

Plate-forme de détection d'intrusions Orchids

*Analyse et corrélation temporelle
d'évènements en temps réel.*

LSV - ENS de Cachan & CNRS UMR 8643 & INRIA Futurs projet SECSI

<http://www.lsv.ens-cachan.fr/orchids/>

Plan

- Sécurité des systèmes d'information.
- La plate-forme de détection d'intrusion Orchids.
- Présentation technique.
- Démonstration.



Jean Goubault-Larrecq



Julien Olivain



Jean Goubault-Larrecq



Julien Olivain

Equipes sur des thèmes proches

Projet  LANDE,  **IRISA**
institut de recherche en informatique
et systèmes aléatoires] IRISA / INRIA

détection d'intrusions.

Projet Gemo , *Futurs*:

continuous data streams.

Sécurité en général:

LOGICAL, TANC, POPS (*Futurs*)

CASSIS, MADYNES (Nancy)

VASY (Rhône-Alpes)

MOSCOVA (Rocquencourt)

MIMOSA, LEMME, OASIS (Sophia)

Sécurité des systèmes d'information

- Virus, vers, chevaux de troie, buffer overflows, etc.
(attaques système)
- Dénis de service, IP/ARP spoofing, sniffing, etc.
(attaques réseau)
- Attaques sur formulaires http (perl, pgp), insertion SQL, virus [vers] Internet Explorer/Word, etc.
(attaques applicatives)

Évolution actuelle

- Systèmes plus vastes.

Sécurité plus difficile à assurer.

- Enjeux plus grands.

Bases de données en ligne [banque, santé, impôts, ...],
commerce électronique, etc.

- Attaques plus complexes (automatisées et distribuées).

Packages tout prêts [via Google]

Attaques nécessitant de nombreuses étapes,
... toutes bénignes individuellement

- Nouveaux besoins de détection d'intrusions

Tracking de configs utilisateur

Détection de fraudes

Cartes à puce

Attaque de démonstration

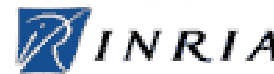
- Exploitation d'un problème d'héritage de permissions et de l'appel système `ptrace()`.
 - ... l'appel système utilisé par tous les debuggers [bénin!]
 - ... même Linux n'est pas sûr (il n'y a pas que Windows)
 - ... attaque subtile, fondée sur une race condition dans le noyau
- Plus de détails dans la partie technique!

Plan

- Sécurité des systèmes d'information.
- La plate-forme de détection d'intrusion Orchids.
- Présentation technique.
- Démonstration.

Projet Orchids

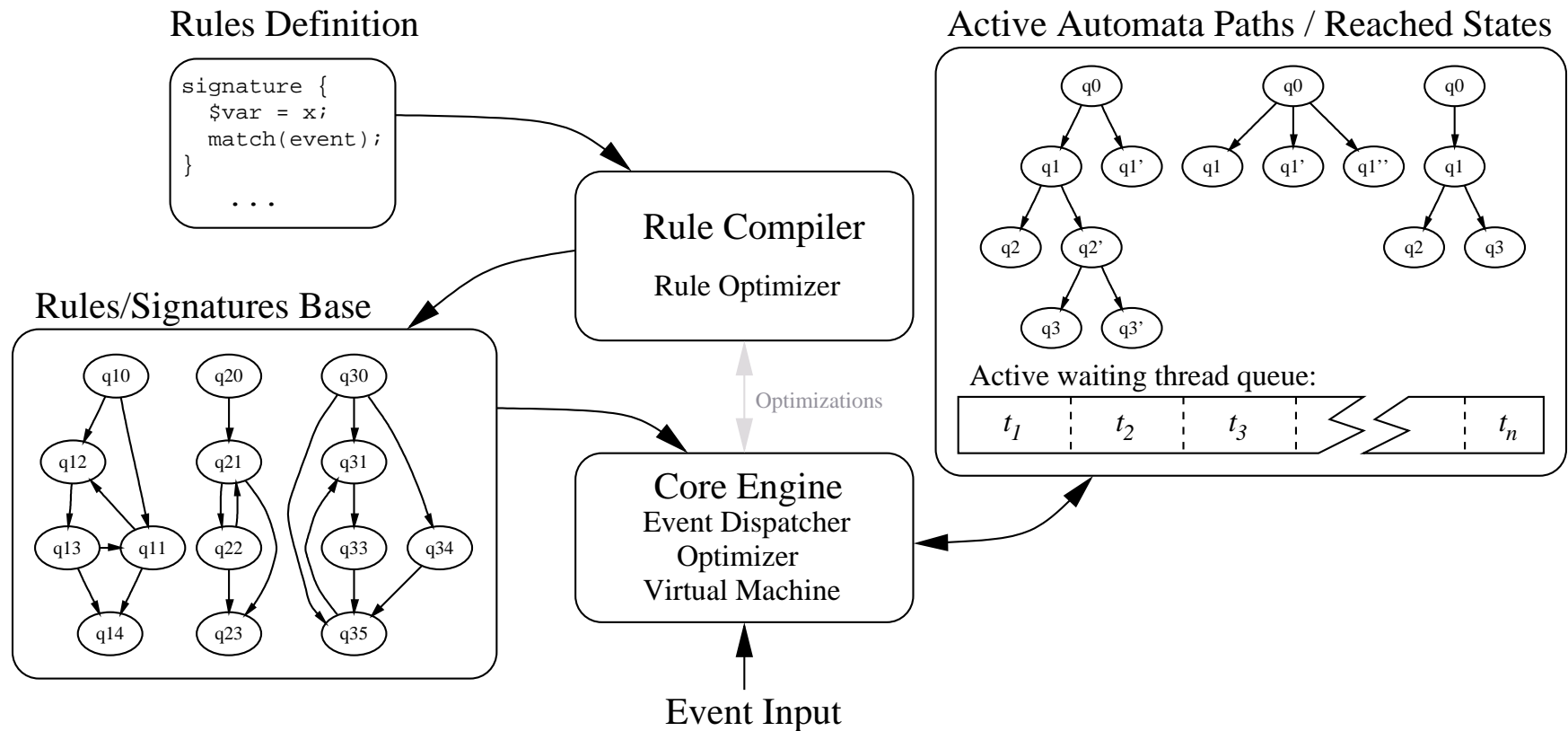
Débuté en 2003 dans le projet RNTL DICO.



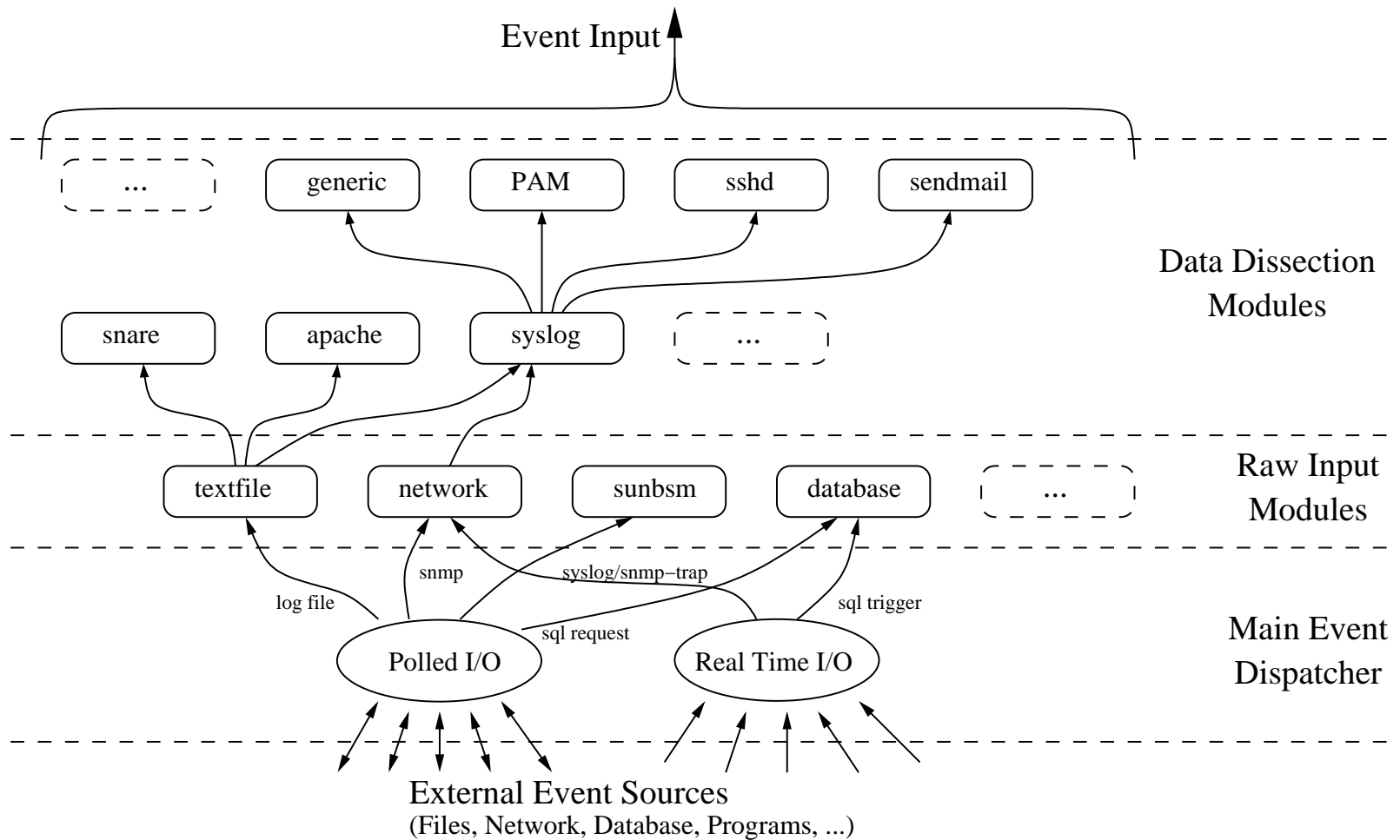
Orchids: Détection générique

	Hôte	Réseau	Application
Recherche explicite (“misuse”)	•	•	•
Vérification (“anomaly”)	•	•	•
	Temps réel (“online”)	Différé (“offline”)	
	•	•	

Architecture de la plate-forme Orchids



Hiérarchie de modules d'entrée



Sources d'entrée d'Orchids

Multi-équipements:

- Audit d'appel systèmes (*Raw Snare*).
- Évènements/journaux *Cisco*.
- Journaux système *Unix* (*Syslog*).
- Journaux système *MS Windows* (*MS EVT*).
- Informations de supervision d'équipements (*SNMP*).
- Informations réseau (*Linux NetFilter Firewall*).
- Autres...

Architecture modulaire...

En cours de développement: BSM.

Plan

- Sécurité des systèmes d'information.
- La plate-forme de détection d'intrusion Orchids.
- Présentation technique.
- Démonstration.

Spécification de scénarios d'attaques

- Trois niveaux de langages de spécification de signatures d'attaque:
 - 1) Spécification d'automates;
 - 2) Logique temporelle;
 - 3) Logique d'intervalles.
- Compilation vers un *bytecode* efficace.

Spécification de scénarios d'attaques

- Logique temporelle linéaire élémentaire:
 - Relations entre dates;
 - Succession;
 - Égalité / Proximité;
 - Horloges de référence / Propagation d'incertitude.

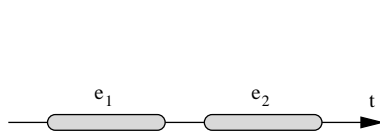
Spécification de scénarios d'attaques

- Logique d'intervalles

- Relations entre instances d'évènements proches de celles d'un langage *naturel*

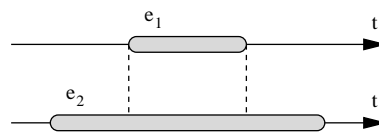
à la J.Allen

- Permet notamment de gérer les *événements synthétiques*.



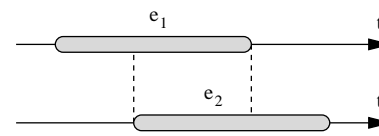
e1 avant e2

e2 après e1



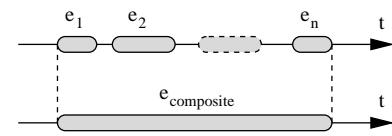
e1 pendant e2

e2 contient e1



e1 recouvre e2

e2 est recouvert par e1



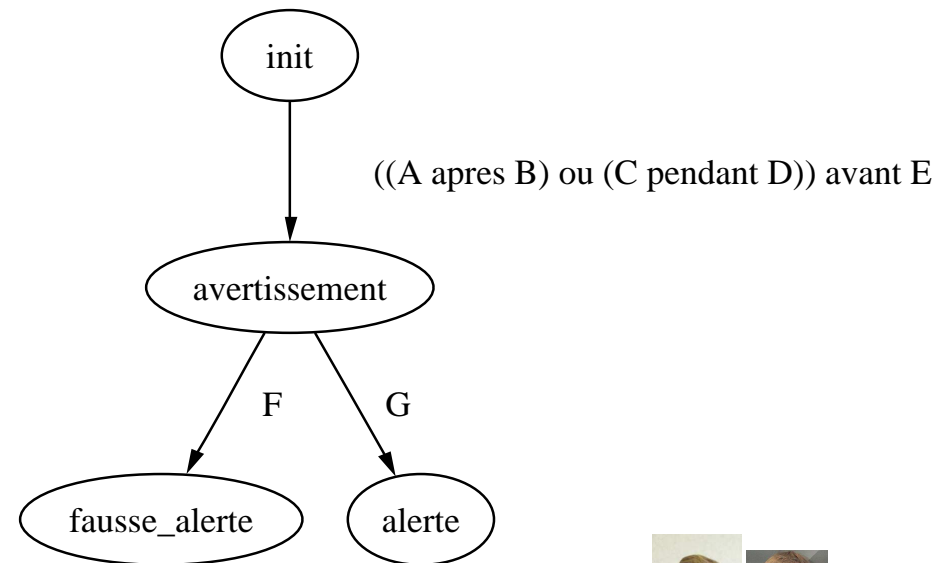
compose(e1, ..., en)

Exemple de scénario

```
rule demo_rule {  
  state init {  
    if (((A after B) or (C while D)) before E)  
      goto warning  
  }  
}
```

```
state warning {  
  warn("possible attack");  
  if (F) goto false_positive;  
  if (G) goto alert;  
}
```

```
state alert {  
  alert("attack!!!");  
}  
[...]
```

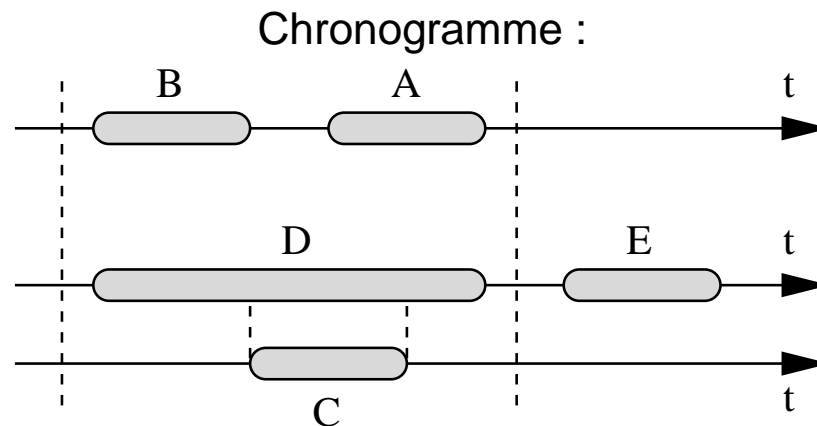


Exemple de scénario

Relation dans la logique d'intervalles :
((A après B) ou (C pendant D)) avant E

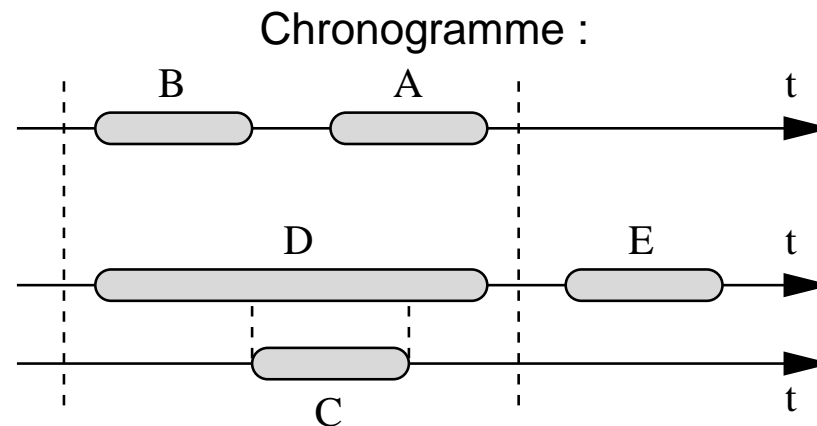
Exemple de scénario

Relation dans la logique d'intervalles :
((A après B) ou (C pendant D)) avant E



Exemple de scénario

Relation dans la logique d'intervalles :
 $((A \text{ après } B) \text{ ou } (C \text{ pendant } D)) \text{ avant } E$



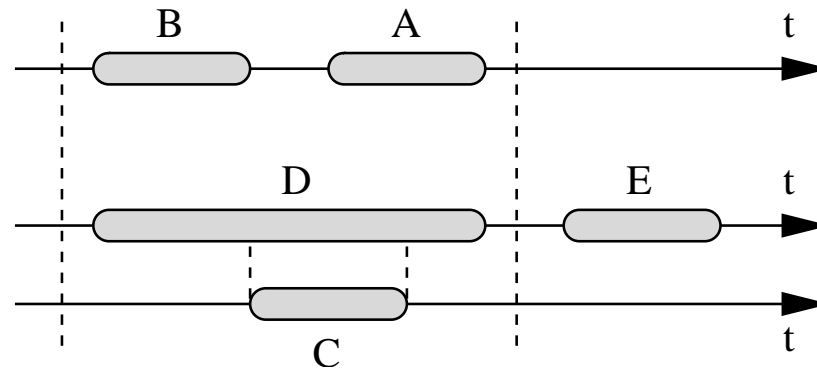
Relation dans la logique temporelle élémentaire :
 $((B^- ; B^+ ; A^- ; A^+) \text{ ou } (D^- ; C^- ; C^+ ; D^+)) ; E^- ; E^+$

Exemple de scénario

Relation dans la logique d'intervalles :

$((A \text{ après } B) \text{ ou } (C \text{ pendant } D)) \text{ avant } E$

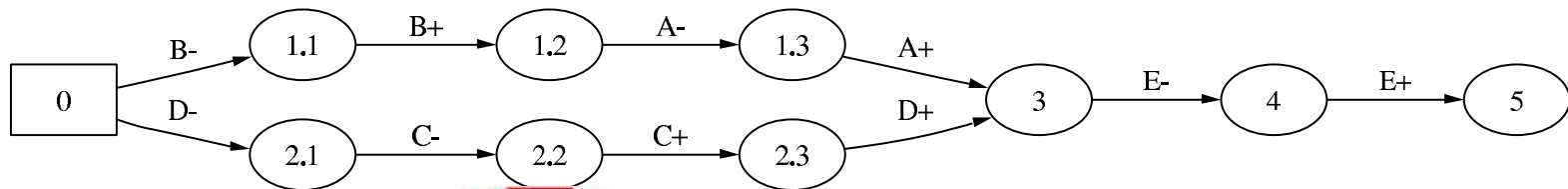
Chronogramme :



Relation dans la logique temporelle élémentaire :

$((B^- ; B^+ ; A^- ; A^+) \text{ ou } (D^- ; C^- ; C^+ ; D^+)) ; E^- ; E^+$

Automate :



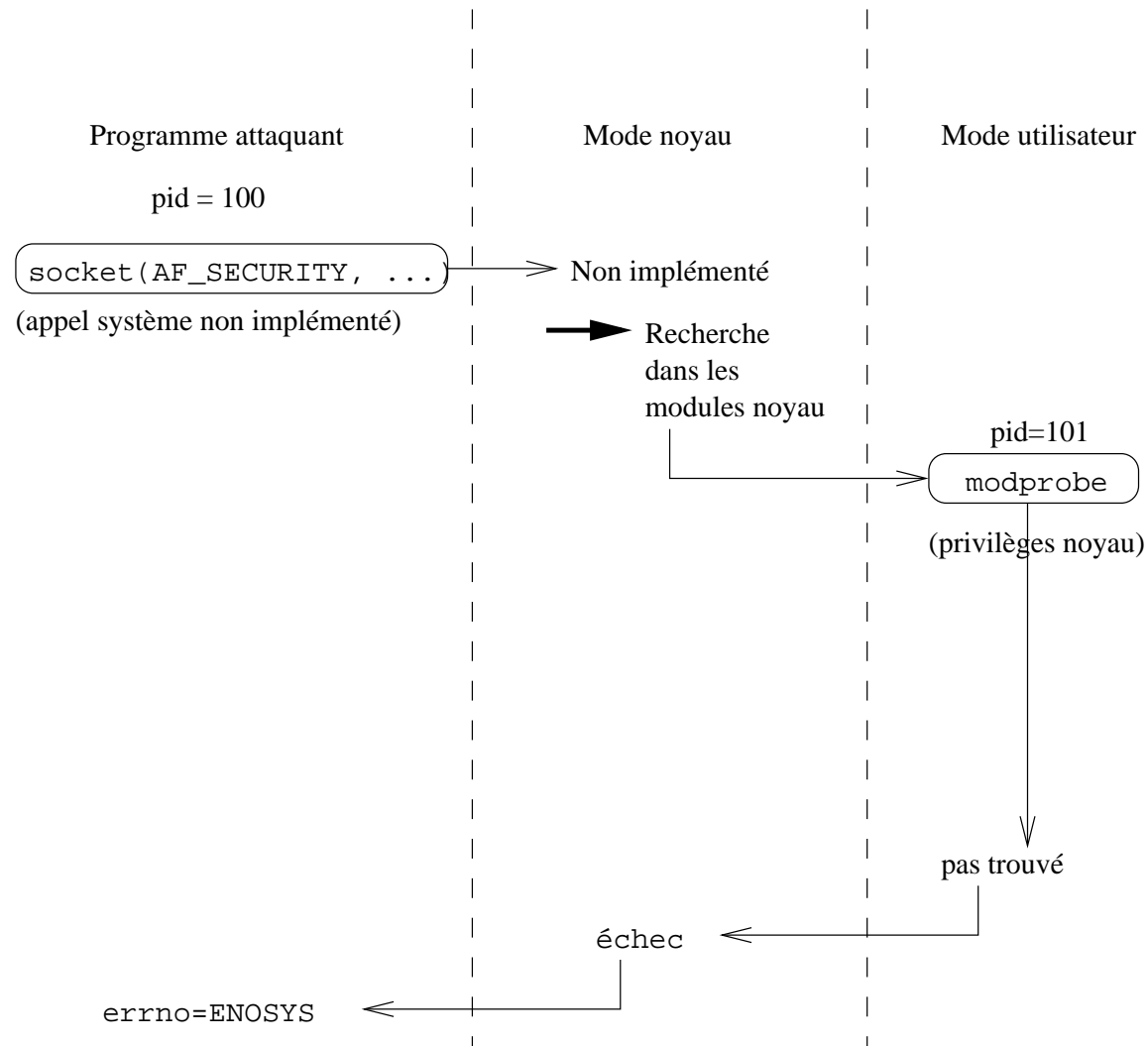
Plan

- Sécurité des systèmes d'information.
- La plate-forme de détection d'intrusion Orchids.
- Présentation technique.
- Démonstration.

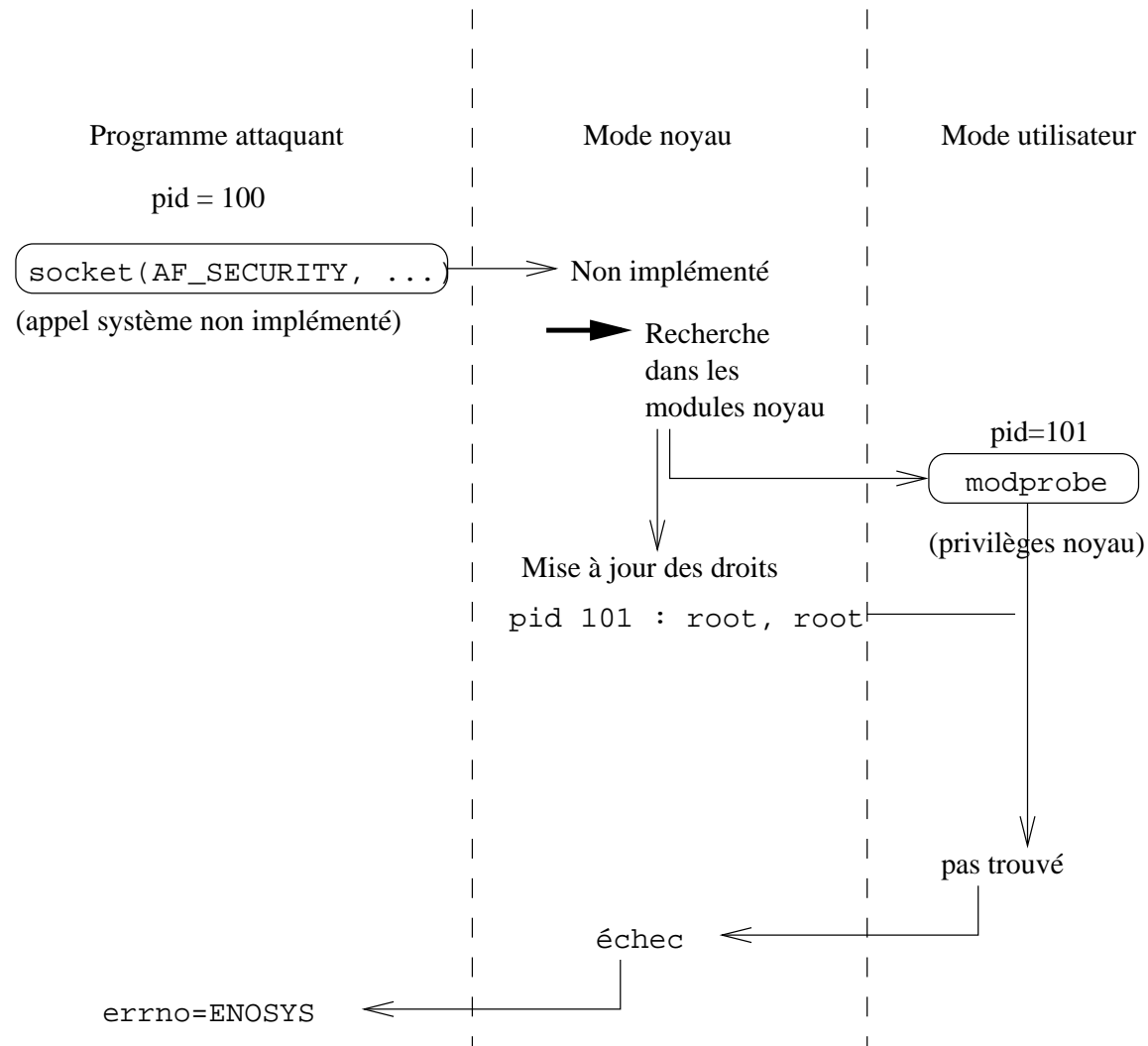
Attaque de démonstration

- Exploitation d'un problème d'héritage de permissions et de l'appel système `ptrace()`.
 - ... l'appel système utilisé par tous les debuggers [bénin!]
 - ... même Linux n'est pas sûr (il n'y a pas que Windows)
 - ... attaque subtile, fondée sur une race condition dans le noyau

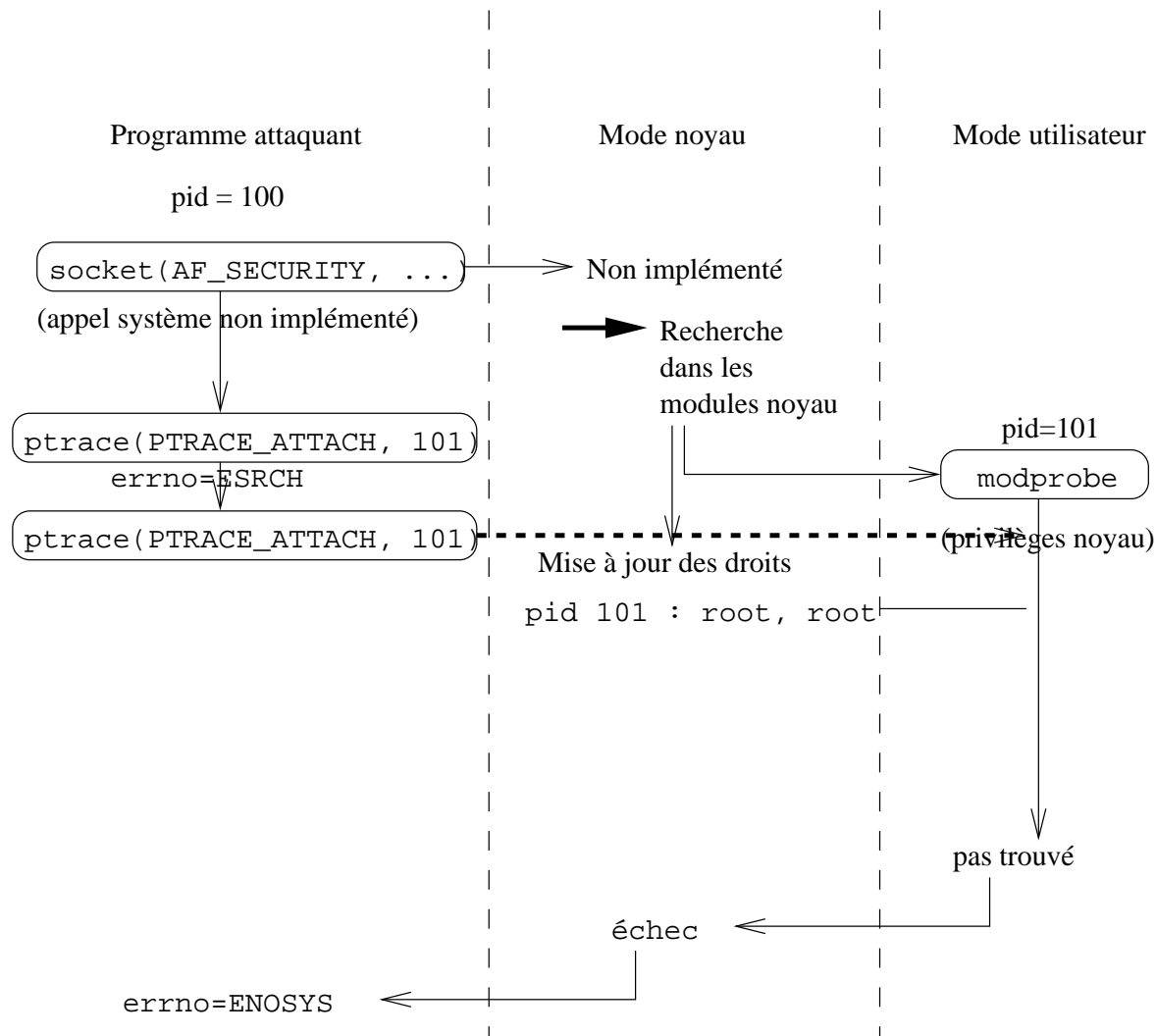
L'attaque ptrace (1)



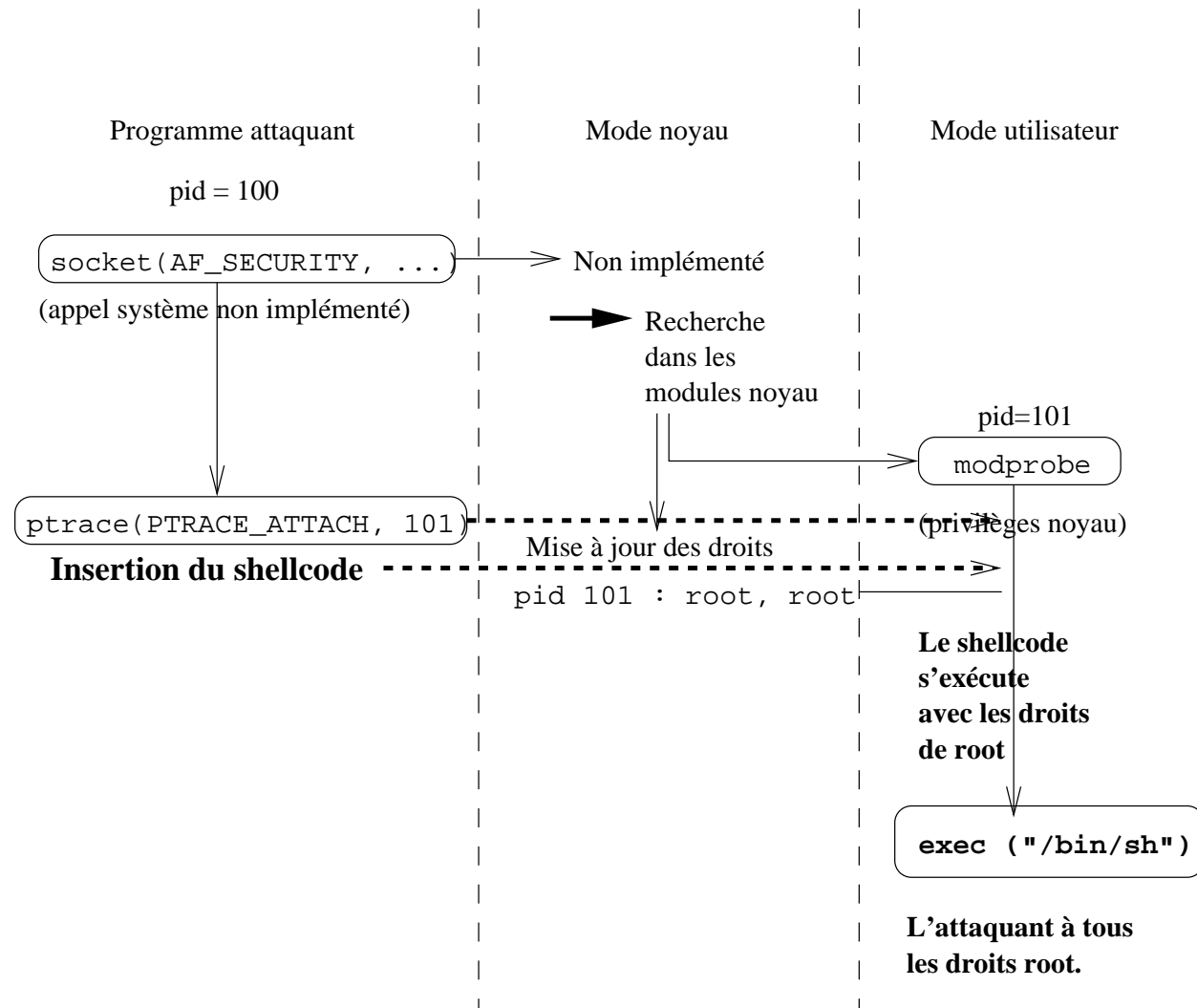
L'attaque ptrace (2)



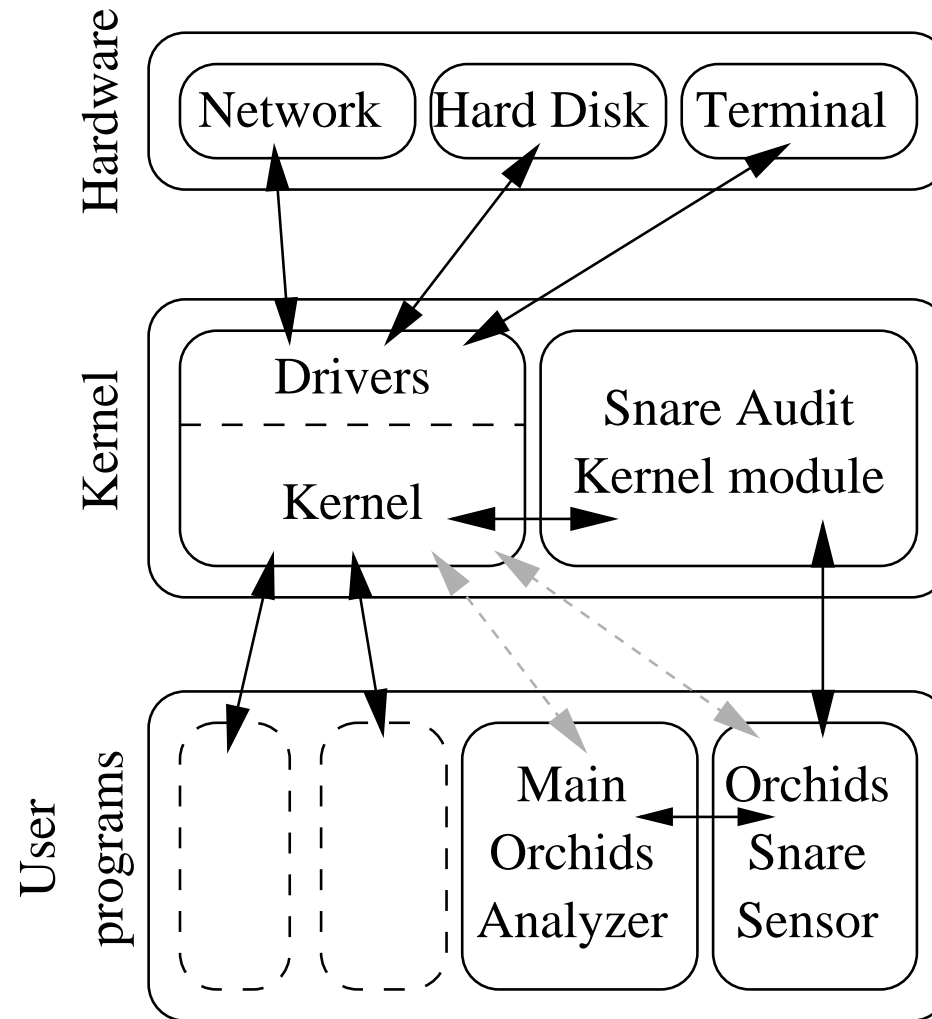
L'attaque ptrace (3)



L'attaque ptrace (4)

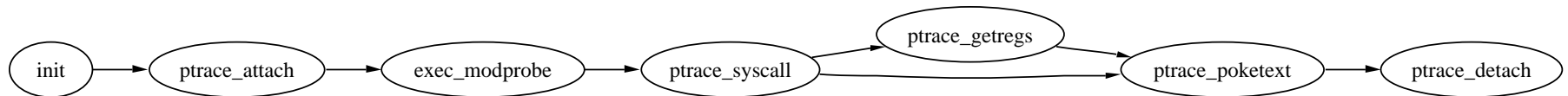


Détail de la démonstration



Résultats de la détection

Automate représentant le scénario:



États atteints par l'instance de l'alerte:

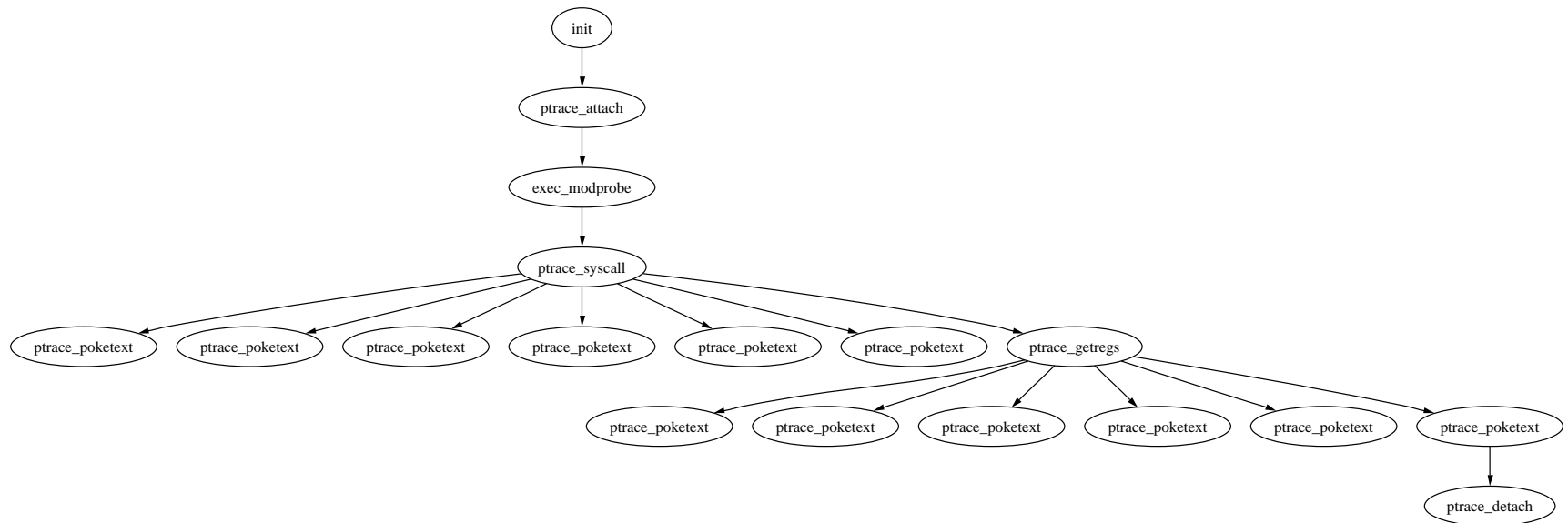


Plate-forme de détection d'intrusions Orchids

*Analyse et corrélation temporelle
d'évènements en temps réel.*

LSV - ENS de Cachan & CNRS UMR 8643 & INRIA Futurs projet SECSI

<http://www.lsv.ens-cachan.fr/orchids/>