Blare:
a Policy-Based HIDS for Linux

J. Zimmermann, L. Mé, C. Bidan

Supélec ÉCOLE SUPÉRIEURE D'ÉLECTRICITÉ

Démonstration

SSTIC '04

IDS à base de Politique

- Modèle de Politique de Sécurité
  - pas de scénario d'attaque connu
  - pas de comportement appris ni spécifié
- Objectifs
  - détection d'attaques connues ou nouvelles
  - moins de fausses alertes
  - facilité de maintenance
- Contrôle des flux d'informations

Pour en savoir plus...

- Introducing Reference Flow Control for Intrusion Detection at the OS Level
  - *Zimmermann, Mé, Bidan, RAID 2002*
- Improved Reference Flow Control Model For Policy-Based Intrusion Detection
  - *Zimmermann, Mé, Bidan, ESORICS 2003*
- Experimenting With A Policy-Based HIDS Based on an Information Flow Control Model
  - *Zimmermann, Mé, Bidan, ACSAC 2003*

Bientôt disponible

- Implémentation pour le noyau Linux 2.6.x sous licence *GPL*
  - Disponible avant l'été 2004
- Utilisation commerciale par IPDiva
  - Produit lancé courant 2005

http://www.rennes.supelec.fr/blare