Sécurité des Systèmes Informatiques

Evaluation de la Sécurité

TLS-SEC

Rodolphe Ortalo
CARSAT Midi-Pyrénées
rodolphe.ortalo@free.fr
(rodolphe.ortalo@carsat-mp.fr)
http://rodolphe.ortalo.free.fr/ssi.html

Questions

1. Est-ce que mon système d'information est suffisamment sûr ?
   - Analyse de risque

2. Quels produits/services choisir pour construire ou améliorer mon système d'information ?
   - Évaluation et comparaison entre les produits

1. Comment évolue la sécurité de mon système ?
   - Mesure quantitative

Évaluation de la sécurité

Analyse de risques et méthodologies

Méthodes d'analyse de risques de sécurité

MARION - MELISA - CRAMM - …

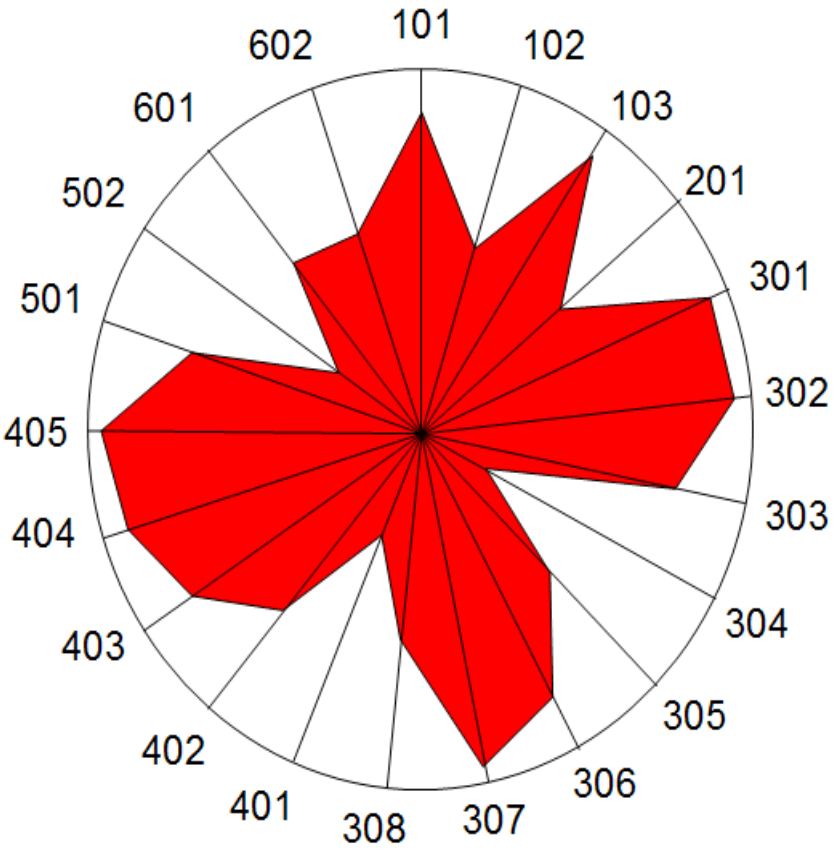
Démarche :

- Identifier les vulnérabilités
- Estimer les menaces (physiques, maladresses, malveillances)
- Analyser les risques et leurs conséquences possibles
- Évaluer les coûts des dégâts correspondants
- Calculer les fréquences*coûts
- Évaluer les coûts des contre-mesures
- Implémenter les plus rentables
- Suivre l'évolution

Indicateurs (Marion)

- Répartis en 6 thèmes
  - la sécurité organisationnelle
  - la sécurité physique
  - la continuité de service
  - l'organisation informatique
  - la sécurité logique et l'exploitation
  - la sécurité des applications
- Face à 17 types de menaces

  Accidents physiques, Malveillance physique, Panne du SI, Carence de personnel, Carence de prestataire, Interruption de fonctionnement du réseau, Erreur de saisie, Erreur de transmission, Erreur d'exploitation, Erreur de conception / développement, Vice caché d'un progiciel, Détournement de fonds, Détournement de biens, Copie illicite de logiciels, Indiscrétion / détournement d'information, Sabotage immatériel, Attaque logique du réseau



Méthodologies de sécurité

- Vont au-delà de l'évaluation des risques : MARION -> MEHARI, OCTAVE
  - ANSSI : EBIOS (expression des besoins et identification des objectifs de sécurité)
  - ISO 27000 : Système de Management de la Sécurité de l'Information (SMSI)
    <http://www.iso27001security.com/html/iso27000.html>
    - 27000 : Vue d'ensemble et vocabulaire (publié en 2009)
    - 27001 : Exigences (2005)
    - 27002 : Code de bonnes pratiques pour le SMSI (2005, anciennement ISO 17799)
    - 27003 : Lignes directrices pour la mise en œuvre du SMSI (publié en 2010)
    - 27004 : SMSI — Mesurage (publié en 2009)
    - 27005 : Gestion des risques en sécurité de l'information (publié en 2008)
    - 27006 : Exigences pour les organismes d'audit et de certification (publié en 2007)
    - 27007 : Lignes directrices pour l'audit des SMSI (publié en 2011)
    - 27008 : Lignes directrices pour le management de la sécurité de l'information (2011)
    - 27010 : SMSI inter-organisationnel (publié en 2012)
    - 27011 : Guide pour les organisations de télécommunications (publié en 2008)
    - 27031 : Lignes directrices … pour continuité des affaires (publié en 2011)
    - 27032 : Cybersécurité (2012)
    - 27033 : Sécurité de réseau (parties 27033-1 à 3 publiées)
    - 27034 : Sécurité des applications (27034-1 publiée en 2011)
    - 27035 : Gestion des incidents de sécurité de l'information (2011)
    - 27799 : SMSI pour le domaine de la santé, basé sur 27002 (publié en 2008)

Pros (my view)

- *Identification* of assets and their relative values
- Assets value offers an opportunity to budget realistically (for protection)
- Is understandable by end users
  - Quite easier than assembly language exploits or cryptographic hash functions
- Risk management alternatives
  - Transfer (insurance, state, etc.)
  - Acceptance (life is deadly after all)
  - Reduction (work, work, work, work, ...)
  - Avoidance (just do it the other way)
- Management could express clear priorities

Cons (my view)

- Threat determination is an oracle problem
- May be used to demonstrate that (any) risk is (already) managed
  - Some forgotten successes of risk management
    - Lehman-Brothers financial risk exposure
    - Greek debt control
  - Qualitative also means manipulable
- Relies a lot on best practices or risks lists
  - Fuels paranoia and ready-made useless tools
  - Does not help target real assets
- Management rarely wants to decide
- Sometimes does not end well morally speaking
  - For example : product lifetime optimization
    (NB : Inherently viewpoint-based)

Évaluation de la sécurité

Critères d'évaluation de la sécurité

Livre Orange (TCSEC) : 1983

Trusted Computer Security Evaluation Criteria

- Issus du souci du DoD de trouver sur étagère des produits satisfaisant les besoins de la défense US :
  - Confidentialité >> Intégrité > Disponibilité
  - 7 "classes" ordonnées (D, C1, C2, B1, B2, B3, A1) : chaque classe reprend les exigences de la classe précédente et y ajoute les siennes
  - Un produit est évalué dans une classe s'il satisfait à la fois :
    - des critères sur la doctrine de sécurité
    - des critères sur la responsabilité
    - des critères sur l'assurance
    - des critères sur la documentation

Caractéristiques des TCSEC

- Le Livre Orange ne vise que les systèmes informatiques isolés, et les seules politiques proposées sont : discrétionnaire (DAC) & Bell-LaPadula (MAC)

- Série “arc-en-ciel” <http://en.wikipedia.org/wiki/Rainbow_Series>
  - Le Livre Rouge (TNI 1987) donne un interprétation "réseau" et introduit Biba
  - Le livre Violet (TDI 1991) donne une interprétation “base de données”
  - Il y a divers guides (PC, mots de passe, audit, DAC, *covert channels*…)

Le livre orange : critères (1/2)

- Doctrine de sécurité
  - Contrôle d'accès discrétionnaire
  - Réutilisation d'objet
  - Labels
  - Contrôle d'accès obligatoire
- Responsabilité
  - Identification et authentification
  - Cheminement sûr
  - Audit
- Assurance opérationnelle
  - Architecture du système
  - Intégrité du système
  - Analyse des canaux cachés
  - Gestion d'une installation
  - Reprise sûre

Le livre orange : critères (2/2)

- Assurance du cycle de vie
  - Essai de la sécurité
  - Spécification et vérification
  - Gestion de la configuration
  - Distribution sûre
- Documentation
  - Guide l'utilisateur
  - Manuel d'installation sûre
  - Documentation des essais
  - Documentation sur le concept de sécurité

ITSEC (1991)

Information Technology Security Evaluation Criteria

- Proposés par GB, D, F, NL, soutenus par l'UE
- Sépare les aspects fonctionnels …
  Target of Evaluation (TOE), classes de fonctionnalités : 10 prédéfinies
  - F1 à F5 = C1 à B3 des TCSEC, ordonnées, confidentialité
  - F6 à F10 : non-ordonnées : intégrité, disponibilité, réseaux, …
- …des aspects "assurance" :
  - "*Correctness*" : niveaux E1 à E6
  - Efficacité : pertinence des fonctionnalités, résistance des mécanismes, facilité d'emploi, analyse de vulnérabilités…

ITSEC - Critères

- Classe de fonctionnalité
- Assurance de conformité : E1 à E6
- Assurance d'efficacité
  - Construction
    - Pertinence de la fonctionnalité
    - Cohésion de la fonctionnalité
    - Résistance des mécanismes
    - Estimation de la vulnérabilité de construction
  - Exploitation
    - Facilité d'emploi
    - Estimation de la vulnérabilité en exploitation

Critères Communs (CC)

- Développés par une organisation internationale (*CC Development Board → CC Management Board*) : version actuelle 3.1r4 (septembre 2012)
- Norme ISO/IEC 15408 (2008-2009)

- Mêmes principes que les ITSEC (TOE, séparation fonctionnalités / assurance) +
  - 7 niveaux de "*evaluation assurance*": EAL 1 à 7
  - + de classes de fonctionnalités (ex. *Privacy*)
  - Profils de protection prédéfinis (fonctionnalités + assurance) pour des classes d'applications : ex. *firewalls*, *smartcards*, …

CC - Classes de fonctionnalités

- FAU : Security audit
- FCO : Communications
- FCS : Cryptographic support
- FDP : User data protection
- FIA : Identification and Authentication
- FMT : Security management
- FPR : Privacy
- FPT : Protection of the TSF
- FRU : Resource utilization
- FTA : TOE Access
- FTP : Trusted paths/channels

CC - Niveaux d'assurance

- EAL1 : Functionally tested
- EAL2 : Structurally tested
- EAL3 : Methodically tested and checked
- EAL4 : Methodically designed, tested and checked
- EAL5 : Semiformally designed and tested
- EAL6 : Semiformally verified design and tested
- EAL7 : Formally verified design and tested

CC - Profils de protection

- Il y en a une cinquantaine (http://www.ssi.gouv.fr) :
- Exemples :
  - Module de vérification de signature électronique (EAL3+)
  - Application de création de signature électronique (EAL3+)
  - Application VPN cliente (EAL3+)
  - Pare-feu d'interconnexion IP (EAL3+)
  - Pare-feu personnel (EAL3+)
  - Appli. chiffrement à la volée pour mémoire de masse (EAL2+)
  - Système d'horodatage
  - Javacard configuration
  - CB-EMV payment/withdrawal smartcard application
  - Distributeur de billets
  - Autorité de certification
  - …

Nice quote on criteria

- CC – ISO 15408
  - Common Criteria évaluation of a version of RedHat Linux distribution

« For the most part, the protection profiles define away nearly all of the interesting threats that most systems face today. » *in* Fedora and CAPP, lwn.net, 10 dec. 2008.

Évaluation de la sécurité

Évaluation quantitative de la sécurité

Évaluation quantitative : Approche LAAS

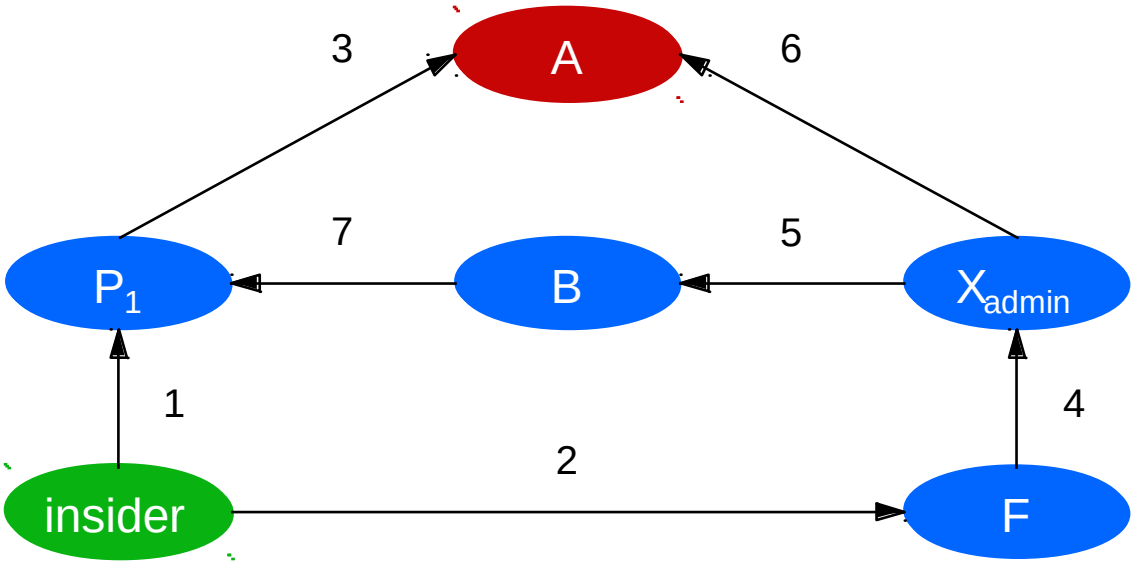
- Objectifs:
  - Prendre en compte les compromis sécurité/fonctionnalités
  - Surveiller les évolutions de la sécurité opérationnelle dues à des modifications du système ou de l'environnement
  - Identifier les configurations offrant la meilleure sécurité pour le minimum de contraintes au niveau fonctionnalités
- Cadre de modélisation probabiliste
  - Vulnérabilités
  - Attaquants
- Mesure = effort nécessaire à un attaquant potentiel pour mettre en défaut la politique de sécurité

Approche générale

- Définition des objectifs de sécurité
  - politique de sécurité
- Modélisation des vulnérabilités
- Modélisation des processus d'attaque
- Calcul des mesures

Modélisation des vulnérabilités

Graphe des Privilèges



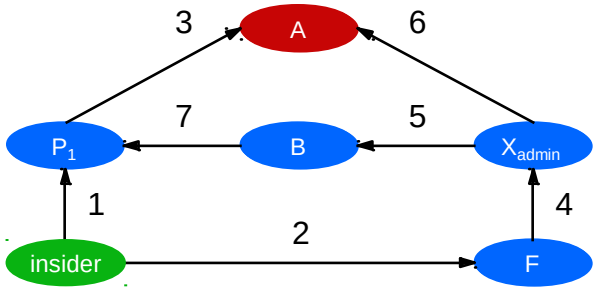
1) X can guess Y's password
2) X can install a Trojan horse that Y can activate
3) X can exploit a flaw in Y's mailer
4) Y is a subset of X
5) Y uses a program that X can modify
6) X can modify a "setuid" program owned by Y
7) X is in Y's `.rhosts`

- Nœud = ensemble de privilèges
- Arc = méthode de transfert de privilèges = vulnérabilité
- chemin = ensemble de vulnérabilités pouvant être exploitées par un attaquant pour mettre en défaut un objectif de sécurité
- poids = pour chaque arc, effort pour exploiter la vulnérabilité

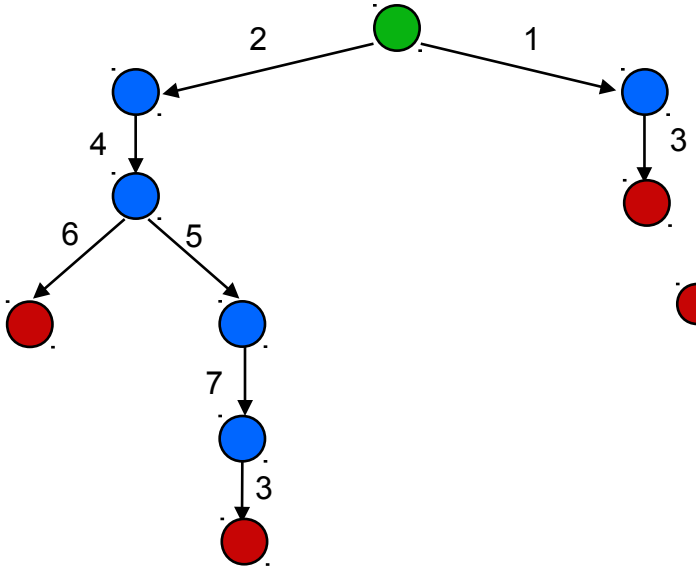
Processus d'attaque : Hypothèses

- Processus d'attaque = tous scénarios d'attaques réussies
- Hypothèses générales
  - L'attaquant ne connaît que les vulnérabilités qu'il peut exploiter avec les privilèges dont il dispose déjà
  - L'attaquant ne tentera pas d'attaques qui lui donneraient des privilèges qu'il possède déjà
- et, soit:
  - *Mémoire Totale (MT)*: l'attaquant se souvient de toutes les vulnérabilités qui n'ont pas été exploitées dans les étapes *précédentes* et peut revenir en arrière.
  - *Mémoire locale (ML)*: l'attaquant considère seulement les vulnérabilités qui peuvent être exploitées avec les privilèges nouvellement acquis.

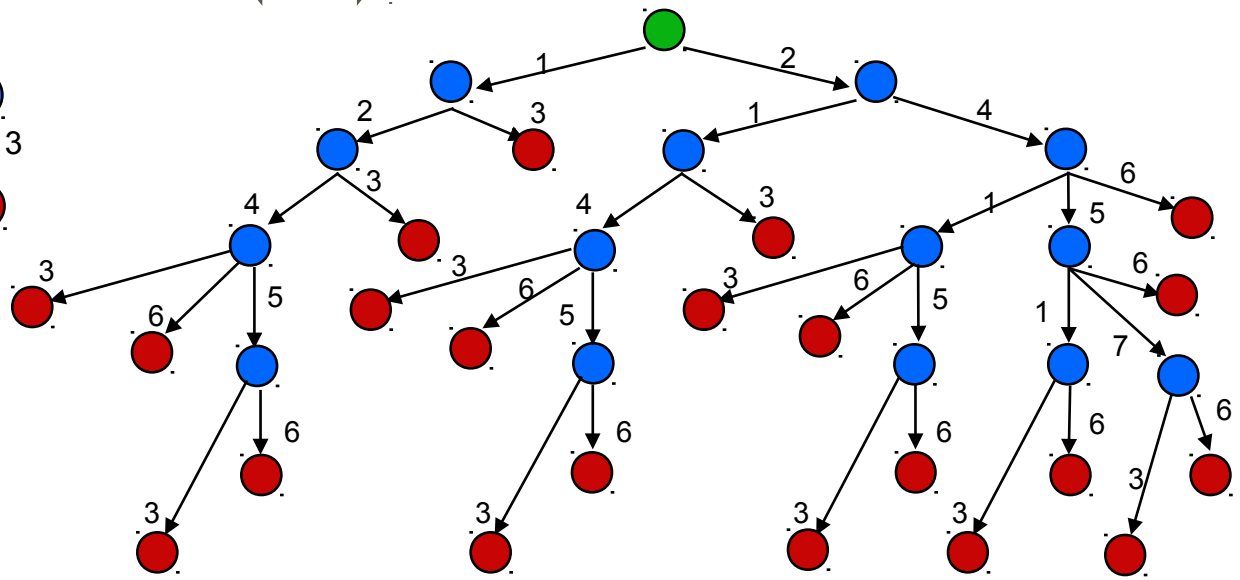
Processus d'attaque : Exemples



Hypothèse ML



Hypothèse TM



Calcul des mesures

① Définition des couples attaquant-objectif

② Pour chaque couple, calcul des mesures :

METF-ML: "*Mean Effort To security Failure"*
(c-à-d pour atteindre l'objectif) avec l'hypothèse ML

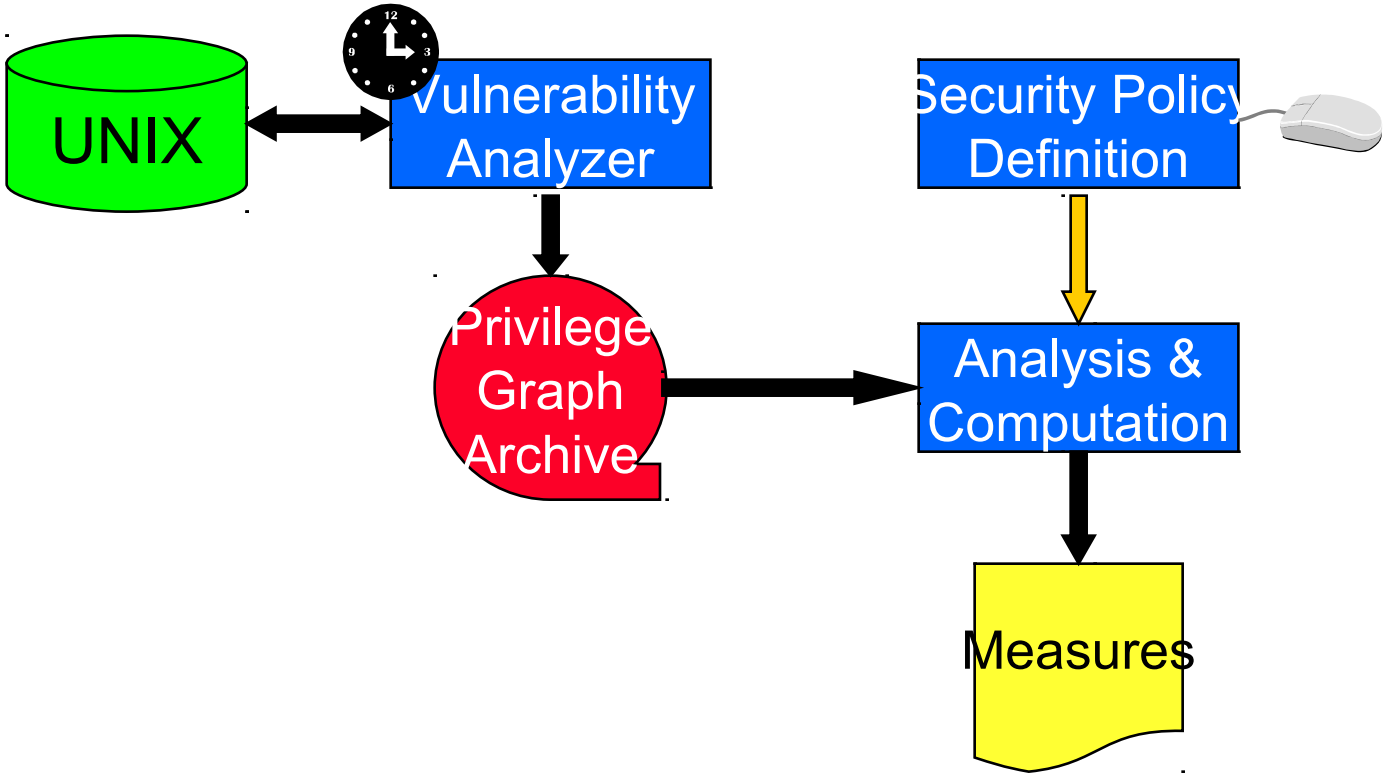
METF-TM: "*Mean Effort To security Failure*" avec l'hypothèse MT

SP : Effort moyen correspondant au plus court chemin.

Nombre de chemins : Nombre de chemins possibles entre l'attaquant et l'objectif

L'outil ESOPE

(Évaluation de la Sécurité OPErationnelle)



Expérimentations : Réseau du LAAS

- Objectifs:
  - Valider l'approche
    - pertinence des mesures pour refléter les évolutions de la sécurité consécutives à des évolutions du système (configurations, utilisateurs, etc.)
    - faisabilité de l'approche sur un système réel
  - Il ne s'agissait *pas* de :
    - corriger les vulnérabilités identifiées

Contexte expérimental

Système cible

- Unix
- 700 utilisateurs - 300 machines - LAN
- 13 mois (Juin 1995 - Juillet 1996)

Objectifs de sécurité

	Attaquant	Cible
Objectif 1	insider	root
Objectif 2	insider	admin_group

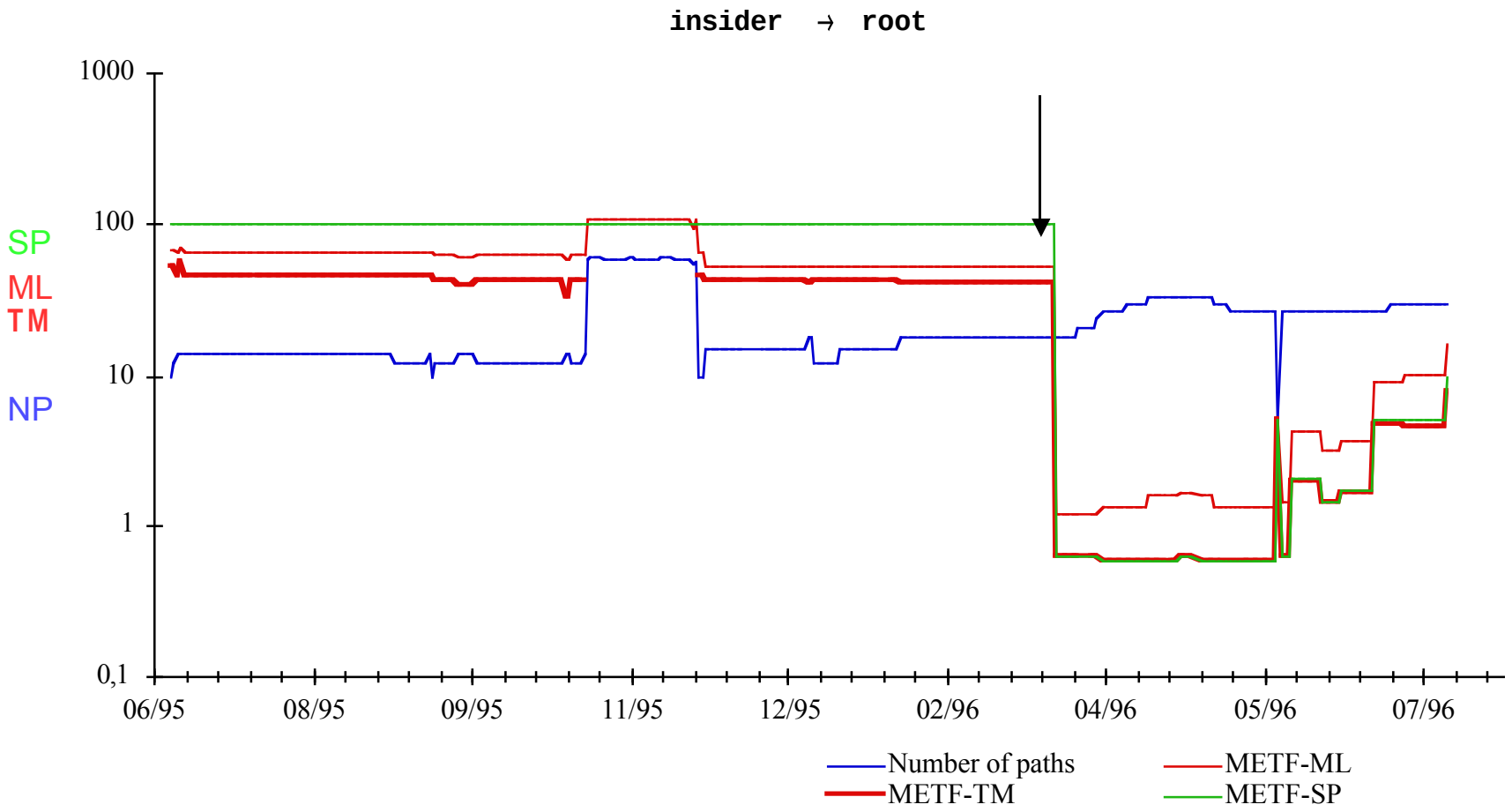
13 types de vulnérabilités

(fichiers `.rhosts`, `.*rc`, passwords, etc.)

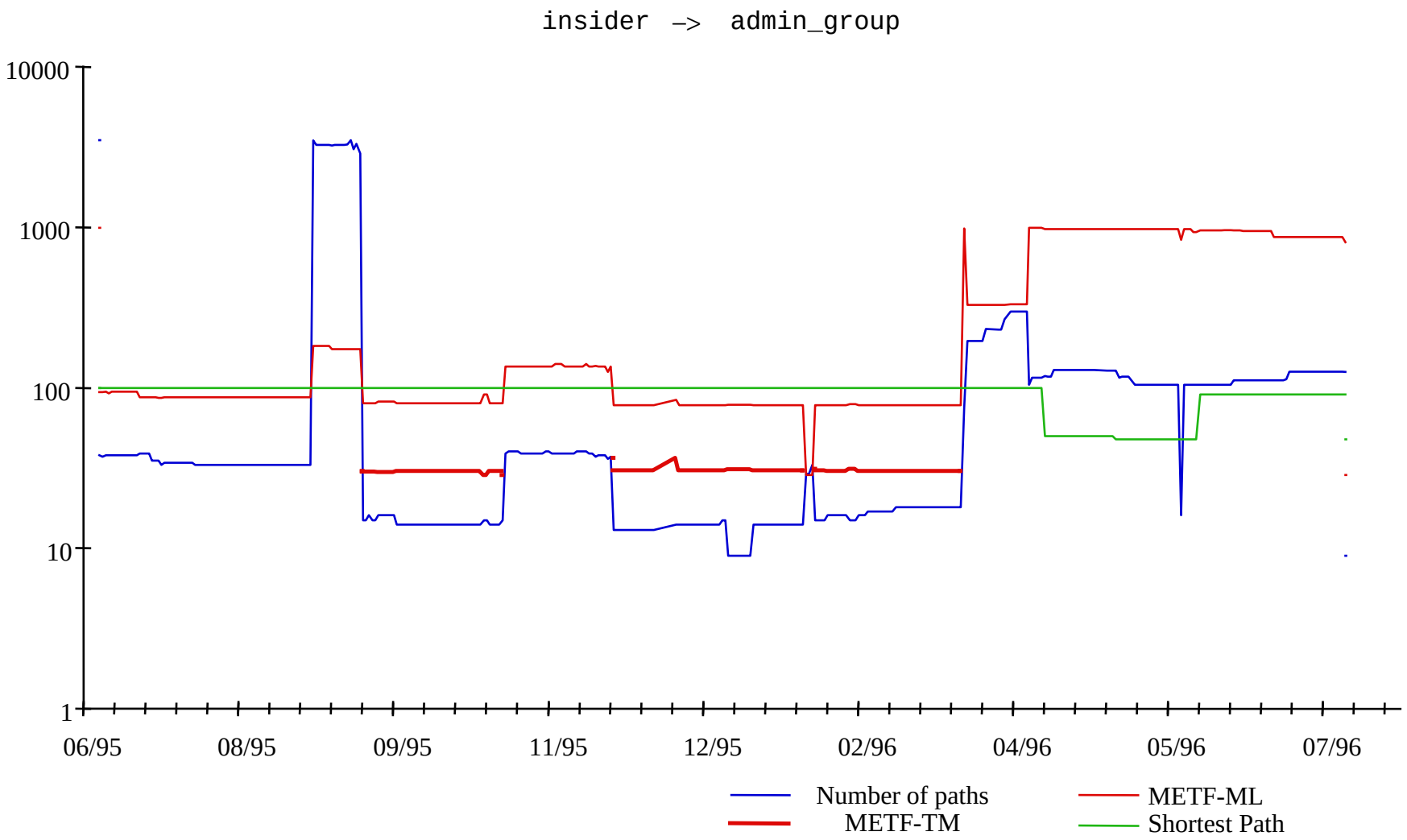
4 niveaux de difficulté

Type	poids
très facile	10
facile	10^2
difficile	10^3
très difficile	10^4

Résultats expérimentaux (1)



Résultats (2)

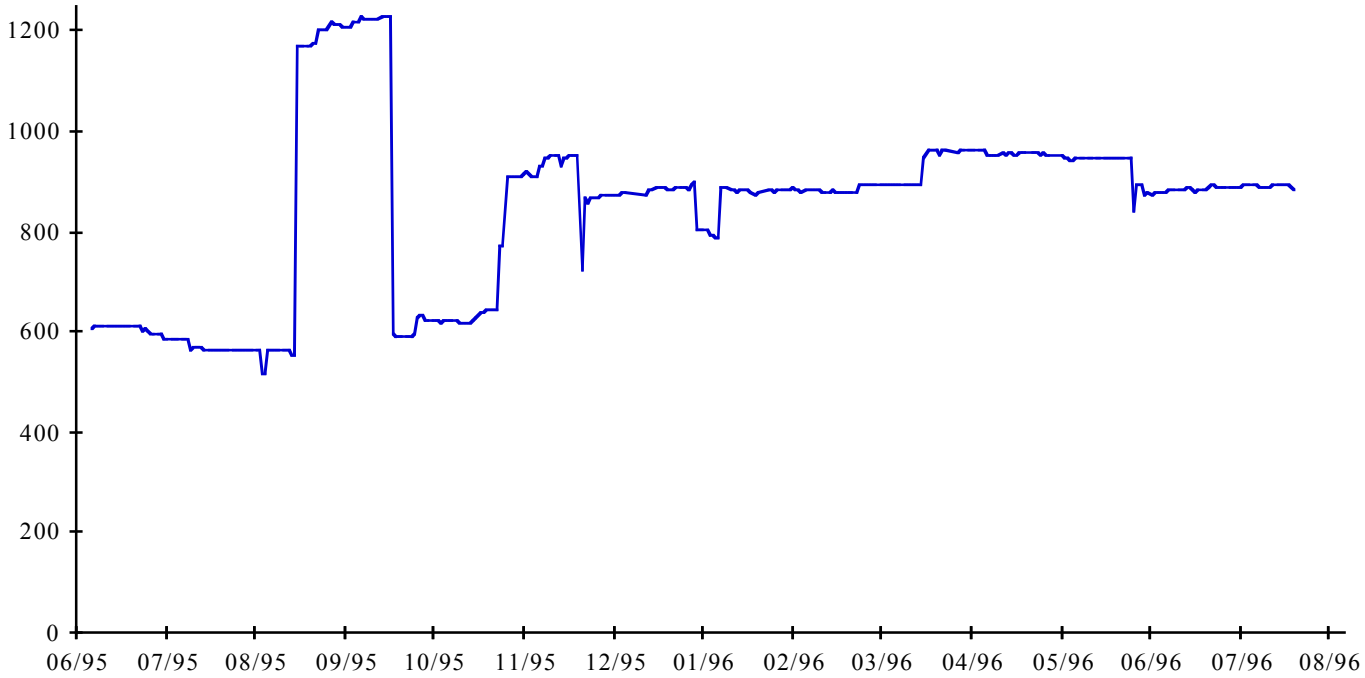

insider -> admin_group
10000
1000
100
10
1
06/95
08/95
09/95
11/95
12/95
02/96
04/96
05/96
07/96
Number of paths
METF-TM
METF-ML
Shortest Path

Comparaison des mesures

- Le chemin le plus court (**SP**) n'est pas assez sensible et ne permet pas d'identifier des événements de sécurité importants
- Le nombre de chemins (**NP**) change trop fréquemment et déclencherait un grand nombre d'alarmes parfois douteuses
- **METF-ML** présente une sensibilité intéressante aux événements de sécurité significatifs.
- **METF-TM** est également sensible aux événements de sécurité significatifs, mais est parfois difficile à calculer quand le graphe est complexe.

Comparaison avec d'autres outils

Évolution du nombre de vulnérabilités



Évolution de METF-ML et METF-MT