NuFW, un parefeu authentifiant

E. Leblond
INL

Séminaire Eole 2006

INL

- Création février 2004
- Jeune Entreprise Innovante
- Hébergée par Paris Développement
- Palmarès L'Usine Nouvelle (fév 2006)
- Références
  - Conseil de l'Europe,
  - Altitude Telecom
  - CNES ...

INL : SSLL et éditeur

- SSLL
  - Conseil/audit
  - Intégration
  - Support/maintenance
  - Formation
- Editeur de NuFW, NuLog, NuFace
  - NuFW inclus dans Debian Ubuntu Mandriva
  - Trophées du Libre
  - Partenaire IBM

Besoins

- Un réseau unique peut contenir des utilisateurs différents :
  - Professeurs
  - Élèves
- Le filtrage devrait donc être différent :
  - Plus de droits pour le professeur
  - Contrôle de l'activité des élèves
- Filtrage par utilisateur

État de l'art

- IP == Utilisateur
  - Authentification A Priori
  - Association entre machine et utilisateur
- Sécurité insuffisante :
  - Contournement (même involontaire)
    - Association sans preuve pendant une durée
    - Attaque par spoofing, ...
  - Problème des machines multi user

NuFW

- Briser le paradigme IP==Utilisateur
  - Authentification A Posteriori
    - pas de sessions
    - Authentification connexion par connexion
  - Mécanisme sécurisé

- Algorithme “exclusif”
  - Inventé pour NuFW
  - Validé auprès de la communauté sécurité française et internationale
- Logiciel libre sous GPL

Fonctionnalités

- Surcouche de Netfilter :
  - enrichissement des fonctions
  - cohabitation
- Filtrage authentifiant :
  - Filtrage par groupe (niveau, classe, élève)
  - Reporting avancé
- Routage par utilisateur
- Qualité de service par utilisateur

Historique de NuFW

- 2001 : idée du principe
- Début 2003 : démarrage du développement
- 1er sept 2003 : première version publique
- 2004 : création d'INL qui accompagne NuFW
- 8 mars 2005 : NuFW 1.0
- mai 2005 : Trophés du libre
- Octobre 2005 : présentation au Netfilter Workshop
- 22 mai 2006 : NuFW 2.0

Fonctionnalités “détaillées”

- Système modulaire :
  - intéractions avec l'extérieur au moyen de greffons
  - journalisation, authentification, autorisation, ...
- Client pour l'authentification :
  - Sur le poste de travail
  - Transparent ou non
- Authentification :
  - Utilisation de PAM
  - Par certificat

Fonctionnalités “détaillées”

- Autorisation :
  - LDAP, fichier plat
- Journalisation :
  - ouverture, établissement, fermeture des connexions
  - enrichi les données réseaux par les informations utilisateurs
  - stockage en SQL
  - envoi vers Prelude

Fonctionnalités “détaillées”

- Filtrage horaire strict :
  - Ouverture pendant la plage horaire
  - Fermeture à la fin de la plage horaire
- Authentification Unique :
  - Le serveur demande au pare-feu l'identité
  - Transparent pour l'utilisateur
  - Indépendante du protocole
  - Modules pour apache, squid

NuFW et Amon

- Moyen fiable de contrôler les accès suivant le statut, par exemple :
  - Élèves passent par proxy filtrant
  - Professeurs sortent en direct
- Augmenter le contrôle :
  - couper le réseau pour une classe
  - ou pour un élève ...
  - passage en mode examen

NuFW et Amon

- Régles de filtrage différenciés :
  - suivant l'individu et son emplacement dans l'établissement
  - utilisation des annuaires globaux
- Suivi de l'activité des élèves :
  - Outil de reporting
  - Prelude (module dédié)

NuFW et Amon

- Responsabilisation des élèves et ... :
  - Fin de l'anonymat
  - Prise de conscience ?
  - Page de reporting individuelle ?
- [vos idées ici]
  - Système ouvert
  - Apporte la notion d'utilisateur à l'ensemble des couches réseaux
  - ...

Conclusion

- NuFW permet de traiter :
  - Différence des statuts propres à l'enseignement
  - Besoin de suivi de l'activité
  - Besoin d'authentification
- Il permet une intéraction humaine :
  - Manipulation des entités structurelles
  - Apporte au réseau la notion d'élève, de classe
- Augmente la sécurité

Fin

NuFW : http://www.nufw.org
INL : http://www.inl.fr/

Questions ?