

République Algérienne Démocratique et Populaire
Université des Sciences et de Technologie
Houari Boumedienne (USTHB)

Institut d'Informatique

Mémoire de Fin d'Etudes

En vue de l'obtention d'un diplôme
d'Ingénieur d'Etat en Informatique

THEME

Mise en Oeuvre d'un Système d'Authentification Avancée

Présenté Par :

- Mr Mounir Benzaid
- Mr Bachir Mihoubi

Encadrés Par :

- Mme Nadia Nouali

Membres du Jury :

- Mme Samira Moussaoui
- Mme Aicha Mokhtari
- Mme Djamila Medjahed

Organisme d'accueil :

Centre de Recherche sur l'Information Scientifique & Technique
" CERIST "

Promotion 1998 N° 55 / 98

RESUME

Etant donné la croissance des systèmes informatiques et le nombre de plus en plus grand de réseaux interconnectés et le caractère de plus en plus sensible et confidentiel des données, le problème de la sécurité des données est aujourd'hui incontournable .

L'un des problèmes rencontrés est qu'il est devenu considérablement plus difficile d'authentifier les utilisateurs et de vérifier que la personne qui demande à accéder à une ressource (données, services) est bien celle qui en a les droits .

La technique classique d'authentification basée sur les mots de passe n'est plus valable dans le contexte réseau car les mots de passe transmis sur le réseau peuvent être espionnés et réutilisés pour une violation d'accès. Des techniques d'authentification avancées ont été conçues pour pallier à ces faiblesses .

Dans ce mémoire une méthode d'authentification basée sur la notion de mots de passe utilisés une fois (*One Time Password*) a été mise en œuvre. Le système réalisé permet d'authentifier les utilisateurs désirant se connecter à partir d'un système distant sans craindre d'avoir leurs mots de passe espionnés sur le réseau .

Mots Clés : Réseaux, Sécurité, Cryptographie, Authentification, Mot de passe, OTP (One Time Password), Kerberos .

SOMMAIRE

INTRODUCTION	1
---------------------------	----------

CHAPITRE I : Les réseaux informatiques et leurs architectures

1 - Introduction	3
2 - Catégories de réseaux	3
3 - Architecture de réseaux	4
3.1 - Le modèle de référence OSI	4
3.2 - Internet et le protocole TCP/IP	5
3.2.1 - Qu'est ce qu'un Réseau Internet ?	5
3.2.2 - Les Hôtes d'Internet	6
3.2.3 - Caractéristiques de TCP/IP	6
3.2.4 - Architecture des protocoles TCP/IP	7
3.3 - TCP/IP et le Modèle OSI	13

CHAPITRE II : Problématique de la sécurité informatique

<u>Partie 1</u> : Un aperçu sur les problèmes de sécurité informatique	14
--	----

1.1 - Introduction	14
1.2 - Objectifs de la sécurité informatique	14
1.3 - Menaces de sécurité	15
1.4 - Sécurité sur Internet et vulnérabilités du protocole TCP/IP	21
1.4.1 - Facteurs contribuant aux problèmes de sécurité sur <i>Internet</i>	23
1.4.2 - Authentification faible	23
1.4.3 - Facilite d'espionnage / interception	24
1.4.4 - Facilite de déguisement / duperie	24
1.5 - Les services de sécurité vue par le modèle « OSI »	26
1.6 - Les mécanismes de sécurité	27

<u>Partie 2</u> : Mécanismes de base de la sécurité informatique : les outils cryptographiques	30
---	----

2.1 - Introduction	30
2.2 - Définitions	30
2.3 - La cryptographie moderne	30
2.4 - Techniques de la cryptographie moderne	31
2.4.1 - Algorithmes à clef secrète	32
2.4.2 - Algorithmes à clef publique	33
2.4.3 - Fonctions de hachage à sens unique	36

CHAPITRE III : Authentification avancée

1 - Introduction	39
2 - Authentification avancée	39

3 - Principes de l'authentification	40
4 - Les mécanismes d'authentification	42
4.1 - Authentification basée sur les mots de passe (méthode classique)	42
4.1.1 - Aspect général	42
4.1.2 - Facteurs qui affectent la sécurité du mot de passe	42
4.1.3 - Problèmes avec l'authentification basée seulement sur les mots de passe	46
4.2 - Authentification par un système de question-réponse	47
4.3 - Authentification basée sur le Jetons	48
4.3.1 - Aspect général	48
4.3.2 - Facteur de Forme	48
4.3.3 - Interface de station de travail	49
4.3.4 - Capacité de traitement	50
4.3.5 - Résumé	53
4.4 - Authentification basée sur la biométrie	54
4.4.1 - Aspect général	54
4.4.2 - Fonctionnement	55
4.5 - Combinaison des méthodes	57
4.6 - Protocoles Cryptographiques	58
4.6.1 - Introduction aux protocoles cryptographiques	58
4.6.2 - Authentification grâce à la cryptographie à clef secrète	59
4.6.3 - Authentification grâce à la cryptographie à clef publique	60
4.6.4 - Authentification mutuelle par mots de passe et fonction à sens unique	61
4.6.5 - Authentification de Needham et Schroeder par cryptosystème à clef symétrique	62

CHAPITRE IV : Systèmes d'authentification complets

1 - La méthode <i>KERBEROS</i>	64
1.1 - Introduction	64
1.2 - Le modèle de <i>KERBEROS</i>	65
1.2.1 - Sécurité modulable	66
1.2.2 - Les composantes logicielles	66
1.3 - Les noms de <i>KERBEROS</i>	68
1.4 - Fonctionnement de <i>KERBEROS</i>	68
1.4.1 - Les accréditations	69
1.4.2 - Obtention du premier ticket	70
1.4.3 - Obtention de tickets pour un service	71
1.4.4 - Demande d'un Service	72
1.5 - Sécurité de <i>KERBEROS</i>	73
2 - La méthode <i>ONE TIME PASSWORD</i>	76
2.1 - Introduction	76
2.2 - Objectifs	77
2.3 - Description du système <i>S/KEY</i>	77
2.3.1 - Fonction de hachage à sens unique	78

2.3.2 - Génération des mots de passe one-time	79
2.3.3 - Vérification des mots de passe one-time	80
2.3.4 - Changement de la phrase de passe secrète	80
2.4 - Fonctionnement du Système <i>S/KEY</i>	81
2.5 - Vulnérabilités	83
2.6 - Algorithme de hachage à sens unique <i>MD4</i> et <i>MD5</i>	84
2.6.1 - Description de <i>MD5</i>	84
2.6.2 - La différence entre <i>MD4</i> & <i>MD5</i>	87
3 - Etude comparative entre <i>KERBEROS</i> et <i>ONE TIME PASSWORD</i>	88
4 - Conclusion	90

CHAPITRE V : Mise en œuvre du système d'authentification OPAL

1 - Introduction	91
2 - Déroulement de l'authentification <i>OPAL</i>	91
3 - Fonctionnalités du système	92
3.1 - Côte Client	92
3.2 - Côté Serveur	94
4 - Composantes logicielles	96
4.1 - Outils de génération de mots de passe <i>OTP</i>	96
4.1.1 - La commande <i>OPALKEY</i>	96
4.1.2 - La commande <i>OPALGEN</i>	97
4.1.3 - La commande <i>WINKEY</i>	97
4.2 - Outil d'initialisation	98
4.3 - Applications pratiques de connexion	100
4.3.1 - La commande <i>OPALOGIN</i>	100
4.3.2 - Modification de l'application <i>Telnet</i>	106
4.3.3 - Modification d'autres programmes	110
5 - Bases de données	111
5.1 - La base de données <i>OPAL /etc/opalkeys</i>	111
5.2 - La base de données d'autorisation <i>/etc/opalaccess</i>	112
6 - Bibliothèque du système <i>OPAL " libopal.a "</i>	113
7 - Environnement d'implémentation	117
8 - performances et perspectives	118
CONCLUSION	122

BIBLIOGRAPHIE

ANNEXES

- Annexe A - Les couches OSI et TCP/IP*
- Annexe B - Autres protocoles cryptographiques*
- Annexe C - Le modèle Client / Serveur*
- Annexe D - Extrait du dictionnaire standard OTP*

GLOSSAIRE