Journées MATHRICE "Dijon-Besançon"
DIJON 15-17 mars 2011

Projet MySafeKey
Authentification
par clé USB

Sommaire

Introduction

- Réflexions
  - Méthodes pouvant améliorer l'accès au Système d'Information
  - Problématique des mots de passe
- Réalisation antérieure
  - Morphomatique
    - Accès au poste de travail par reconnaissance du visage.

Authentification au Système d'Information

- Besoins d'une authentification unifiée
  - Accès :
    - aux postes de travail
    - à la messagerie, l'ENT (web)
    - aux applications nationales (SGBD)
  - Connexions identifiées
    - Filaires et WIFI.
- Annuaires répartis et distribués
  - OpenLDAP (SAMBA) ou Active Directory
  - Impact majeur sur le Système d'Information

Problématiques des mots de passe

- Type de systèmes
  - Linux, MS Windows XP(2003), MS Seven (2008)
- Linux :
  - Fichiers (/etc/passwd, /etc/shadows)
  - Mot de passe crypté (MD5++) → crypt
- MS Windows XP & 2003
  - Base de registre
  - 2 types de cryptage LM et NTLM (DES, MD4)
- MS Vista & Seven & 2008
  - Cryptage NTLM (MD4)

Authentification forte

- Combinaison d'éléments
  - Connaissance (mdp, code, …)
  - Détention matérielle (carte, token, téléphone, …)
  - Caractère biométrique (empreinte, voix, visage, ...)
  - Comportement (signature, question, …)
- Technologies
  - One Time Password
  - Certificats Numériques (PKI, RSA, ...)
  - Biométrie
  - Clé d'authentification
  - Token hybride

Types de chiffrements

- Symétrique – asymétrique
- DES (Data Encryption Standard)
  - Depuis 1971 (standard en 1976) FIPS PUB 46
  - Blocs de 56 bits
  - Réseau Feistel, chiffrement par bloc, structure symétrique
  - Basé sur permutations et substitutions (S-Boxes)
  - Remplacé par 3DES en 1997

Types de chiffrements

- AES (Advanced Encryption Standard) - NIST
  - Concours pour remplacer DES (1997) FIPS PUB 197
    - Serpent, Twofish, ...
  - Joan Daemen and Vincent Rijmen
  - Rijndael, blocs 128, 192 ou 256 bits
  - Réseau substitution-permutation
  - Basé sur permutations, transformations linéaires, XOR
  - Standard actuel
  - www.worldlingo.com/ma/enwiki/en/Advanced_Encryption_Standard

Types de chiffrements

- Fonctions de hachage
  - Empreinte résistant aux collisions et identifiant une entrée
- Salage
  - chaine aléatoire ajoutée à l'entrée avant de hacher
  - Deux entrées identiques → empreintes différentes
- MD5 (Message Digest 5) – 1991 (128 bits)
  - Basé sur permutations et opérations logiques de blocs
  - Sensible aux attaques (force brute et tables arc en ciel)
- SHA (Secure Hash Algorithm)
  - SHA1 (160 bits) remplacé par SHA256 et SHA512
  - 2004 publication de failles sur SHA1

Faiblesse des mots de passe

- Récupération des empreintes
  - Besoin d'un compte administrateur
  - Linux : Facile
  - Windows : Facile mais détection par antivirus
- Linux
  - Empreintes avec sel et crypté ($hash$salt$pass)
  - TA impossible, force brute difficile
- Windows
  - Empreintes sans sel et chiffrement simple
  - Si LM, TA et force brute aisés
  - Si NTLM, TA plus importante, force brute

Faiblesse des mots de passe

- Quelques solutions
  - Protection de l'accès à la machine
  - Bannir LM
  - Complexification du mot de passe, test dictionnaire
  - Utilisation de coffres (Passwordsafe, KeePass, …)
- Complexification en T^N
  - Nombre de caractères N
  - Types de caractères T (26M+26m+10c+33s)
- GPU et CUDA, nouveaux problèmes (10^{11}h/s)
  - FB : (N=8,T=62) → 36 m; (N=9,T=62) → 1,5 j; (N=10,T=62) → 97 j
  - TA : (N=8,T=62) → 109 Go; (N=9,T=62) → 7 To; (N=10,T=62) → 419 To
  - (N=15, T= 92) → 10^{11} années; $1{,}5.10^{17}$ Go

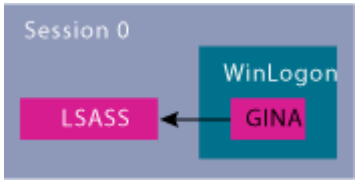
Technologies d'authentification sur les SE

- Winlogon et GINA
  - Jusqu'à MS XP – 2003
  - Winlogon : composante du système fournissant le support pour l'ouverture de session interactive.
  - GINA : Graphical Identification and Authentication
  - Fonctionnement :
    - Winlogon détecte événement SAS (séquence d'action sécurisé).
    - Winlogon détermine l'état du système lorsque le SAS a été détecté.
    - Winlogon appelle la fonction GINA appropriées.
    - La fonction GINA appelée effectue l'opération nécessaire.
    - La fonction GINA passe une valeur de retour à Winlogon.
- Difficile à programmer, problèmes de sécurité (niveau 0)

Technologies d'authentification sur les SE

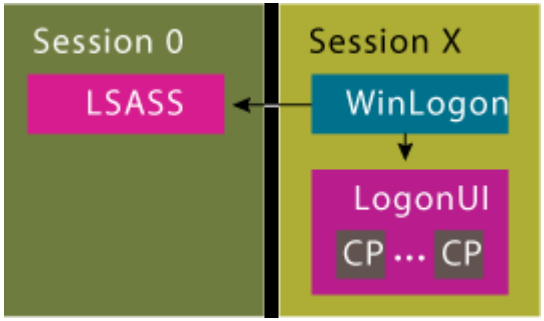
- Credential Providers (CP)
  - Depuis MS Vista – 2008
  - Plus sécurisé : pas de fonctionnement au niveau 0
  - Winlogon lance un processus interface hôte de connexion utilisateur (logonui.exe)
  - Ce processus charge un ou plusieurs fournisseurs d'informations d'identification (CP)
  - Développement simplifié et modulable

Système antérieur



LSASS
=
Local Security
Authority acceSS

Système actuel



Technologies d'authentification sur les SE

- Pluggable Authentication Module (PAM)
  - Unix (Linux, FreeBSD, AIX, HPUX, …)
  - Fournit une authentification indépendamment du reste du système.
  - Mécanismes implémentés :
    - Account, auth, password, session
  - Nombreux modules dynamiques
  - Source libre

PGINA

- PGina
  - système open source d'authentification qui remplace l'interface (GINA) du système d'exploitation Microsoft Windows.
  - Utilise des modules facile à écrire qui permettent à un système pour s'authentifier sur pratiquement n'importe quelle source.
- Problème
  - Fonctionne en aval de la saisie d'identifiant !

Authentification par clé USB

- USB : connecteur universel
- Produits avec puces cryptographiques
- Clés classiques
  - avec chiffrement des identifiants
  - besoin de vérifier l'unicité de la clé
  - utilisation en complément d'un coffre
- Besoins
  - Amélioration de la sécurité des mots de passe
  - Intégration dans le système d'information existant
  - Facilite l'accès en augmentant la sécurité

Produits existants

- Token USB
  - Aladdin, Genalto
- ROHOS
  - MS, Apple, authentification forte
- PAM_USB
  - OTP
- Smartlogon
  - MS XP, Gina, source libre, mais problèmes.

Paramètres pour une authentification forte

Utilisateur
- code pin
- mot de passe
- autres :
  Signature
  Question
  Pictogramme
  ....

Poste de travail
- codes
- identifiant
- validité

Clé USB
- identifiant clé
- identifiant volume SF
- fichier
  Taille, dates, ...

Arrangement de trois paramètres = authentification forte

MySafeKey

Projet avec un ensemble d'applications
- authentification forte avec une clé USB classique.

L'authentification se fait grâce à plusieurs éléments :
- l'identifiant de la clé USB
- l'identifiant de l'utilisateur et son mot de passe
- code PIN, ...

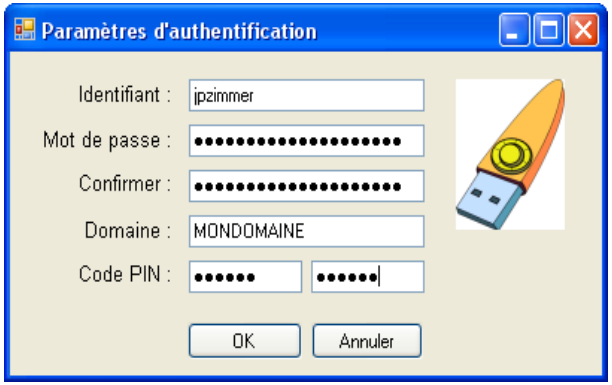
L'ensemble de ces éléments sont mélangés, cryptés et enregistrés sur la clé USB.

Amélioration de la sécurité de votre système :
- augmenter la longueur et la complexité des mots de passe,
- mots de passe complexes cryptés sur la clé USB,
- libèrent d'une mémorisation difficile ou de travers courants (mots de passe très simples, copiés sur post-it, ...).

MySafeKey

Applications développées :

- MySafeKeyGen : cryptage des identifiants sur la clé USB,
- la librairie d'authentification (GINA) pour l'ouverture de session automatique grâce à la clé USB.



MySafeKey

- Programme d'installation
- Programme de test MSKG_Test
- Documentation
- Multilingue : Français, Anglais, Espagnol
- Site : www.mysafekey.org
- Projet GPL v3 : www.sourceforge.net/projects/mysafekey

MySafeKey ≠ coffre de mots de passe généraliste

- vient en complément de ces applications,
- Password Safe ou Keepass.

Conclusions

- Travail important, mais concluant
  - Mécanisme permettant une authentification forte mais facile à utiliser
  - Intégration dans SI sans changement global
- A réaliser
  - Réalisation des implémentations CP et PAM
  - Réalisation d'un serveur de BD des clés
  - Changement du mot de passe avec celui du coffre.
  - Autres … (OTP ?)
- Une démonstration : www.mysafekey.org

Bibliographie

Sécurité :

http://www.ssi.gouv.fr/site_documents/politiqueproduit/..

..Mecanismes_cryptographiques_v1_10_standard.pdf

Winlogon – GINA :

http://technet.microsoft.com/en-us/library/bb742447.aspx

http://msdn.microsoft.com/en-us/magazine/cc163803.aspx

http://msdn.microsoft.com/en-us/magazine/cc163786.aspx

Credential Providers :

http://msdn.microsoft.com/fr-fr/magazine/cc163489.aspx

Linux :

http://geekfault.org/2009/05/19/authentification-avec-une-cle-usb/

Divers :

http://www.worldlingo.com/ma/enwiki/en/Cryptography

J. P. Zimmer, J. Mitéran, F. Yang, M. Paindavoine, "Security software using neural networks", IECON 98, Aachen, Germany, 72-74 (1998).