

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderahmane Mira de Béjaïa
Faculté des Sciences et Sciences de l'Ingénieur

Département d'Informatique
ÉCOLE DOCTORALE RÉSEAUX ET SYSTÈMES DISTRIBUÉS



Mémoire de Magister en informatique

Option

Réseaux et Systèmes Distribués

Thème

Détection de l'attaque Eclipse dans le réseau eDonkey

Présenté par : Asma DAOUDI

Directeur du mémoire : Pr. BOUABDALLAH Abdelmadjid

Devant le jury composé de :

Président	DAHMANI Adbennasser	Professeur	Université de Bejaia,Algérie
Rapporteur	BOUABDALLAH Abdelmadjid	Professeur	UTC, Compiègne,France
Examineur	AHMED-NACER Mohamed	Professeur	USTHB, Alger,Algérie
Examineur	BADACHE Nadjib	Professeur	USTHB, Alger,Algérie
Invité	TARI Abdelkamel	Chargé de cours	Université de Bejaia,Algérie

Promotion 2006 – 2007

Résumé

Dans ce présent travail, nous avons analysé l'attaque Eclipse dans le cadre du réseau eDonkey. Dans cette attaque, un serveur attaquant a pour but de cacher la partie surveillée du reste du réseau en prenant comme cible la liste des serveurs du réseau eDonkey. Nous avons identifié deux scénarios différents de l'attaque Eclipse : Le premier scénario traite le cas où l'attaque est menée par un seul attaquant et le deuxième scénario traite le cas de plusieurs attaquants. Pour faire face à cette attaque nous avons proposé une solution basée sur la taille des listes des serveurs d'un client détecteur. Les résultats obtenus montrent l'efficacité de la solution proposée à détecter les deux scénarios d'attaques et à isoler les serveurs attaquants du reste des serveurs du réseau. Cependant, des fausses (accusations) alertes peuvent avoir lieu. Pour cela, nous avons proposé d'utiliser le profilage des utilisateurs, des ports TCP, UDP pour minimiser l'impact de ces fausses accusations.

Mots clés : réseaux pair-à-pair, eDonkey, l'attaque Eclipse, détection d'attaques dans les réseaux P2P.

Abstract

In this work, we analyzed the Eclipse attack in an eDonkey network. In an Eclipse attack, attacker goal is to keep the supervised part hidden from the rest of the network using the list of servers in eDonkey network as a target. Two different scenarios of Eclipse attack are identified. The first one treats the case where there is only one attacker mount an Eclipse attack on an eDonkey network. The second scenario treats the case of several attackers. To prevent from this attack, we propose solution based on lists of servers size of detector's client. The obtained result shows the efficiency of our solution to detect the two scenarios of Eclipse attack and avoid (isolate) those attackers from the rest of the network. However, false positive can happened. We proposed to use a profiling of the users, TCP and UDP ports to mitigate false positive affect.

Keywords : Peer To Peer Networks, eDonkey Network , Eclipse attacks, attacks detection in P2P networks .

Dédicaces

*Je dédie ce travail à ma très chère mère ,
A mon adorable père,
A mes très chères sœurs et frères ,
A toute ma famille,
A tous ceux que je ne cite pas mais aux quels je pense très fort,
vous mes amis(es)*

Remerciements

Je remercie Dieu le tout Puissant qui m'a donné la force et la volonté pour réaliser ce modeste travail.

Mes remerciements iront à mes encadreurs Abdelmadjid BOUABDALLAH, Professeur à l'UTC (Compiègne, France) et Hani Ragab Hassen, Docteur à l'UTC (Compiègne, France) pour m'avoir soutenu durant cette année de Magister. Ce travail n'aurait jamais pu aboutir sans eux, qui sont toujours su me consacrer des moments de leurs temps, me guider et me conseiller. Je souhaite leur transmettre l'expression de ma reconnaissance et ma plus profonde gratitude.

Je remercie tout particulièrement les membres de jury, qui ont accepté de juger mon travail.

Je tiens aussi à remercier chaleureusement Kamel TARI, le Chef de département d'informatique et responsable de l'école doctorale, qui nous a toujours encouragé et soutenu, et je tiens aussi à remercier Monsieur Djoudi TOUAZI responsable du centre de calcul pour son aide et sa gentillesse avec tous le monde.

Mes sincères remerciements à tous nos enseignants et tous ceux qui ont contribué à la création et la réussite de l'école doctorale ReSyD de Bejaia.

Je remercie également mes amis et collègues de l'école doctorale de Béjaïa pour avoir créé un environnement d'études convivial durant toute cette formation.

Je ne pourrais clôturer ces remerciements sans me retourner vers ma raison d'être qui ont toujours été à mes côtés et qui m'ont entourée d'affection, de soutien et d'amour, ma très chère mère et mon adorable père. Qu'ils trouvent dans ce modeste travail le fruit de leur soutien.

Je voudrais aussi remercier profondément mes frères et sœurs, ainsi que toute ma famille.

Enfin je remercie tous ceux qui, de près ou de loin, ont contribué à l'aboutissement de ce travail.

Table des matières

Table des matières

Liste des figures	iv
Liste des tableaux	v
Introduction générale	1
1 Les réseaux pair-à-pair	4
1.1 Introduction	4
1.2 Modèle P2P	4
1.2.1 Taxonomie des systèmes informatiques	5
1.2.2 Taxonomie des systèmes Pair-à-Pair	5
1.2.3 Quelques caractéristiques d'un réseau Pair-à-Pair	5
1.2.4 Les applications Pair-à-Pair	6
1.2.5 Objectif du modèle P2P	7
1.2.6 P2P vs Client/Server	8
1.2.7 Quelques avantages des réseaux P2P	9
1.2.8 Quelques inconvénients des réseaux P2P	9
1.3 Les différentes architectures des réseaux peer to peer	10
1.3.1 Architecture centralisée	10
1.3.2 Architecture Distribuée (Pur P2P)	10
1.3.3 Architecture Superpeers (Hybrid P2P)	11
1.4 Etude des mécanismes de base de fonctionnement des réseaux P2P	13
1.4.1 Méthodes de recherche dans les réseaux P2P non-structurés	13
1.4.2 Les réseaux à index	14
1.4.3 Les réseaux à " traînée "	14
1.4.4 Réseaux à tables de hashage Distribuées (DHT)	15
1.5 Conclusion	16
2 Le réseau eMule/eDonkey et le protocole BitTorrent	17
2.1 Introduction	17
2.2 eMule/eDonkey	17
2.2.1 Fonctionnement du réseau	17
2.2.2 Le serveur eMule	19
2.2.3 Connexion Client/ Serveur	19
2.2.4 Connexion Client/ Client	20

2.2.5	Liste des serveurs eDonkey	22
2.3	BitTorrent	22
2.3.1	Présentation	22
2.3.2	Principe de fonctionnement	23
2.4	Comparaison de BitTorrent avec eDonkey	24
2.5	Conclusion	25
3	Sécurité dans les réseaux P2P	26
3.1	Introduction	26
3.2	Sécurité informatique	26
3.2.1	Sécurité proactive	27
3.2.2	Sécurité réactive	28
3.2.3	Sécurité dans les systèmes actuels	28
3.3	Quelques propriétés de la sécurité informatique	29
3.3.1	Confidentialité	29
3.3.2	Intégrité	30
3.3.3	Disponibilité	30
3.4	Quelques fonctions de la sécurité informatique	30
3.5	Quelques algorithmes de chiffrement et mécanismes de sécurité	32
3.5.1	Cryptographie symétrique	32
3.5.2	Cryptographie asymétrique	32
3.5.3	Fonctions de hachage	33
3.5.4	Signature numérique	33
3.5.5	Infrastructures de confiance	33
3.5.6	Autorités de confiance	34
3.6	Conclusion	35
4	Quelques attaques sur les réseaux P2P et leurs contre-mesures	36
4.1	Introduction	36
4.2	l'attaque Sybil	36
4.2.1	Principe et conséquence	36
4.2.2	Défense	37
4.3	l'attaque Eclipse	38
4.3.1	Principe et conséquence	38
4.3.2	Défense	38
4.4	l'attaque déni de service (DoS) et Distributed DoS dans les réseaux P2P . . .	39
4.4.1	Principe et conséquence	39
4.4.2	Défense	40
4.5	l'attaque Man In The Middle	40
4.5.1	Principe et conséquence	40
4.5.2	Défense	41
4.6	l'attaque Rational	42
4.6.1	Principe et conséquence	42
4.6.2	Défense	42
4.7	Empoisonnement et pollution (Poisoning and pollution attacks)	43
4.7.1	Principe et conséquence	43
4.7.2	Défense	44
4.8	les Vers dans les réseaux P2P	44

4.8.1	Principe et conséquence	44
4.8.2	Défense	45
4.9	Conclusion	46
5	La détection d'attaques dans les réseaux P2P	47
5.1	Introduction	47
5.2	Quelques techniques de détection des attaques sur les réseaux P2P	47
5.2.1	La réputation	48
5.2.2	Agents mobiles	48
5.2.2.1	Détection multi-point	49
5.2.2.2	Architecture résistante aux attaques	49
5.2.2.3	Agents errants	49
5.2.2.4	Imprévisibilité	49
5.2.2.5	Diversité génétique	50
5.2.3	Profilage (profiling)	50
5.2.3.1	Profilage des utilisateurs	50
5.2.3.2	Profilage de groupes	51
5.2.3.3	Profilage d'utilisateurs de ressources	51
5.2.4	Observation de seuil	51
5.3	Quelques approches pour la détection d'intrusions sur les réseaux P2P	52
5.3.1	Approche par scénario	52
5.3.2	Approche comportementale	52
5.3.2.1	Inconvénient	52
5.3.3	Comparaison des deux approches	53
5.3.4	Systèmes hybrides	53
5.4	Quelques systèmes existants de détection d'intrusions sur les réseaux P2P	54
5.4.1	EMERALD	54
5.4.2	AAFID	54
5.4.3	GrIDS	55
5.4.4	MAIDS	55
5.4.5	INDRA	55
5.4.6	NetBiotic et Trust-Aware	55
5.4.7	SNORT	56
5.4.8	MAPIDS	56
5.5	Conclusion	57
6	Un algorithme de détection de l'attaque Eclipse sur le réseau eDonkey	58
6.1	Introduction	58
6.2	Protocole de communication dans un réseau eDonkey	58
6.3	Scénarios de l'attaque Eclipse sur le réseau eDonkey	60
6.3.1	Attaque menée par un seul serveur	60
6.3.2	Attaque menée par plusieurs serveurs	62
6.4	Proposition d'un algorithme de détection de l'attaque Eclipse sur le réseau eDonkey	63
6.4.1	Ports TCP et UDP ouvert (test 1)	63
6.4.2	Des réponses négatives aux requêtes de recherche (message Not_Found) test 2	63

6.4.3	Découverte des serveurs et utilisation d'une liste de serveurs attaquants (test 3)	64
6.4.4	Déclenchement d'alerte	67
6.4.5	Discussion et résultats	67
6.4.5.1	Cas $A=B$	67
6.4.5.2	Cas $A = 1$ et $B > 1$	68
6.4.5.3	Cas $B > A$	69
6.4.6	Exemple de fausse alerte	70
6.5	Conclusion	71
Conclusion et Perspectives		72
Liste des Abbreviations		74
ANNEXE		75
Bibliographie		79