EdelWeb

Utilisation des cartes à puce avec Windows 2003

Nicolas RUFF

nicolas.ruff@edelweb.fr

Plan

EdelWeb

- Pourquoi les cartes à puce ?
- Architecture logicielle
  - PKI
  - AD
  - Format des certificats
  - Protocoles d'authentification
- Utilisation courante
  - Options
  - Audit
  - Différences entre Windows 2000 et 2003
  - Limites
- Bibliographie

Pourquoi les cartes à puce ?

EdelWeb

- **Les problèmes adressés**
  - **Mots de passe faibles**
    - **Les mots de passe sont choisis par les utilisateurs**
      - **Mots de passe vides, triviaux ; attaques par dictionnaire**
  - **Algorithmes LM / NTLM / NTLMv2 faibles**
    - **DES-56 vs. RSA à longueur de clé variable**
  - **Systèmes de sécurité logiciels cassables**
    - **Récupération des mots de passe dans la SAM**
    - **"Keyloggers"**
    - **Etc.**
  - **Multiplication des mots de passe**

- **Avantages des cartes à puce**
  - **La clé est générée par le système (pas de clés faibles)**
  - **La longueur de la clé est choisie par l'administrateur**
  - **Les algorithmes sont supposés robustes (/!\ non prouvé mathématiquement)**
  - **La clé privée est stockée dans la carte et ne peut pas être extraite**
  - **Le certificat de l'utilisateur devient son identité numérique car il est standard (multi-plateformes, utilisable à travers le Web)**

Architecture logicielle PKI

EdelWeb

- **Génération : Microsoft Certificate Services**
  - **Modèles prédéfinis dans la partition "Configuration" de AD**
    - **cn=Certificate Templates, cn=Public Key Services, cn=Services**
  - **Modèles à utiliser**
    - **"SmartCard Logon"**
    - **"SmartCard User" = "SmartCard Logon" + Messagerie sécurisée**
  - **Seul un utilisateur possédant un certificat de type "agent d'inscription" peut effectuer l'opération**
- **Publication : Active Directory (LDAP) et/ou IIS (HTTP)**
  - **Certificats**
  - **AIA (Authority Information Access)**
  - **CRL (Certificate Revocation List)**
- **Microsoft ne supporte pas l'utilisation d'une CA non Microsoft**
  - **… mais ça marche !**

Architecture logicielle
Active Directory

- Seuls attributs "obligatoires" dans AD
  - cn [Unicode String] "Nicolas RUFF"
  - instanceType [Integer] 4
  - objectCategory [DN] CN=Person, CN=Schema, CN=Configuration, DC=win2k, …
  - objectClass [Object Identifier] top;person;organizationalPerson;user
  - objectSid [SID] 0x01 0x05 0x00 ...
  - sAMAccountName [Unicode String] ruff
- Autres attributs d'intérêt sur l'objet utilisateur
  - distinguishedName [DN] CN=Nicolas RUFF, OU=Mes utilisateurs, DC=w2003, …
  - userCertificate [Octet String] 0x30 0x82 ...
  - userPrincipalName [Unicode String] ruff@w2003.edelweb.fr
- Remarques
  - Il est possible d'associer plusieurs certificats à un objet utilisateur
  - Le DN est un objet "critique" du système (entièrement géré par Windows)

Architecture logicielle
Format des certificats

EdelWeb

- OID requis
  - Key Usage
    - digitalSignature
    - keyEncipherment
  - Extended Key Usage
    - clientAuthentication 1.3.6.1.5.5.7.3.2
    - smartCardLogon 1.3.6.1.4.1.311.20.2.2
- Certificat "presque" standard (décodable par OpenSSL)
  - Subject: …, DC=w2003, OU=Mes utilisateurs, CN=Nicolas RUFF
    - Le DN varie en fonction de l'appartenance aux UO
    - Il n'est *pas* utilisé par Windows
  - OID 1.3.6.1.4.1.311.20.2 inconnu de OpenSSL
  - X509v3 Subject Alternative Name: othername:<unsupported>
    - "User Principal Name" dans un format Microsoft
    - Le champ fondamental pour l'authentification
    - Le certificat doit être régénéré si l'utilisateur change de login/domaine
- Autres contraintes (non vérifiées par mes soins)
  - Date d'expiration du certificat < date d'expiration de l'agent d'inscription
  - Présence d'un CDP

Architecture logicielle
Protocole d'authentification

EdelWeb

- Protocole d'authentification
  - Kerberos + extension PKINIT (en cours de normalisation IETF)
    - Le "timestamp" est signé avec la clé de l'utilisateur
    - Le KDC signe également le TGT
    - La clé de session est une clé Diffie-Hellman
  - Draft 9 implémenté par Microsoft
    - Interopérabilité avec les implémentations futures ?
  - Utilisation du champ "Subject Alternative Name"
    - Lorsque plusieurs certificats sont présents, le "premier" est utilisé
    - Quels critères ?
  - Documentation
    - http://support.microsoft.com/?kbid=248753
    - http://www.ietf.org/internet-drafts/draft-ietf-cat-kerberos-pk-init-17.txt
- La carte à puce peut être utilisée par d'autres applications
  - Transparence pour les applications grâce à la CryptoAPI
  - Utilisation par SSL/TLS, EAP-SmartCard, etc.

Utilisation courante
Options disponibles

EdelWeb

- Forcer un utilisateur à utiliser une carte à puce
  - Option activable individuellement par utilisateur
  - Si cette option n'est pas active
    - A tout moment l'utilisateur peut utiliser son mot de passe (login, déverrouillage écran de veille) au lieu de sa carte
  - Si cette option est active
    - Accès à des ressources par mot de passe impossible sur les systèmes supportant cette option
      - Ex. NET USE sans /SMARTCARD vers un Windows 2000 "de confiance"
    - Accès à des ressources par mot de passe possible sur les systèmes ne supportant pas cette option
      - Ex. Windows NT4
- Par GPO
  - Forcer un groupe d'utilisateurs à utiliser une carte à puce pour l'ouverture de session
  - Comportement du système en cas de retrait de la carte à puce
    - No action, lock, logoff

Utilisation courante
Audit (1/2)

EdelWeb

- Logon / logoff
  - Aucune différence entre un logon SmartCard et mot de passe (logon type 3)

- "Account logon" (672)
  - Authentication Ticket Request (sans)
    - User Name: superdupont
    - Supplied Realm Name: W2003
    - User ID: W2003\superdupont
    - Service Name: krbtgt
    - Service ID: W2003\krbtgt
    - Ticket Options: 0x40810010
    - Result Code: -
    - Ticket Encryption Type: 0x17
    - Pre-Authentication Type: 2
    - Client Address: 192.168.0.1
    - Certificate Issuer Name:
    - Certificate Serial Number:
    - Certificate Thumbprint:

Utilisation courante
Audit (2/2)

EdelWeb

- Authentication Ticket Request (avec)
  - User Name: ruff
  - Supplied Realm Name: W2003.EDELWEB.FR
  - User ID: W2003\ruff
  - Service Name: krbtgt
  - Service ID: W2003\krbtgt
  - Ticket Options: 0x40810010
  - Result Code: -
  - Ticket Encryption Type: 0x17
  - Pre-Authentication Type: 15
  - Client Address: 192.168.0.1
  - Certificate Issuer Name: w2003
  - Certificate Serial Number: 19A663EE00000000000B
  - Certificate Thumbprint: 6E0A28AE955922F51782D809816835E041A4DE6B

Utilisation courante
Différences entre Windows 2000/2003

EdelWeb

- **Au niveau CA**
  - Plus de modèles prédéfinis dans Windows 2003
  - Supporte des fonctions supplémentaires
    - Certification croisée, etc.
  - Présence de champs supplémentaires
    - AIA, etc.
- **Au niveau IIS**
  - 2 modes de mapping entre utilisateurs et certificats
    - Mapping via IIS (manuel)
    - Mapping via AD
  - En mode AD
    - IIS 5.0 ne peut pas transmettre l'authentification à des ressources externes (forwarding de ticket)
    - IIS 6.0 est capable de transmettre l'authentification
- **Probablement d'autres nouveautés non mentionnées ici**

Utilisation courante
Limites

EdelWeb

- Liste de compatibilité matérielle (HCL) limitée
  - 2 cartes : Gemplus, Schlumberger
  - Une dizaine de lecteurs
  - Pour les produits non supportés, vérifier la disponibilité de drivers !
- Une fois insérée, la carte à puce est toujours accessible
  - Un attaquant peut faire générer des réponses à la carte
  - Seule protection : flag "protection forte des clés privées" (très pénible pour l'utilisateur !)
- Les mots de passe ne disparaissent pas
  - Protocole LM / NTLM toujours utilisé sur les ressources non "kerberisées"
  - Protocoles non "kerberisés" (FTP, Telnet, authentification Web via proxy …)
- Comportements non testés
  - Expiration d'un certificat
  - Gestion des listes de révocation
- Risques matériels ?
  - Théoriquement la technologie est éprouvée
  - Mais par exemple sur Schlumberger présence de clés PIN, PUK et Clé usine (unique)

Bibliographie

EdelWeb

- Implémentation SSO au CERN
  - http://it-div-is-techmeet.web.cern.ch/it-div-is-techmeet/TechMeeting/2003-03-10/SingleSignOn.pdf
    - Hétérogène Unix / Windows
    - Utilisation de cartes à puce
    - Utilisation de Kerberos 5
    - Authentification Web & ouverture de session

- Docs Microsoft
    - http://www.microsoft.com/technet/prodtechnol/windows2000serv/evaluate/featfunc/pkiintro.asp
    - http://msdn.microsoft.com/library/en-us/dnsecure/html/pki.asp
  - Step by Step
    - http://www.microsoft.com/windows2000/techinfo/planning/walkthroughs/default.asp
  - How it works
    - http://www.microsoft.com/windows2000/techinfo/howitworks/default.asp
  - Kerberos
    - http://www.microsoft.com/windows2000/techinfo/planning/security/kerbsteps.asp