

MÉTHODES ET OUTILS DE LA DÉTECTION D'INTRUSIONS

Ludovic Mé

`lme@supelec-rennes.fr`

`http://www.supelec-rennes.fr/rennes/si/equipe/lme/`

Supélec

BP28

35511 Cesson-Sévigné Cedex

tél.: 02.99.84.45.00

Prévention et correction des problèmes de sécurité

- Définir une politique de sécurité
- Mettre en œuvre cette politique
- Surveiller afin d'assurer le respect de la politique
 - Identifier les failles de sécurité issues d'une mauvaise configuration du système (contrôle des fichiers de conf. et des exécutable) ⇒ **surveillance statique**
 - Analyser *après coup* ce qui s'est produit (activités utilisateurs et/ou activités système) afin de détecter d'éventuelles intrusions ⇒ **surveillance dynamique**

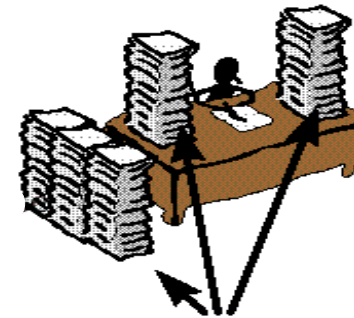
Vous avez dit "intrusion" ?

- Actions illégitimes par rapport à ce que définit la politique de sécurité
- Actions pouvant être entreprises par un utilisateur (légitime ou non) ou par un programme malveillants (virus, vers, bombe, cheval de Troie) et portant atteinte à la confidentialité, à l'intégrité ou à la disponibilité des services et des données :
 - Furetage, vol de données (lecture, copie, prise), exploitation d'un canal caché
 - Modification illégitime de données, destruction de données
 - Déni de service (réduction illégitime ou abusive des droits des usagers légitimes)

Pour une surveillance efficace

Problème

Il faut garder des traces de ce qui se passe \Rightarrow mécanisme de surveillance (audit, entre autres) \Rightarrow énorme volume de données \Rightarrow travail de dépouillement titanesque



Données à analyser

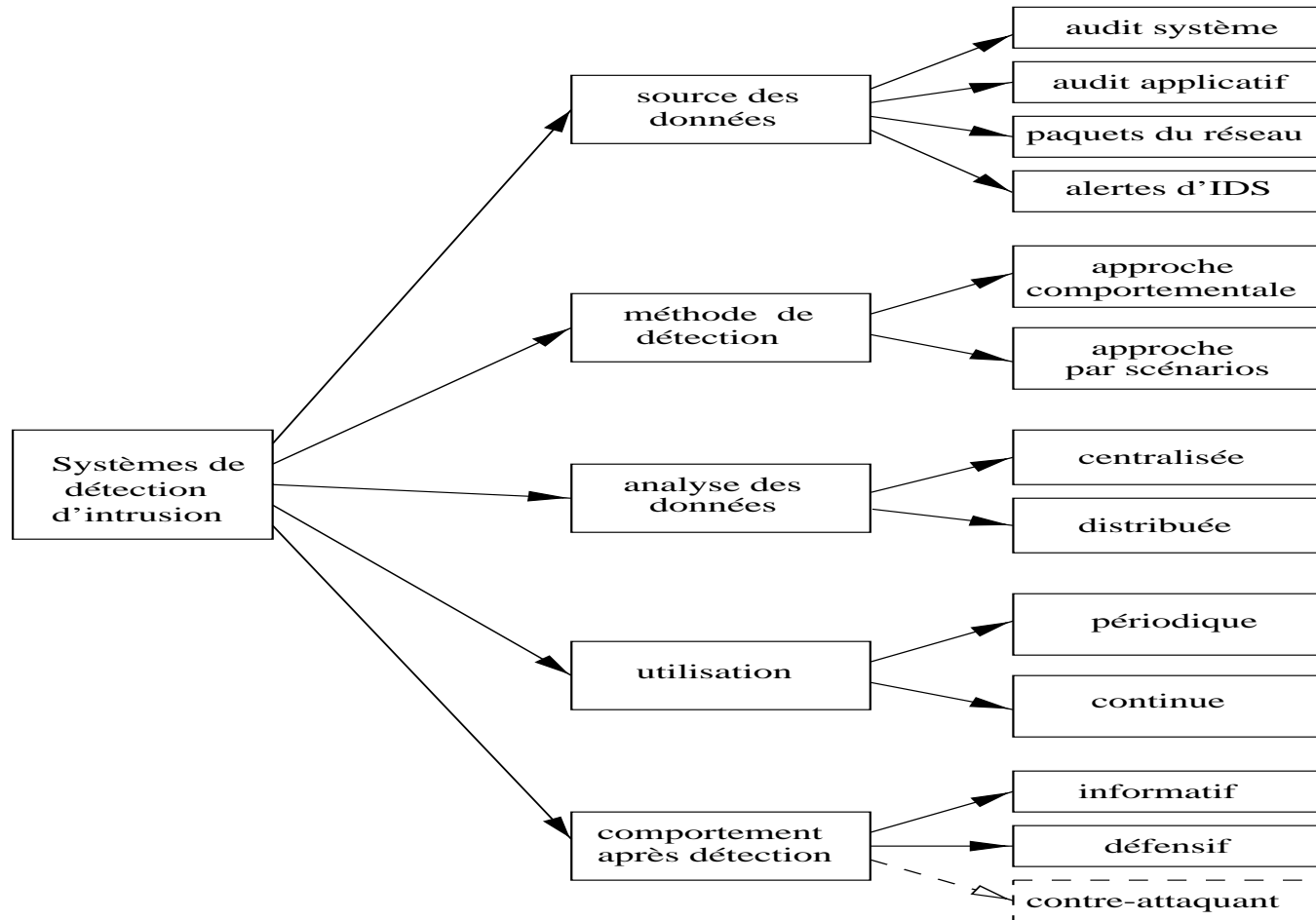
Conséquence

Automatiser le travail \Rightarrow offrir des outils (IDS, *Intrusion Detection Systems*)

Les IDS : des outils parmi d'autres

- un système d'authentification forte (biométrie, serveur d'authentification (kerberos, ...), etc.)
- du chiffrement (VPN, PKI, PGP, mécanismes intégrés à des protocoles de communication (IPSec), ...)
- un firewall
- un logiciel anti-virus
- un outil de détection des failles de sécurité
- un système de détection des intrusions
- un système d'exploitation sécurisé (multi-niveaux ou autre)

Caractéristiques des IDS



Sources des données

- **Informations système** (Host based) : accounting, audit C2, etc.
 - **Accès au système** : qui a accédé au système, quand et depuis où ?
 - **Usage fait du système** : commandes système, accès aux unités d'entrée/sortie, utilisation CPU
 - **Usage fait des fichiers** : horodatage, type et source de l'accès, volume d'informations échangées
 - **Violations éventuelles de la sécurité** :
 - * tentative d'exécution d'une application dans un mode privilégié
 - * tentative d'accès à un fichier non autorisé ou fourniture d'un mot de passe erroné pour cet accès
 - * changement des droits d'accès à des fichiers sensibles
 - * accès au système à des moments ou depuis des lieux inhabituels
 - * etc.
- **Informations réseau** (Network based) : utilisation de *sniffers*
- **Informations applicatives** : lancements et arrêts, modules réellement exécutés, données entrées, sorties produites

Méthode de détection (1)

Approche comportementale : principe

- Proposée par Anderson dès 1980 et reprise par Denning et Whiterhurst en 1987
- Basée sur l'hypothèse qu'une intrusion implique un usage anormal du système et donc un comportement inhabituel d'un utilisateur
- Cherche donc à répondre à la question : **le comportement actuel de l'utilisateur est-il cohérent avec son comportement passé ?**

Méthode de détection (2)

Approche comportementale : notion de profil

- Vue synthétique du comportement d'un utilisateur ou d'un groupe d'utilisateurs
- Obtenu grâce à une étude statistique
- Nécessite la définition de "variables aléatoires", quantité accumulée pendant une période de temps ou entre 2 événements particuliers :
 - nombre de mails reçus par jours
 - nombre de quants de temps CPU utilisés entre connexion et déconnexion
 - etc.

Méthode de détection (3)

Approche comportementale : bilan

Avantage	Inconvénients
Pas besoin d'une base d'attaque	Pour un utilisateur au comportement erratique, toute activité est normale
Détection d'intrusions inconnues possible	En cas de profonde modification de l'environnement du système cible, déclenchement d'un flot ininterrompu d'alarmes ⇒ gros risque de faux positifs
	Utilisateur pouvant changer lentement de comportement dans le but d'habituer le système à un comportement intrusif ⇒ risque de faux négatifs

Méthode de détection (4)

Approche par scénarios : principe

- Pour pallier les inconvénients de l'approche comportementale, on cherche à répondre à la question : **le comportement actuel de l'utilisateur correspond-il à un comportement "intrusif" connu ?**
- Nécessite donc de construire une base de données d'attaques
- La recherche des attaques dans les données se fait généralement par application de techniques d'analyse de signature (*pattern matching*)

Méthode de détection (5)

Approche par scénarios : bilan

Avantage	Inconvénient
Prise en compte des comportements exacts des attaquants potentiels ⇒ peu de faux positifs ... pas si sûr !!!	Base de scénarios difficile à construire et, surtout à maintenir ⇒ risque de faux négatifs Pas de détection d'attaques non connues ⇒ risque de faux négatifs Détection de scénarios complexes difficile

Méthode de détection (6)

Mise en œuvre des deux approches

	Modèle statistique	Système expert	Réseau de neurones	Analyse de signature
Approche comportementale	X	X	X	X
Approche par scénarios		X		X

Quelques outils commerciaux

- BlackICE, NetworkICE, <http://www.networkice.com/products/blackice>
- Centrax, Cybersafe Corp., <http://www.centraxcorp.com>
- CyberCop Monitor, Network Associates,
http://www.nai.com/asp_set/products/tns/cybercop_intrusion.asp
- Dragon, Network Security Wizards, <http://www.network-defense.com/dragon.html>
- Intruder Alert, Axent, <http://www.axent.com/Axent/Products>
- NetProwler, Axent, <http://www.axent.com/Axent/Products>
- NetRanger, Cisco,
<http://www.wheelgroup.com/warp/public/cc/cisco/mkt/security/nranger/index.shtml>
- Network Flight Recorder, NFR, <http://www.nfr.net>
- Real Secure, ISS, <http://www.iss.net/RealSecure/>
- Session Wall, Abirnet, <http://www.sessionwall.com>

Quelques outils du domaine public

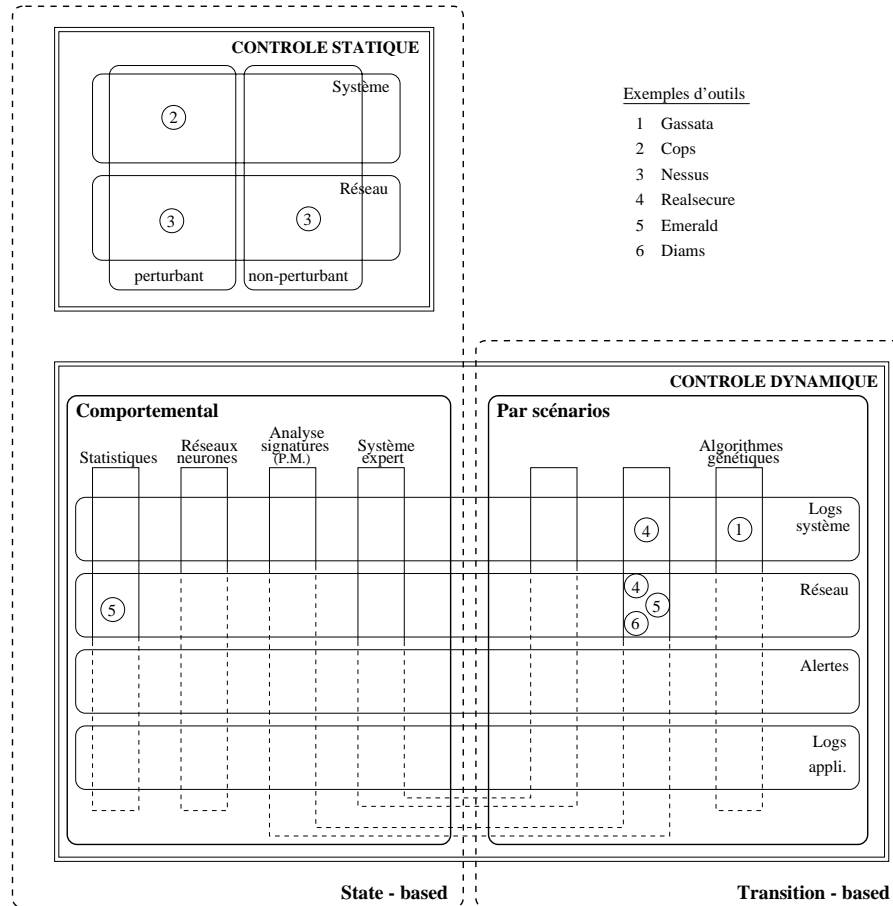
- AAFID, Purdue University, CERIAS (ex COAST),
<http://www.cerias.purdue.edu/coast/projects/aafid.html>
- ASAX, Université de Namur, <http://www.info.fundp.ac.be/amo/publications.html>
- BRO, Lawrence Berkeley Nat. Lab., <http://www-nrg.ee.lbl.gov/nrg-papers.html>
- DIAMS, ENSTB,
- EMERALD, SRI International, <http://www2.csl.sri.com/emerald/index.html>
- G^ASAT^A, Supélec, <http://www.supelec-rennes.fr/ren/rd/ssi/>
- GrIDS (Graph-based Intrusion Detection System), University of California at Davis, <http://olympus.cs.ucdavis.edu/arpa/grids/welcome.html>
- Shadow, Naval Surface Warfare Center, <http://www.nswc.navy.mil/ISSEC/CID>
- SNORT, Martin Roesch, <http://www.cark.net/roesch/security.html>

Que permettent ces outils ?

	Host based	Network based	Approche comport.	Approch scénarios	Réaction
BlackICE		pk IP		A.S.	Défensif
Centrax	Log NT	pk IP		A.S.	
CyberCop Monitor	Log Unix/NT	pk IP	X		Défensif
Dragon		pk IP		A.S.	
Intruder Alert	Log Unix	pk IP		A.S.	Défensif Reconf. FW
NetProwler		pk IP		A.S.	
NetRanger		pk IP		A.S.	Reconf. routeur
NFR		pk IP		A.S.	
Real Secure	Log Unix/NT	pk IP		A.S.	Reconf. FW Défensif
Session Wall		pk IP		A.S.	
AAFID	Log Unix			S.E.	Coupe cnx
ASAX	Log Unix			A.S.	
BRO		pk IP		A.S.	Coupe cnx
DIAMS		pk IP		A.S.	
EMERALD		pk IP	Stat.	A.S.	Informatif
G _S SA _T A	Log Unix			A.S.	
GrIDS		pk IP	S.E.		Informatif
Shadow		pk IP		A.S.	
SNORT		pk IP		A.S.	

A.S. : Analyse de Signature; S.E. : Système Expert; X : le fait mais comment ?

En résumé ...



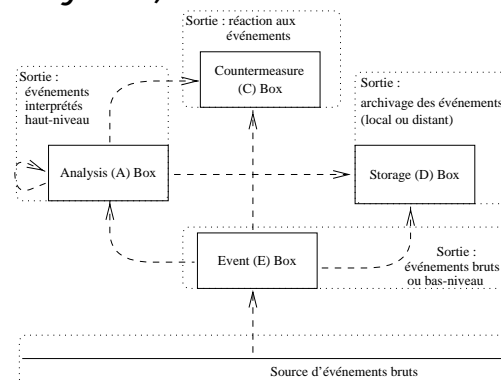
Et maintenant ? (1)

- De nombreux projets de recherche : ex. de RAID 2000
 - 27 full papers
 - 30 extended abstracts
- Exemples de projet :
 - DARPA Intrusion Detection Evaluation
<http://www.ll.mit.edu/IST/ideval/>
 - PEA DGA MIRADOR
Alcatel, ENSTB, ONERA/CERT, Supélec

Et maintenant ? (2)

Des efforts de normalisation

- Objectif : permettre la coopération et le dialogue entre IDS
- Common Intrusion Detection Framework (CIDF), DARPA,
<http://www.isi.edu/~brian/cidf/>
 - Définition de composants dont les E/S sont "standards" (GIDO : *Generalized ID Objects*)



- Intrusion Detection Working Group (IDWG), IETF,
<http://www.ietf.org/html.charters/idwg-charter.html>
 - Définition d'un protocole et de formats de messages (\Rightarrow spécif. des infos à partager entre IDS) pour le dialogue entre IDS

Et après ?

Des problèmes encore ouverts

- Diminution du taux de faux positifs
- Détection de scénarios de quelques événements
- Disponibilité de bases de vulnérabilités/exploits
- Langage de description des signatures d'attaque (description précise et "standardisée" des attaques et de la manière de les détecter)
- Distribution de l'analyse des logs
- Attaque ou contournement des IDS
- Protection des logs
- Respect de la vie privée des utilisateurs surveillés
- Tolérance aux intrusions

Conclusion provisoire

- Aucune approche ne domine
- Aucun mécanisme ne domine
- Un impératif :
 - Utiliser simultanément une panoplie d'outils pour bénéficier de leurs avantages respectifs
 - Faire collaborer ces outils (trouver comment ...)
- Un domaine qui reste largement ouvert où des travaux de recherche sont encore nécessaires

Pour plus d'information

- Ludovic Mé et Cédric Michel. La détection d'intrusions : bref aperçu et derniers développements. Actes de EUROSEC'99. Mars 1999.
<http://www.supelec-rennes.fr/rennes/si/equipe/lme/perso/publi/eurosec99.pdf>
- Herve Debar and Marc Dacier and Andreas Wespi, Towards a Taxonomy of Intrusion-Detection Systems Tech. Report, IBM Zurich Research Laboratory, 1999, <http://domino.watson.ibm.com/library/>
- Kathleen A. Jackson, Intrusion Detection System (IDS) Product Survey, Tech. Report, Los Alamos National Laboratory, 1999
<http://lib-www.lanl.gov/la-pubs/00416750.pdf>
- La page de Michael Sobirey recensant les outils de détection d'intrusion
<http://www-rnks.informatik.tu-cottbus.de/sobirey/ids.html>
- Listes de diffusion :
 - Liste IDS : <http://www.ticm.com/kb/faq/idsfaq.html>
 - Liste CIDF : <http://seclab.cs.ucdavis.edu/cidf/archive/messages/>
 - Liste du groupe IDWG de l'IETF : <http://www.semper.org/idwg-public/>

Pour encore plus d'information ...

- Toulouse, du 2 au 4 octobre 2000
- RAID'2000 : *Third International Workshop on the Recent Advances in Intrusion Detection*
- Une trentaine de présentations et 2 tables rondes
- Des actes regroupant 14 papiers
- <http://www.raid-symposium.org/Raid2000/>