Identification: la fin du mot de passe ?

par
Christophe Wolfhugel

Hervé Schauer Consultants

© Hervé SCHAUER Consultants - Mars 1993 - Reproduction interdite

Identification: la fin du mot de passe ?

par
Christophe Wolfhugel

Email: wolf@fr.net
Télécopie: +33 1 46 38 05 05
Téléphone: +33 1 46 38 89 90

Version 1.0
Février 1994

La composition de ce document a été entièrement réalisée sur le système d'exploitation Unix, à l'aide :

— du formatteur de document standard *troff*, accompagné des filtres standards *pic*, *tbl* et *eqn*,

— du filtre *accent* de Philipe Dax (Télécom Paris),

— du logiciel de dessin *xfig*, et des filtres *f2ps* et *psfig*,

— du prévisualiseur *Ghostscript*,

— du traducteur PostScript *tscript* de Gilles Dauphin (Télécom Paris).

Copyright © Hervé Schauer Consultants 1994

I. Prouver son identité

— Mot de passe

— *Login* et mot de passe

— Moyens biométriques

— Outils demandant des extensions matérielles: cartes à puce

— Outils facilement transportables: calculettes de chiffrement

© Hervé SCHAUER Consultants - Mars 1993 - Reproduction interdite

II. Login et mot de passe

— Méthode la plus simple

— Implémentée partout

— Le *login* est toujours utilisé sur les systèmes d'information

— Mais il reste des méthodes d'accès par mot de passe seul

— Risque de divulgation

— Risque d'écoute

© Hervé SCHAUER Consultants - Mars 1993 - Reproduction interdite

III. Méthodes lourdes

— Demandent des investissement importants en matériel (lecteur de cartes, ...)

— Dépendance vis-à-vis du matériel rendant l'accès pour les personnes en déplacement peu commode

— Sécurité à priori très bonne

— Facilité d'utilisation: pas de code secret, pas de manipulation: *plug and play*

© Hervé SCHAUER Consultants - Mars 1993 - Reproduction interdite

IV. Méthodes légères

— Investissements matériels moins importants (bien que non négligeables)

— Méthode plus pratiquable pour les personnes qui bougent beaucoup

— Sécurité à priori également très bonne

— Utilisation demandant éventuellement une intervention de l'utilisateur (saisie de code secret, retaper le challenge et la réponse)

© Hervé SCHAUER Consultants - Mars 1993 - Reproduction interdite

V. SecurID

— Produit de Security Dynamics Inc.

— Génération d'un mot de passe unique toutes les 60 secondes

— Synchronisation des horloges entre calculette et serveur par ajustement des dérives

— L'utilisateur dispose d'un code secret (PIN) qu'il tape avec le code généré par la SecurID

— Algorithme secret: aucun source n'est fourni, il s'agit de faire confiance a Security Dynamics

— La sécurité par l'obscurité ne créée-t-elle pas plus de problèmes qu'elle n'en corrige ?

— Autonomie: 1 à 3 ans au choix

© Hervé SCHAUER Consultants - Mars 1993 - Reproduction interdite

VI. DigiPass

— Produit de Digiline (France, Belgique, Pays-Bas)

— Le logo ressemble étrangement à celui de Digital Pathways (qui a pompé sur l'autre ?)

— L'utilisateur dispose d'un PIN de 5 chiffres

— Un mot de passe est généré, fonction du temps, du numéro de série et du PIN chiffrés par DES

— Peut gérer l'accès jusqu'à 9 systèmes différents

— Utilisation du DES: algorithme connu

— Autres fonctions: signature et test

— Autonomie: 3 and, rechargement nécessaire après le changement de pile

© Hervé SCHAUER Consultants - Mars 1993 - Reproduction interdite

VII. Optical Key

— Produit de ADV Technologies

— Modes de fonctionnement: question - réponse, génération de mot de passe aléatoire ou génération de mot de passe à partir d'un identifieur

— Mode question - réponse: identique au fonctionnement de la SecureNet Key

— Mode génération de mot de passe: ressemble à SecureID, mais algorithme DES

— Mode génération à partir d'un identifieur: mode hybride, permet d'avoir plusieurs serrures (points d'accès)

— Utilisation du DES

— Jusqu'à 10 clés

© Hervé SCHAUER Consultants - Mars 1993 - Reproduction interdite

— Possibilité de lecture optique (gadget ?) pour les communications de la serrure vers la carte

— Autonomie: 1 an, remplacement de la pile sans perte d'information grâce à une pile secondaire

© Hervé SCHAUER Consultants - Mars 1993 - Reproduction interdite

VIII. SecureNet Key

— Fabricant: Digital Pathways

— Fonctionne sur le mode question - réponse

— Périphérique le plus simple

— Accès protégé par un PIN allant jusqu'à 8 chiffres connu de l'utilisateur

— La serrure génère une question sous la forme d'un nombre pseudo-aléatoire de 8 chiffres unique dans le temps (algorithme laissé au choix de l'implémenteur) et utilisé pour un chiffrement DES par une clé secrete. Résultat sur 8 caractères

— Utilise un chiffrement DES d'une clé secrète connue de la serrure et de la calculette

— Mode décimal ou mode hexadécimal

© Hervé SCHAUER Consultants - Mars 1993 - Reproduction interdite