

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Centre Universitaire Larbi Tébessi

TEBESSA

Institut des Sciences de l'Ingénieur

Département d'Informatique

N° d'ordre :

Série :

MEMOIRE

En vue de l'obtention du diplôme de magister en informatique

Option : Système d'Information Avancés

et Bases de Connaissance

Une Architecture Basée Agent
Pour la Gestion de la Sécurité des
Systèmes d'Information WEB

Présenté par : **Mr Derdour Makhoulf.**

Dirigé par : **M^{me} Z.Boufaïda.**

Soutenance le : 25/11/2004

Devant le jury :

Président : **Dr. Mahmoud Boufaïda**

Rapporteur : **Dr. Zizette Boufaïda**

Examineurs: **Dr. Mohamed Chaouki Batouche**

Dr. Nacereddine Zarour

Professeur

Professeur

Professeur

Maître de conférence

Univ.Constantine

Univ.Constantine

Univ.Constantine

Univ.Constantine

Résumé

La sécurité sur Internet est un problème complexe surtout dans les entreprises pratiquant le B2B, pour la simple raison qu'elle n'a pas été introduite en même temps que les logiciels qu'ils utilisent.

Pour vendre les produits rapidement, les concepteurs des logiciels ont laissé la sécurité de côté en pensant qu'ils pouvaient l'intégrer facilement par la suite. Mais en fait, l'assurance de la sécurité dans un environnement qui a été conçu sans, pose de nombreux problèmes tels que l'intégration des systèmes pour la gestion des accès, des autorisations, de l'intégrité des données, de l'authentification des utilisateurs...

Afin d'éviter tous ces problèmes, nous proposons une stratégie de sécurité qui s'appuie sur un système Multi-agents pour la construction d'un système de sécurité homogène, évolutif dans le temps, robuste et adaptatif en terme de protection. Par ailleurs, le but de ce système est d'éloigner au maximum l'agent humain (personnels de l'entreprise) car ce dernier est classé parmi les failles les plus dangereuses dans les systèmes d'informations actuels (Problème de confiance).

Summary

Security on Internet is a complex problem especially in the companies practicing the B2B, for the simple reason, which it was not introduced at the same time as the software that they use.

To sell the products quickly, the software designers left the safety on side by thinking that they could integrate it easily later. However, assuring security in an environment, which was conceived without, poses many problems such as the systems integration for the management of the access, the authorizations, the integration of the data, the authentication of the users, etc.

In order to avoid all these problems, we propose a strategy of security, which is based on a Multi-agents system for the construction of a homogeneous security system. This system is evolutionary in time, robust and adaptive in term of protection. In addition, its goal is to avoid the interaction of human agents (personal of the companies) classified among the most dangerous faults in the current information systems (confidence problem).

ملخص

إن الأمن داخل الإنترنت يمثل مشكلة معقدة خاصة في المؤسسات التي تعمل بنظام **B2B** هذه المشكلة وليدة عدم تزامن ظهورها مع مختلف البرمجيات التي اعتقد المصممون و للإسراء ببيعها أنه يمكن إدراج الناحية الأمنية بسهولة في هذه البرمجيات لكن في الحقيقة ، ضمان الأمن في محيط مصمم دون الأخذ بعين الاعتبار هذه الناحية تطرح عدة مشاكل منها إدماج الأنظمة لتسيير البلوغ ، الموافقات و التحقق من المستعملين و المعطيات.

و لتجنب كل هذه المشاكل ، نقترح إستراتيجية للأمن و التي تركز على نظام متعدد الأعوان ، لإنشاء نظام أمن متجانس ، قابل للتطوير خلال الزمن ، قوي و متلائم فيما يخص الحماية ، إضافة إلى ذلك هدف هذا النظام هو الاستغناء على أبعاد مدى عن تدخل العنصر البشري و المتمثل في عمال المؤسسة ، ذلك لأن هذا الأخير يمثل أخطر الثغرات في أنظمة المعلومات المعاصرة (مشكل الثقة)

SOMMAIRE

INTRODUCTION GENERALE.....	1
----------------------------	---

Chapitre 1 : Problème de sécurité des systèmes informatiques
--

I. INTRODUCTION	6
II. Sécurité.....	7
II.1. Définition et terminologie.....	7
II.2. Objectifs et règles de sécurité	8
II.2.1. <i>La disponibilité</i>	8
II.2.2. <i>L'intégrité</i>	8
II.2.3. <i>L'authentification</i>	8
II.2.4. <i>Le contrôle d'accès</i>	8
II.2.5. <i>La confidentialité</i>	9
II.3. Causes de la vulnérabilité des systèmes.....	9
II.4. Sûreté des systèmes de sécurité	9
II.5. Les principaux facteurs de sécurité.....	10
II.5.1. <i>Environnement Organisationnel et économique</i>	10
II.5.2. <i>Facteurs socio-économiques</i>	10
II.5.3. <i>Sécurité physique des bâtiments</i>	10
II.5.4. <i>Sécurité informatique générale</i>	11
II.5.5. <i>Sécurité de l'exploitation</i>	11
II.5.6. <i>Sécurité des applications</i>	12
II.5.7. <i>Assurances informatiques</i>	12
III. Attaque.....	12
III.1. Définition d'une attaque.....	12
III.2. Classification des attaques.....	13
III.3. Types d'attaques et d'intrusions.....	13
III.3.1. <i>Différentes méthodes d'attaques</i>	13
III.3.2. <i>Différentes formes d'attaques</i>	15
III.4. Mécanismes d'attaques contre un système informatique.....	16
III.4.1. <i>Le spoofing</i>	16
III.4.2. <i>Le flooding</i>	20
III.4.3. <i>Le sniffing</i>	22
III.4.4. <i>Le scanning</i>	22
III.4.5. <i>Les virus, vers et chevaux de Troie</i>	22
III.4.6. <i>Les attaques en déni de service</i>	25
III.4.7. <i>L'exploitation des vulnérabilités système</i>	25
III.4.8. <i>L'exploitation des vulnérabilités protocolaires</i>	26
IV. CONCLUSION.....	26

Chapitre 2 : Différentes techniques de sécurité

I. INTRODUCTION	28
II. La protection	28
II.1. La cryptographie.....	29
II.1.1. <i>Le chiffrement</i>	29
II.1.2. <i>Les condensés de message</i>	30
II.1.3. <i>Les signatures numériques</i>	32
II.2. L'authentification	32
II.2.1. <i>Mots de passe</i>	33
II.2.2. <i>Certificats de clés publiques</i>	33
II.2.3. <i>Biométrie</i>	35
II.3. La gestion des autorisations.....	36
II.3.1. <i>Hôte Bastion</i>	37
II.3.2. <i>Filtre de paquets</i>	38
II.3.3. <i>Passerelle Proxy</i>	38
II.4. L'audit de sécurité	40
II.5. Les VPN	40
II.5.1. <i>Principe</i>	41
II.5.2. <i>Principaux protocoles de VPN</i>	41
III. La détection.....	41
III.1. Définition.....	42
III.2. Classification des IDS (Intrusion Detection System).....	42
III.2.1. <i>La technique utilisée</i>	42
III.2.2. <i>La source d'information</i>	42
III.2.3. <i>Le comportement en cas d'attaque détectée</i>	43
III.2.4. <i>Le paradigme de détection</i>	43
III.2.5. <i>La fréquence d'utilisation</i>	43
III.3. Détection d'intrusion utilisant l'approche par scénario.....	43
III.3.1. <i>Les systèmes experts</i>	44
III.3.2. <i>Les algorithmes génétiques</i>	44
III.3.3. <i>Le pattern matching</i>	44
III.4. Détection d'intrusion utilisant l'approche comportementale.....	44
III.4.1. <i>Modèle statistique</i>	45
III.4.2. <i>Système expert</i>	46
III.4.3. <i>Réseaux de neurones</i>	46
III.4.4. <i>Immunologie</i>	46
III.5. Limitation des IDS	46
III.5.1. <i>Architecture « monolithique »</i>	46
III.5.2. <i>Analyse des données imparfaites</i>	46
III.5.3. <i>Manque de corrélation et d'évaluation des dommages</i>	47
III.5.4. <i>Imperfections générales</i>	47
III.6. Caractéristiques souhaitées d'un IDS	48
IV. CONCLUSION.....	50

Chapitre 3 : les systèmes Multi-agents et la sécurité

I. INTRODUCTION	51
II. L'approche agents.....	51
II.1. Définition des Systèmes Multi-agents	52
II.2. Classification des agents	53
II.2.1. <i>Catégories d'agents</i>	54
II.2.2. <i>Types d'agents</i>	54
II.3. Format d'échange des données	54
II.3.1. <i>Format XML (description de la forme)</i>	55
II.3.2. <i>Format ACL / KIF / KQML (description du fond)</i>	55
II.4. Communication entre les agents	55
II.4.1. <i>Types de communication</i>	56
II.4.2. <i>Transport de messages</i>	56
II.4.3. <i>Architecture du SMA</i>	57
II.5. Problème lié aux SMA	58
III. Travaux de recherche en rapport avec notre travail	58
III.1. Détection des intrusions basée agents	58
III.2. Protection à base d'agents	59
III.3. Différents outils	61
IV. Conclusion	61

Chapitre 4 : Le système de sécurité « AASWIS »

I. INTRODUCTION	63
II. Système « AASWIS »	63
II.1. Architecture de système « AASWIS »	64
II.2. Différents composants du système « AASWIS »	65
II.2.1. <i>Protection</i>	65
II.2.2. <i>Détection</i>	66
II.2.3. <i>Service</i>	66
II.2.4. <i>Tolérance aux pannes</i>	66
II.3. Rôles des Agents	66
II.3.1. <i>Les agents de protection</i>	68
II.3.2. <i>Les agents de détection</i>	74
II.3.3. <i>Les agents de service</i>	76
II.3.4. <i>Les agents pour la tolérance aux pannes</i>	77
II.4. Spécification du protocole de communication entre agents	79
III. CONCLUSION.....	81

Chapitre 5 : Implémentation

I. INTRODUCTION	82
II. Implémentation sous JADE	83
II.1. Présentation et la mise en route de JADE	83
II.2. Création d'agents sous JADE	85
II.3. Outils JADE.	86

II.3.1. <i>Jade GUI</i>	86
II.3.2. <i>DF Agent</i>	86
II.3.3. <i>Dummy Agent</i>	87
II.3.4. <i>Sniffer Agent</i>	87
II.3.5. <i>Introspector Agent</i>	87
III. Applications	87
III.1. Agent d'authentification	91
III.1.1. <i>Actions de l'agent</i>	91
III.1.2. <i>Messages du protocole d'authentification</i>	92
III.2. Agent de cryptage.....	93
III.3. Agent d'inspection	94
IV. CONCLUSION	95
COCLUSION & PERSPECTIVE.....	96
GLOSSAIRE.....	98
BIBLIOGRAPHIE.....	100