Pôle SSI RENATER

Claude Gross

Le pôle SSI RENATER

- Sécurité du GIP

- CERT RENATER
  - Publication des dernières vulnérabilités
  - Détection des attaques sur RENATER
  - Assistance aux contacts sécurité
  - Coordination avec les autres CERT

Le pôle SSI RENATER

- Support aux établissements
  - Support aux RSSI
    - PSSI
    - Documentation, liste de diffusion, …
    - Intranet juridique
  - Relai FSSI
    - Organisation de la SSI dans l'Enseignement Supérieur et la Recherche
  - JRSSI, Formations, …

- Certificats
  - Administration AC GRID2-FR
  - TCS

Gestion des identités

Authentification

SSO

Niveaux de confiance

...

Fédération d'identités

- Fournisseurs d'identités d'établissement
  - Techno Shibboleth
- Ressources internes ou partagées
- Cercles de confiance

Les fournisseurs d'identités

- Compte unique
  - Un seul compte
  - Une seule authentification
  - Accès à différentes ressources
  - SSO

➔La simplicité pour les utilisateurs (et les administrateurs)

➔Mais aussi pour les attaquants (phishings, …)

+ compromissions plus graves

Problématique du compte unique

- Une seule méthode d'authentification
  - En général : login + mot de passe
  - Gestion du mot de passe
    - Qualité, robustesse ?
    - Durée de vie ?
- Différents niveaux de sécurité
  - Intranet de laboratoires
  - Application RH
  - …

Niveaux de confiance

- Dépend :
  - du niveau de qualité de l'enregistrement d'un profil
  - du niveau de qualité de l’authentification des utilisateurs

Niveaux de confiance

Niveau de confiance

Qualité de la méthode d'authentification

+

Qualité des procédures organisationnelles

Niveaux de confiance

Niveau 4 Confiance très élevée, identité corroborée *Impact extrêmement grave*
Niveau 3 Confiance élevée, identité vérifiée *Impact grave*
Niveau 2 Confiance raisonnable, identité vraisemblable *Impact limité*
Niveau 1 Confiance minimale, identité anonyme/pseudo, … *Impact non significatif*

Méthodes d'authentification

- Très faible :
  - 2 facteurs faibles
- Faible :
  - 1 facteur prédictible + un facteur robuste
- Moyenne :
  - 2 facteurs
    - Mot de passe fort
    - Sel dans la base de hash
    - deux facteurs sont inconnus et non prédictibles
    - 1 prédictible, 1 fort et un anti brute force (captcha)
- Renforcé : 3 facteurs avec un lien
  - OTP logiciel sur le poste utilisateur
- Forte : 3 facteurs indépendant
  - Ce que je suis (login)
  - Ce que je sais (mot de passe / code pin)
  - Ce que je possède (objet)

Méthodes d'authentification

Mot de passe statique
Mot de passe statique stocké dans une carte magnétique activée par code **PIN**
Mot de passe dynamique généré par un outil logiciel
Mot de passe dynamique généré par un outil matériel
Certificat X.509 dans le navigateur de l'ordinateur
Certificat X.509 dans un token USB
Certificat X.509 dans une carte a puce
Biométrie et caractéristiques de référence dans une base de données en réseau
Biométrie associée a une carte magnétique
Biométrie associée a un certificat X.509 dans une carte a puce

Quels critères ?

- Sécurité (force, nb de facteurs)
- Ergonomie utilisateur
- Coût
- Utilisabilité
  - *Couverture géographique, possession d'un smartphone*
- Résistance aux attaques
  - *photocopie cryptocard, regarder par-dessus l'épaule, copie du fichier de certificat*
- Industrialisation
  - *tout OS, support …*
- Résilience

Quels critères ?

La **Qualité** d'une méthode d'authentification

=

Robustesse théorique face aux attaques

+

Adaptation aux contraintes techniques, organisationnelles, temporelles de même que financières et légales de l'établissement

Comme toute solution de sécurité, le choix de la méthode d'authentification sera un compromis (parfois long à obtenir…).

Ce qu'il ne faut pas faire

Objectifs

- Réflexion globale sur le sujet
- Documentation
- Recommandations
- Aspects techniques

Questions ?