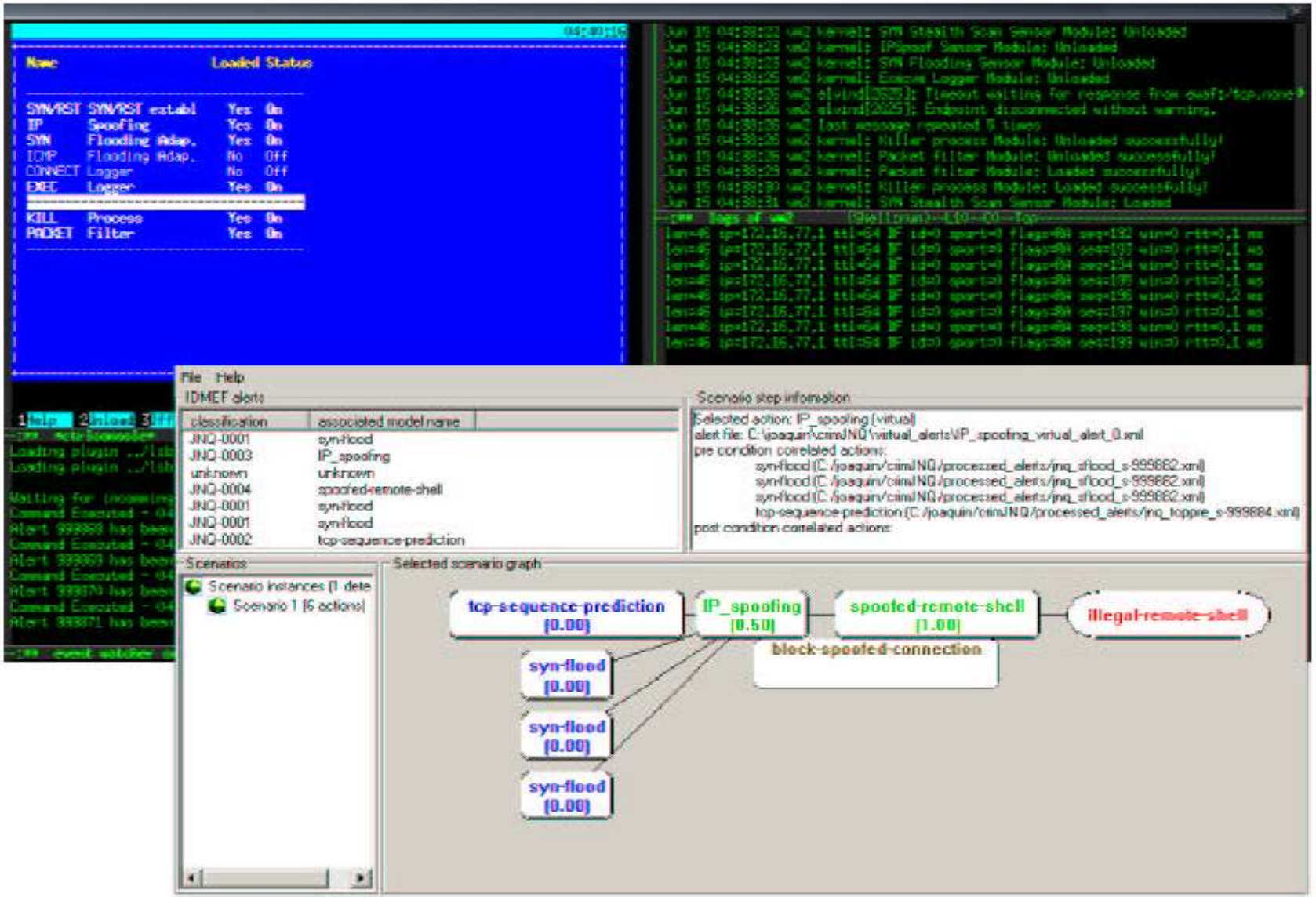


- S_0: état du système avant l'intrusion
- S_n: état du système dans lequel la politique de sécurité est violée

Corrélation d'alertes

- Différents types de corrélation
  - Corrélation implicite
    - Par fonctions de similarité
  - Corrélation explicite
    - Langage d'expression de scénarios (Chroniques)
    - Définition de règles (application EAS d'Exaprotect)
  - Approche CRIM : corrélation semi-explicite
    - Modélisation des actions élémentaires
    - Découverte automatique des liens entre alertes
    - Génération automatique des scénarios

Exemple


Name
Loaded Status
SYNRST SYNRST establ Yes On
IP Spoofing Yes On
SYN Flooding Adap. Yes On
ICMP Flooding Adap. No Off
CONNECT Logger No Off
EXEC Logger Yes On
KILL Process Yes On
PACKET Filter Yes On
File Help
IDMEF alerts
classification
associated model name
JNQ-0001 syn-flood
JNQ-0003 IP_spoofing
unknown unknown
JNQ-0004 spoofed-remote-shell
JNQ-0001 syn-flood
JNQ-0001 syn-flood
JNQ-0002 tcp-sequence-prediction
Scenario step information
Selected action: IP_spoofing (virtual)
post condition correlated actions:
Scenarios
Scenario instances (1 dete
Scenario 1 (6 actions)
Selected scenario graph
tcp-sequence-prediction (0.00)
IP_spoofing (0.50)
spoofed-remote-shell (1.00)
illegal-remote-shell
block-spoofed-connection
syn-flood (0.00)
syn-flood (0.00)
syn-flood (0.00)

Conclusion

- Implantation du prototype en C++
  - Algorithme d'agrégation en-ligne et hors-ligne
  - Corrélation pondérée, génération d'hypothèses, réaction (anti-corrélation)

- Travaux en cours
  - intégration de CRIM dans l'application EAS d'Exaprotect
    - ➢ coopération corrélation explicite (EAS) et semi-explicite (CRIM)

Pour plus d'infos:

application EAS : www.exaprotect.fr

CRIM : http://www.rennes.enst-bretagne.fr/~fcuppens/

Quelques publications sur CRIM

F. Cuppens et R. Ortalo.
LAMBDA: A Language to Model a Database for Detection of Attacks . Third International Workshop on Recent Advances in Intrusion Detection (RAID'2000). Toulouse, Octobre 2000.

F. Cuppens.
Managing Alerts in a Multi-Intrusion Detection Environment . 17th Annual Computer Security Applications Conference New-Orleans, 10-14 Décembre 2001.

F. Cuppens et A. Miège.
Alert correlation in a cooperative intrusion detection framework . IEEE Symposium on Research in Security and Privacy, Oakland, Mai 2002.

F. Autrel, S. Benferhat et F. Cuppens.
Utilisation de la corrélation pondérée dans un processus de détection d'intrusion . Annales des Télécommunications, éditions Hermes. 2004.

J. García, F. Autrel, J. Borrell, S. Castillo, F. Cuppens et G. Navarro.
Decentralized publish-subscribe system to prevent coordinated attacks via alert correlation . Sixth International Conference on Information and Communication Security (ICICS). Malaga, Espagne, October 2004.