Identités numériques

Guillaume Allègre
Allegre.Guillaume@free.fr

Guilde

Guilde

2011-10-13

L'identité numérique de la préhistoire à nos jours

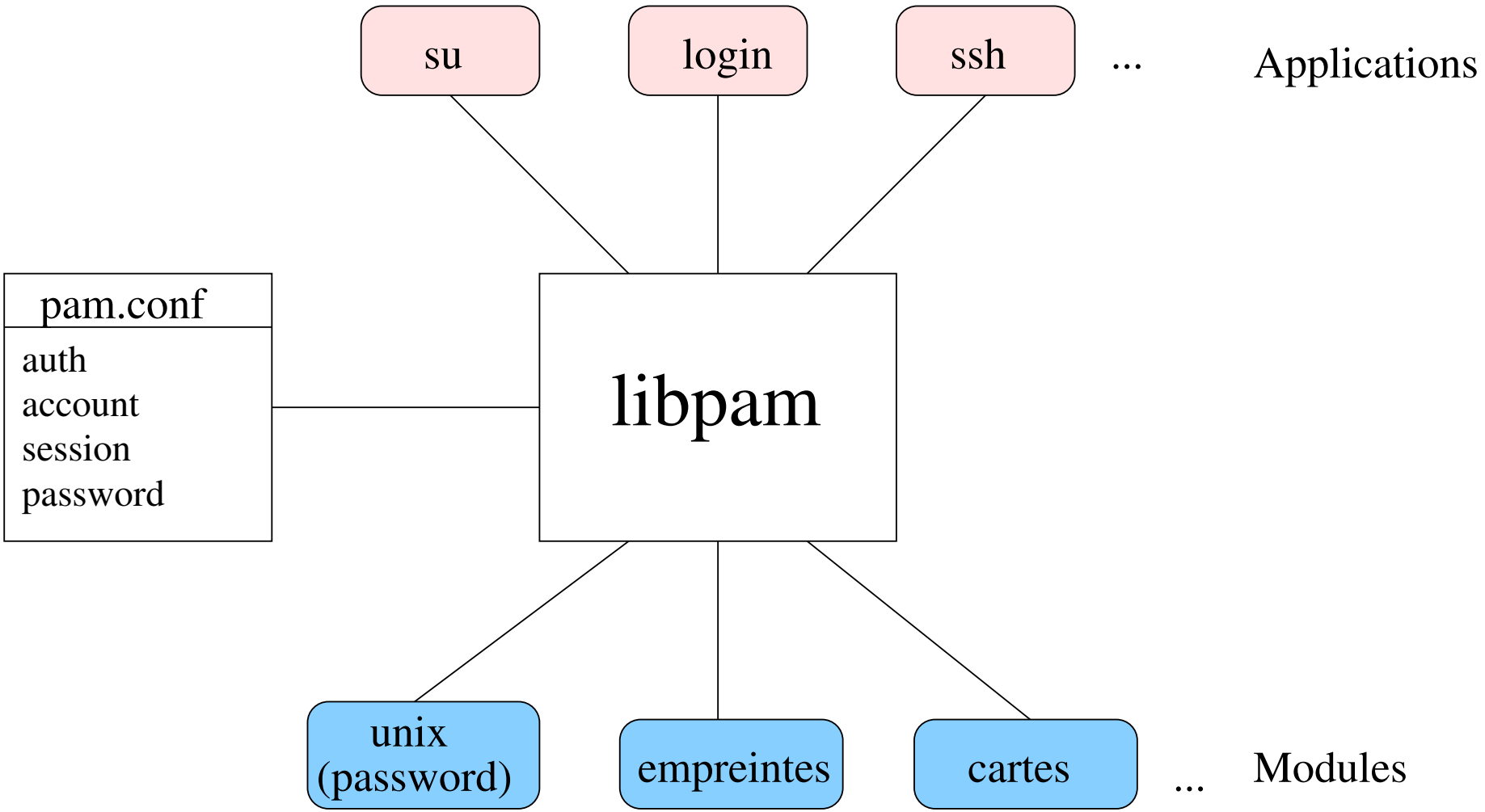
Identité numérique : les trois aspects

- Identification
  - login
  - biométrie...
- Authentification (*authentication*)
  - mot de passe
  - biométrie
  - clé, carte à puce, périphérique OTP...
- Autorisations (*authorization*), ex. Linux
  - groupes
  - Access Control Lists (ACL)
  - capacités (man 7 capabilities)
  - LSM : SELinux, SMACK...

AuthN et AuthZ : Apache

- Apache -> 2.1
  - mod_auth
  - mod_access
- Apache 2.2+
  - mod_auth_basic
  - mod_authn_file
  - mod_authn_dbm
  - mod_authz_host
  - mod_authz_owner
  - mod_authnz_ldap

AuthN et AuthZ : PAM (Pluggable Authentication Modules)



PAM : les 4 gestionnaires (services, types. . .)

- `auth` : ambigüité
  - *authentication* : authentification
  - *authorization* : permissions (*set credentials*)
- *account management* : limitations d'accès auxiliaires (horaires, ressources, origine...)
- *session management*
  - ouverture : montage, logs, permissions sur les périphériques...
  - fermeture
- *password* (le mal nommé)
  mise à jour du "mot de passe" et de tous les *auth. token*

Avant Internet

- Identité liée à la machine
- Autorité de confiance = l'administrateur système

Les premiers réseaux

- Réseaux locaux (d'entreprise...)
  - administration centralisée
  - annuaire disponible (ou possible)
  - contexte local

- Réseaux point à point
  - généralement sur modem RTC (*dial-up*)
  - protocole spécialisé : UUCP (Unix to Unix Copy)
  - méthode "stocke et envoie" (*store-and-forward*)
  - adaptée à une connexion quotidienne

Cas particulier : le mail UUCP

- Fonctionnement
  - connexion point à point de deux machines
  - routage explicite
  - chemin complet (bang-path) :
    `hosta ! hostb ! mit-ai ! ucbvax ! johndoe`
- Remarque
  Reste utilisé dans les newsgroups (usenet, NNTP) pour le suivi de propagation

La boîte à outils cryptographique

- Suite cryptographique (*Cipher suite*) (SSL/TLS)
  - Hachage cryptographique : MD5, SHA-1...
    (MAC, *Message Authentication Code*)
  - Chiffrement symétrique : DES, AES...
    (*bulk encryption*)
  - Chiffrage asymétrique (clés publiques/privées) : RSA, DSA, ECDSA...
    (*authentication*)
  - Protocole d'échange de clés : RSA, Diffie-Hellman, ECDH...
  - Générateur aléatoire
    (PRF *pseudorandom fonction*)

- Auxiliaires
  - compression des données

Réseau de confiance (*web of trust*)

- Origine
  Phil Zimmermann, manuel de PGP 2.0 :
  [...] This will cause the emergence of a decentralized fault-tolerant web of confidence for all public keys.
- Évolution
  PGP (1991) $\longrightarrow$ OpenPGP (IETF, 1997) $\longrightarrow$ GnuPG (1999)
- Utilisation d'un serveur de clés publiques
  ex. `hkp://subkeys.pgp.net`
  - 1 - dépôt de chaque clé publique
  - 2 - signature des clés des personnes connues
    - présence et identité physique
    - clé publique (empreinte)
    - "certificat d'identité" (carte...)

Réseau de confiance (*web of trust*)

- Points forts
  - décentralisé et réciproque, contrairement à une PKI X.509
  - relativement modulable par l'utilisateur (degrés de confiance)

- Points faibles
  - repose sur l'identité réelle (pas de pseudonyme...)
  - repose sur la compétence de chacun à évaluer la fiabilité d'une identité
  - repose sur une autorité nationale (carte d'identité)
  - key-signing party => vos papiers !

Le mythe de l'anonymat

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

Peter Steiner, *The New Yorker magazin*, 1993

Web 2.0 et réseaux sociaux

- "Marc L***", *Le Tigre*, novembre 2008
  Bon annniversaire, Marc. Le 5 décembre 2008, tu fêteras tes vingt-neuf ans[...] Tu ne me connais pas, c'est vrai. Mais moi, je te connais très bien. C'est sur toi qu'est tombée la (mal)chance d'être le premier portrait Google du Tigre. Une rubrique toute simple : on prend un anonyme et on raconte sa vie grâce à toutes les traces qu'il a laissées, volontairement ou non sur Internet.

- *Facebook Connect*, 2008-2009 $\longrightarrow$ fournisseur d'identité (*IdP, identity provider*)

- Google+ (2011) et ses conditions d'utilisation :
  nom et sexe (genre ?) réels

Identité numérique : anonymat et pseudonymat

- Protection des centres d'intérêt disjoints
  Ex.
  - militant politique
  - réseau professionnel
  - cercle d'amis
  - ...

- Cas d'école
  Billet "Anonymat et expertise", *Journal d'un avocat*, Maître Eolas, 15 septembre 2011.
  Je ne suis pas anonyme, j'ai un nom, et il l'utilise : Eolas. Ce nom est un pseudonyme[...]. Je préfère donc parler de pseudonymat.