Contrôle d'accès

le cnam

Introduction

- La sécurité dans le monde des technologies de l'information passe par la prise en compte des facteurs humains
  - Voir le cours introductif
- Le facteur humain est partie prenante dans la sécurité des systèmes
- *Le cours de contrôle d'accès a pour objectif d'examiner la phase qui permet à une personne d'accéder à un système et les moyens mis en oeuvre par le système pour contrôler la personne qui cherche à accéder au système*

le cnam

Plan : contrôle d'accès

- Définitions
- Mot de passe
- Biométrie
- Facteur d'authentification double

le cnam

Authentification (définition)

- L'authentification est la procédure qui vérifie dans un système informatique l'identité de l'entité qui demande un accès à un service ou une fonction
- Dans le cas d'un utilisateur humain (une personne) il s'agira d'authentifier la personne.
- On parle d'authentification.
- Comment authentifier un humain par rappport à une machine un système ?
- Cette opération est basée sur :
  - ce que vous connaissez ;
  - ce que vous possédez/transportez ;
  - ce que vous êtes.

le cnam

Ce que vous connaissez/Mot de passe

- C'est une réponse au qui va là ?
- Mot de passe ou information que seul celui qui cherche à s'authentifier connais dans le contexte
- Cette méthode d'authentification a de nombreuses faiblesses, néanmoins elle a aussi des avantages :
  - les mots de passe sont gratuits :)
  - la mise en oeuvre est relativement simple comparée aux autres méthodes (carte, jeton, biométrie,…)

le cnam

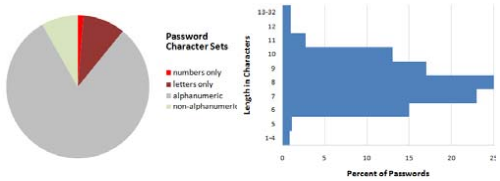
À propos de la qualité des mots de passe

- Mot de passe "simple"
  - love, pierre, cnam,…
- Mots de passe moins simple :
  - o2)!8ze%&u/\:), scjh8é"7sh6,…
- En théorie une clé cryptographique :
  - Sur 64 bits : il y a 2^{64} possibles et une attaque doit tenter 2^{63} clés ?
- Un mot de passe sur 8 caractères à autant de possibilité (8 bits par caractère * 8) soit 2^{64}, mais dans les faits c'est différent… les mots ont un sens et sont dans le dictionnaire !

le cnam

Exemple sur des mots de passe

- Sur 34 000 mots de passe de Myspace capturés en 2006



  - 28% des mots de passe sont composés de minuscules suivies d'un chiffre (qui est, dans 2/3 des cas, le chiffre '1')
  - 3,8% sont un simple mot du dictionnaire; 12% sont un mot du dictionnaire suivi d'un chiffre ('1' dans 2/3 des cas)
  - Mots de passe les plus fréquents :
    – password1, abc123, myspace1, password, qwerty1, fuckyou, 123abc, baseball1, football1, 123456, soccer, monkey1, liverpool1, princess1, jordan23, superman1, iloveyou1, monkey
- Source :
  - http://www.schneier.com/blog/archives/2006/12/realworld_passw.html

le cnam

Attaque de Twitter

- Piratage Twitter, 5 janvier 2009
  - Par force brute car twitter autorisait un nombre illimité d'échecs d'authentification consécutifs
  - Il a fini par trouver le mot de passe du compte 'Crystal' ('happiness')... compte administrateur du site !
  - Il a ensuite réinitialisé les mots de passe des comptes 'officiels' de Barack Obama, Britney Spears et Fox News... et commencé à diffuser de faux messages…
    - http://www.wired.com/threatlevel/2009/01/professed-twitt/

le cnam

Politique de sécurité

- Une politique sur les mots de passe
  - Les mots de passe sont attribués par le système
  - Difficile à maintenir si les utilisateurs peuvent changer leur mot de passe
    - et en terme d'acceptabilité

le cnam

Mécanismes de sécurité

- Assignation des mots de passe par le système
- Changement périodique des mots de passe
- Freiner les attaques par dictionnaire
  - Mettre une temporisation en cas d'échec de l'authentification
    - Quel temporisation
      - Skype après un certain nombre de refus attente 24h !
    - Déblocage administrateur (personne)

le cnam

Sur la gestion des mots de passe

- L'utilisateur présente son mdp
  - `User > lambda`
  - `Pwd  > mdp`
- Le système doit comparer le mdp présenté avec celui de référence
- Comment stocker sur le système les mdp de référence ?
- Solution cryptographique

le cnam

Gestion des mdp

- Le système mémorise pour chaque utilisateur *user* le *mdp*
  - (user, h (mdp_{user}))
- Exercice :
  - Proposer une fonction h
  - Discuter les +/- de celle-ci
  - Quels sont les risques et les attaques possibles
  - Proposer des contre mesures
  - Estimer pour chaque cas/hypothèse les chances (probabilités) de succès d'un attaquant.

le cnam

Un ou des mdp ?

- Un utilisateur à de nombreux de mots de passe à retenir
  - Utiliser le même mot de passe pour des applications avec des niveaux de sécurité différents
  - Le niveau de sécurité final atteint est abaissé au niveau le plus faible de toutes les applications
  - L'application qui protège le moins bien les mots de passe des utilisateurs conditionne le niveau de sécurité de toutes les autres
- En entreprise (voir le cas Twitter) un problème sur un compte peut entrainer de nombreux problèmes...

le cnam

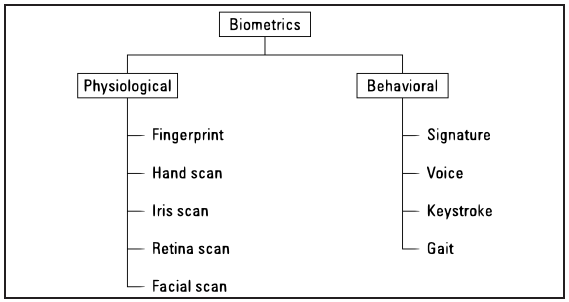
Autres points et problèmes

- Les journaux d'événements (fichiers 'logs') peuvent contenir des mots de passe ou des informations qui leur sont proches
  - « Audit log : failure : login failure for user 'footbamm' on ttyp4 »
- Logiciels espions ('spywares'), enregistreurs de frappe ('keyloggers')…
- Bugs de logiciels, par exemple crash avec vidange mémoire sur disque contenant des mots de passe ou clés privées…
- Systèmes de détection de mdp faibles
  - L'administrateur système peut (doit) utiliser ces outils de détection de mots de passe faibles...
    - 'John the Ripper' http://www.openwall.com/john/
    - L0phtCrack (Windows)
    - http://www.pwcrack.com/
    - http://www.passwordportal.net/

le cnam

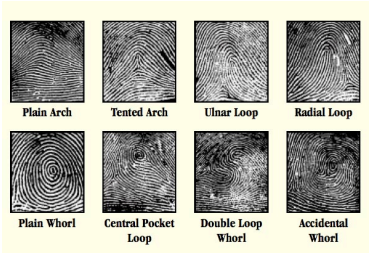
Biométrie

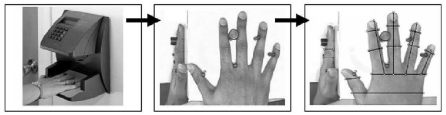
- mdp : ce que vous connaissez
- Biométrie : "ce que vous êtes"
- Les caractéristiques utilisées

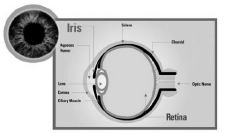


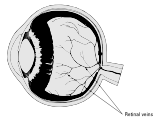
le cnam

Exemples









le cnam

Autres exmples



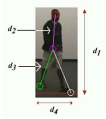
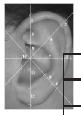



Figure 1.7: Other biometrics: signature, handgrip, gait, ear

Physiological	Behavioural
Fingerprint	Handwritten signature
Face	Keystroke dynamics
Iris	Gait
Retina	Handgrip dynamics
Voice	Voice
Vein pattern	Lips dynamics
Palmprint	Mouse dynamics
Hand geometry	
DNA	
Facial thermograms	
Body odor	
Fingernail bed	
Brainwave pattern	
Biodynamic signature	
Otoacoustic emissions	
Ear shape	
Skin spectrography	

le cnam

Système biométrique

- Un système biométrique comporte les deux phases suivantes :
  - Enrôlement de l'utilisateur
  - Vérification de l'identité
- L'enrôlement consiste pour **chaque** sujet du système à enregistrer les caractéristiques discriminantes et à conserver celle-ci
- La vérification ce fait aux points de contrôle du système. Le sujet se présente, ses caractéristiques sont recueillies puis comparées avec celle de la base de référence.
- À partir des données collectées, il y a identification du sujet.
  - i.e. : recherche dans la base par égalité et/ou similitude si le système reconnaît ou pas le sujet !

le cnam

Schéma (Claude Barral PhD)

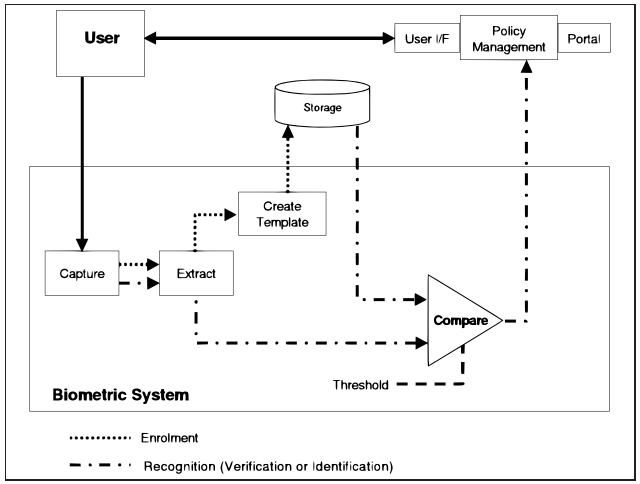


Figure 1.8: General Architecture of a biometric system

le cnam

Caractéristiques d'un système biométrique

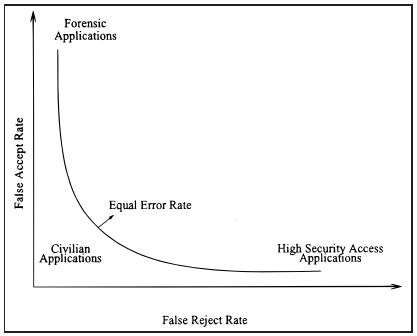
- Identification vs Authentification
- Les caractéristiques doivent être basées sur des facteurs qui varient peu dans le temps
- En fonction des cultures, il y a des enrôlements et des contrôles qui sont plus ou moins bien admis
- En terme opérationnel, on attend d'un système qu'il soit rapide, simple, fiable et précision (discrimination)

1	Universality	Can anyone provide the considered biometrics?
2	Uniqueness	How hard is it to find two persons with close characteristics?
3	Permanence	Stability along the lifetime
4	Collectability	How easy/cheap is it to capture the biometric data?
5	Performance	Which FAR/FRR can the system provide?
6	Acceptability	How well will end-users appreciate the system?
7	Circumvention	How hard is it to fool the system?

le cnam

Mesure de la “qualité” d’un système

- On utilise en général deux taux d’erreurs pour caractériser un système
- Un utilisateur est authentifié à la place d’un autre utilisateur :
  - False Accept Rate (FAR)
- Un utilisateur valide n’est pas reconnu
  - False Reject Rate (FRR)
- Les taux FAR et FRR sont liés
  - Si le FAR est faible alors le FRR sera fort
- Il existe aussi le Crossover Error Rate (‘CER’) : c’est le taux pour lequel le taux de fraude est égal au taux de rejet



le cnam

Et des attaques possibles (C. Barral)

- Au de là du doigt coupé !

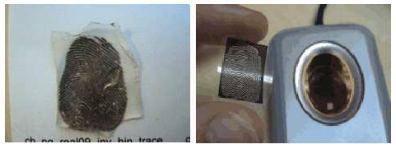


Figure 7.6: Faking with classical prints

Figure 7.4: Glycerin - left: thin layer - center: thick layer - right: 3D models

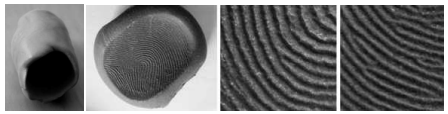


Figure 7.1: Molds and Details

per 100gr	Price (€)	Molds	Appreciation	Setting time	Remark
Siligum	4	6	+++	5 min	resistant, flexible
Plasticine	1.5	10	++	1 min	no hardening, reusable
Fimo	2.5	7	+	30 min	hard material
Patarev	10	25	++	half day	light flexibility
Alginate	6	20	--	5 min	not convenient
UtilePlast	5	8	+	30 min	hard material, reusable
Latex	2	10	-	few days	not convenient
Candle Wax	1	20	-/+	10 min	very fragile, reusable
Repair Paste	20	20	+	half day	hard material, porous

Table 7.1: Fingerprint molding materials

le cnam

Ce que vous portez

- Pièce d’identité, passeport
- Badge d’accès employé
- Clé de voiture
- Ordinateur portable, adresse MAC…
- Carte à puce (Carte bancaire, carte SIM, voir cours SMOS)
- Clé USB
- Token/Jeton (SecurID, Générateur de mots de passe à usage unique)

le cnam

Déploiement

- Complexité ajouté au système :
  - distribution du dispositif
  - perte/vol/destruction
  - diversification des clés

le cnam

Principe du mot de passe à usage unique

- Authentification via un générateur de mots de passe à usage unique
- Protocole :

Alice	Bob
Je suis Alice	
	<- *x*
x & Pin Code	
f(x) ->	
	f(x) ?

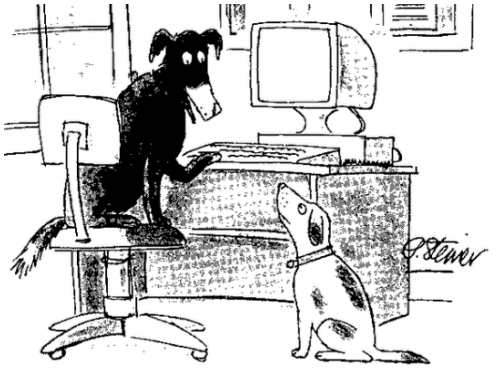
le cnam

Authentification forte

- De plus en plus de réglementation demande une authentification forte ou authentification à **double facteur** reposant sur la combinaison de deux des facteurs suivants :
  - Ce que vous savez
  - Ce que vous êtes
  - Ce que vous possédez
- Exemple : carte à puce et biométrie, security token

le cnam

And on internet...



"On the Internet, nobody knows you're a dog."

le cnam

Identification/Authentification

- Chaque site web sur Internet dispose de son propre système d'authentification et de sa propre base de données contenant la liste de ses utilisateurs
- Cela oblige les utilisateurs à s'enregistrer et à devoir mémoriser des 'pièces justificatives' ('credentials') différentes pour chaque site visité :
  - Typiquement un couple (login, mot de passe)
  - Syndrome de la « fatigue du mot de passe »

le cnam

Authentification unique

- On parle aussi de SSO (Single Sign On)
- Rendre l'identité d'un utilisateur 'portable' à travers plusieurs systèmes administrés de façon autonome :
  - L'utilisateur ne s'authentifie qu'une seule fois
    - Ses 'pièces justificatives' ('credentials') le suivent quel que soit le site visité
    - Les authentifications successives sont transparentes pour l'utilisateur
- Toutefois, l'identité de l'utilisateur ne doit être révélée que s'il le souhaite – et il peut alors choisir quelle identité utiliser s'il en a plusieurs.

Les propositions

- Microsoft Passport / Live ID, CardSpace
- WS-Federation
- Liberty Alliance
- Exercice
  - Comparer les deux approches suivantes :
    - OpenID
    - OAuth

Bibliographie

- Cours Nicolas Pioche (RSX112)
- Claude Barral (PhD)
- Ross Anderson
  - Security Engineering : A Guide to Building Dependable Distributed Systems
  - http://www.cl.cam.ac.uk/~rja14/book.html