République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaïa

Faculté des Sciences et des Sciences de l'Ingénieur

Département d'Informatique

Ecole Doctorale Rséeaux et Systèmes Distribués

Mémoire de Magistère

En Informatique

Option

Réseaux et Systèmes Distribués

Thème

Sécurité de Routage

Présenté par

Abdelaziz BABAKHOUYA

Devant le jury composé de :

Pr M. Ahmed Nacer	**Président**	**USTHB, Alger, Algérie**
Pr N. Badache	**Examinateur**	**USTHB, Alger, Algérie**
MC F. Naït Abdesselam	**Examinateur**	**USTL, Lille, France**
Pr A. Bouabdallah	**Directeur de Thèse**	**UTC, Compiègne, France**
Dr Y. Challal	**Invité**	**UTC, Compiègne, France**

Promotion 2004 – 2005

Résumé

Les protocoles de routage assurent la connectivité du réseau et maintiennent des routes afin que les données envoyées par une source puissent atteindre leurs destinations. Les protocoles de routage utilisés actuellement dans l'Internet, comme BGP, OSPF et RIP sont conçus pour opérer dans un environnement sain sans routeurs malicieux. Cependant, avec la croissance importante de l'Internet, un nombre important d'entreprises et services publics sont devenus dépendants de bon fonctionnement de ces protocoles. De ce fait, la sécurisation des protocoles de routage revêt d'une importance primordiale.
Nous présentons dans ce mémoire une étude sur la sécurité des protocoles de routage. A partir de cette étude, nous avons constaté la difficulté de sécuriser ces protocoles sans compromettre leurs performances et leur efficacité. Même la simple introduction de mécanismes cryptographiques ne peut pas palier à toutes les attaques possibles sur ces protocoles. Pour cela, nous avons proposé une nouvelle approche appelée S-DV "*Secure Distance Vector Routing Protocols*" permettant de sécuriser les protocoles de routage à base de vecteur de distance. En effet, S-DV favorise le choix d'un chemin plus sûr par rapport à un chemin plus court qui a été sujet à des attaques fréquentes. Ceci est rendu possible via une métrique qui mesure le niveau de sécurité associé à un chemin qui passe par un routeur voisin. Nous avons également proposé un nouveau mécanisme appelé DR "*Distance Request, Distance Reply*" permettant de vérifier la cohérence d'une annonce de route envoyée par un routeur voisin. Notre analyse montre l'efficacité de notre approche à détecter tout type d'annonce mensongère avec un coût très réduit.

Mots-clés : Sécurité, Routage, Authentification, Contrôle de Cohérence.

Abstract

Routing protocols ensure the network connectivity, they maintain routes so that the data sent by a source can reach their destinations. Routing protocols used actually in the Internet, like BGP, OSPF and RIP were designed to operate in a safe environment without malicious routers. Although, with the importance growth of the Internet, a significant number of companies and public services became dependent on its correct operation. So that, securing routing protocols becomes of critical importance.
In this report we review routing protocols security. From this study, we conclude that it is very difficult to secure such routing protocols without compromising their performance and efficiency. The simple introduction of cryptographical mechanisms cannot prevent from all the possible attacks on these protocols. For this reason, we proposed a new approach called S-DV "Secure Distance Vector Routing Protocols". S-DV prefers the choice of a secure route than a shortest one which was subject to frequent attacks. This became possible with new metrics that measure the security level associated to a route that passes through a neighbor routers. We proposed also a new mechanism called DR "Distance Request, Distance Reply" to check the coherence of an advertised route received from a neighbor router. Our analysis shows the efficiency of our approach to detect all types of misbehaving advertisements with alow cost.

Keywords : Security, Routing, Authentification, Coherence Check.

Table des matières