جامعة ابن زهر
ⵜⴰⵙⴷⴰⵡⵉⵜ ⵉⴱⵏ ⵣⵀⵔ
UNIVERSITÉ IBN ZOHR

UNIVERSITE IBN ZOHR

FACULTE DES SCIENCES

Licence d'Excellence

Filière Analytique de Données et Intelligence Artificielle

Recherche sur

ARP

et

Usurpation d'identité

Professeur : M. Abdellah BOULOUZ

Réalisé par : Badr-Eddine Hrimech

Année universitaire 2023-2024

Introduction 2
Défauts d'ARP 3
Contre-mesures et Solutions 3
I. **Les approches cryptographiques** 3
S-ARP par Mohamed G. Gouda et Chin-Tser Huang 3
S-ARP : Un Protocole de Résolution d'Adresses Sécurisé par D. Bruschi, A. Ornaghi, E. Rosti 5
L'Authentification ARP (ARP-A) par Osama S. Younes 7
II. **Les approches non cryptographiques** 9
Approche logicielle 9
Approche matérielle 9
Entrées ARP statiques 9
Segmentation et isolation du réseau 9
Conclusion 10
Références 10

Introduction

Une adresse de contrôle d'accès au support (MAC) sert d'identifiant distinctif et inhérent attribué à chaque contrôleur d'interface réseau (NIC) dans un réseau informatique. Cette adresse joue un rôle crucial en identifiant de manière unique les appareils sur le réseau. L'adresse MAC est divisée en deux moitiés, la première moitié étant appelée l'Identifiant Unique Organisationnel (OUI). Cet OUI est attribué par l'Institut des ingénieurs en électricité et électronique (IEEE) au fabricant du NIC, servant d'identification distincte pour ce fabricant spécifique. La deuxième moitié de l'adresse MAC est désignée par le fabricant, garantissant que chaque NIC possède un identifiant unique à l'échelle mondiale afin que deux NIC n'aient pas la même adresse MAC.

Le protocole de résolution d'adresse (ARP) complète le rôle de l'adresse MAC en facilitant l'association entre l'adresse IP au niveau du réseau et l'adresse MAC au niveau de la couche liaison de données. Ce protocole devient essentiel dans les environnements de réseau local (LAN) où les appareils doivent faire correspondre les adresses logiques à leurs adresses physiques correspondantes. ARP fonctionne grâce à un mécanisme de diffusion, où une demande de message en diffusion est envoyée à travers le réseau pour déterminer l'adresse MAC associée à une adresse IP spécifique. Chaque appareil dans le réseau compare le message diffusé avec sa propre adresse IP. En cas de correspondance, une réponse ARP unicast est générée et envoyée. Les appareils qui ne correspondent pas à l'adresse IP diffusée rejettent le paquet. Les mappages résultants d'adresses IP-MAC sont ensuite stockés dans une table de cache ARP, facilitant des transmissions de données futures efficaces et rapides dans le réseau.

Défauts d’ARP

ARP a été conçu sans fonctionnalités de sécurité, de sorte qu'ARP n'inclut pas de mécanismes d'authentification ou garantissant l'intégrité des informations qu'il fournit. Cela signifie que les informations échangées via ARP ne sont pas vérifiées et qu'il n'existe aucun moyen intégré de confirmer la légitimité des réponses ARP et peuvent donc être facilement usurpées. Par conséquent, ARP est très sensible aux attaques d’usurpation d’identité et de poison.

Le "spoofing" ARP est une forme d'attaque informatique où un intrus envoie des messages "spoofed" trompeurs du Protocole de Résolution d'Adresses (ARP), sous la forme de demandes ou de réponses, à travers un réseau local (LAN). Ces messages falsifiés trompent les appareils du réseau en associant l'adresse MAC de l'attaquant à l'adresse IP d'un ordinateur ou d'un serveur ciblé. Par conséquent, le trafic réseau destiné à l'adresse IP de la victime est redirigé vers l'attaquant, permettant une interception ou une modification non autorisée des communications. Cette forme d'attaque est particulièrement préoccupante pour les LAN et est souvent une menace préalable à diverses autres activités malveillantes.

Le "poisoning" ARP, une catégorie plus large, implique la manipulation des tables ARP pour compromettre l'intégrité du réseau. Cela inclut le "spoofing" ARP, où l'attaquant envoie des messages ARP malveillants pour contaminer les caches ARP d'autres appareils. Cette contamination amène les appareils légitimes à lier l'adresse MAC de l'attaquant à une adresse IP valide, facilitant ainsi l'accès non autorisé. Le "poisoning" ARP peut se manifester de différentes manières, comme inonder le réseau de demandes ou de réponses ARP trompeuses, causant de la confusion et perturbant les opérations normales du réseau. En plus de permettre des attaques de type "man-in-the-middle" (MITM), les techniques de "poisoning" ARP peuvent être utilisées pour des attaques de déni de service (DoS), de saturation MAC, et d’autres.

Par exemple, dans une attaque de déni de service, un attaquant inonde le réseau de demandes ARP, submergeant les appareils et provoquant des perturbations de service. Dans une attaque "man-in-the-middle", l'attaquant intercepte et potentiellement altère la communication entre deux parties. La saturation MAC implique l'envoi d'une inondation de trames pour saturer les tables MAC des commutateurs, entraînant un débordement et une possible panne du réseau.

Contre-mesures et Solutions

Au fil des années, de nombreux chercheurs ont proposé diverses solutions, et nous en soulignerons quelques-unes. Ces solutions se répartissent en deux catégories principales : les approches cryptographiques et les approches non cryptographiques.

I. Les approches cryptographiques

Dans ce contexte, les solutions cryptographiques se concentrent généralement sur le renforcement de la sécurité ARP grâce à des améliorations du schéma d'authentification ou d'intégrité.

S-ARP par Mohamed G. Gouda et Chin-Tser Huang

L'architecture S-ARP (Protocole de Résolution d'Adresse Sécurisé), développée par Mohamed G. Gouda et Chin-Tser Huang, propose une solution robuste pour renforcer la sécurité de l'ARP dans un

environnement Ethernet. Cette architecture novatrice intègre un serveur sécurisé connecté à l'Ethernet, ainsi que deux protocoles essentiels : le protocole d'invitation–acceptation et le protocole de demande–réponse.

Essentiellement, le cadre S-ARP aborde les vulnérabilités potentielles de la communication ARP en introduisant un serveur sécurisé dédié à l'Ethernet. La communication au sein de l'architecture S-ARP se produit soit du serveur sécurisé à un ordinateur spécifique dans l'Ethernet, soit vice versa. Cette communication est facilitée par l'utilisation de deux sous-protocoles, à savoir le protocole d'invitation–acceptation et le protocole de demande–réponse.

Pour approfondir, **le protocole d'invitation–acceptation** sert de mécanisme de communication sécurisée entre différents ordinateurs dans l'Ethernet et le serveur sécurisé. Sa fonction principale est de permettre la transmission périodique et sécurisée des adresses IP et des adresses matérielles de chaque ordinateur au serveur sécurisé. Cela garantit que le serveur sécurisé maintient une base de données à jour contenant les associations cruciales d'adresses IP et matérielles pour tous les dispositifs connectés.

Le protocole d'invitation–acceptation joue un rôle crucial dans la promotion d'une communication sécurisée entre divers ordinateurs au sein de l'Ethernet. Sa fonction principale est de permettre aux ordinateurs de transmettre périodiquement et en toute sécurité leurs adresses IP et les adresses matérielles correspondantes au serveur sécurisé. Cela garantit que le serveur sécurisé maintient une base de données à jour et précise des associations d'adresses IP et matérielles pour tous les dispositifs connectés.

D'autre part, **le protocole de demande–réponse** sert à permettre à chaque ordinateur dans l'Ethernet de résoudre l'adresse matérielle associée à une adresse IP spécifique. Ce protocole est essentiel pour améliorer l'efficacité et la sécurité des processus de résolution d'adresses au sein du réseau.

Cette architecture suppose qu'un attaquant peut effectuer les trois types d'actions suivants pour perturber les communications entre le serveur et n'importe quel ordinateur sur l'Ethernet :

- ***Perte de message :***

Après l'envoi d'un message (par un processus dans s ou A), le message est rejeté par l'adversaire et n'est jamais reçu (par le processus prévu dans A ou s, respectivement).

- ***Modification de message :***

Après l'envoi d'un message et avant sa réception, les champs du message sont arbitrairement modifiés par l'adversaire.

- ***Replay de message :***

Après l'envoi d'un message et avant sa réception, le message est remplacé par une copie d'un message antérieur du même type par l'adversaire.

Notez qu'en exécutant une séquence de ces actions adverses, l'attaquant peut lancer des attaques de redirection de messages ou des attaques d'induction de transmission.

Pour contrer ces actions adverses, l'architecture S-ARP utilise :

- ***Délais d'attente pour contrer la perte de messages :***

Dans le cas où un serveur ou une machine envoie un message mais ne reçoit pas de réponse dans un délai prédéfini, le processus expire et envoie une autre copie du même message.

- ***Secrets partagés pour contrer la modification de messages :***

Chaque ordinateur 'A' sur l'Ethernet partage un secret unique (scr[i]) avec le serveur 's'. Ce secret est utilisé pour calculer une vérification d'intégrité ajoutée à chaque message envoyé entre 's' et 'A'.

Par exemple, si un message "acpt(c, ip, hd)" doit être envoyé entre 'S' et 'A', une vérification d'intégrité 'd' est calculée avec une fonction de hachage comme MD5 ou SHA et la clé secrète comme d = MD(c; ip; hd; scr[i]). Cette vérification est ajoutée au message, renforçant sa sécurité. "acpt(c, ip, hd, d)"

Si un attaquant modifie arbitrairement l'un des champs du message, le destinataire peut le détecter car la vérification d'intégrité calculée (d) ne correspondra pas à celle calculée à l'extrémité du destinataire (d').

- ***Nombres pour contrer le replay de messages :***

Les nonces sont des entiers aléatoires et uniques générés par l'émetteur (serveur ou machine) et attachés aux messages avant la transmission.

Lorsque le destinataire envoie une réponse, il inclut le nonce dans le message de réponse.

L'émetteur peut vérifier si le nonce dans la réponse est égal au nonce original, concluant que ni le message original ni la réponse n'ont été modifiés par l'attaquant.

S-ARP : Un Protocole de Résolution d'Adresses Sécurisé par D. Bruschi, A. Ornaghi, E. Rosti

Cette méthode introduit une couche de sécurité robuste dans ARP en incorporant un mécanisme de paires de clés publique/privée pour chaque hôte, certifié par une Autorité de Certification de confiance locale sur le LAN. Cette approche implique la signature numérique des messages à l'extrémité de l'expéditeur, assurant la prévention de l'injection d'informations usurpées.

S-ARP est conçu comme une extension d'ARP, maintenant la compatibilité en respectant les spécifications originales d'ARP pour l'échange de messages, les temporisations et le cache. Pour assurer l'interopérabilité, un en-tête supplémentaire est ajouté aux messages ARP standard, transportant des informations d'authentification. Cela permet aux hôtes ne mettant pas en œuvre S-ARP de traiter ces messages, bien que dans un LAN ARP sécurisé, les auteurs recommandent que tous les hôtes exécutent S-ARP.

Les hôtes activés pour S-ARP respectent une politique stricte, n'acceptant que des messages authentifiés, sauf si l'expéditeur est répertorié comme un hôte connu qui n'exécute pas S-ARP. Cette liste d'hôtes non-S-ARP est essentielle pour les hôtes sécurisés qui souhaitent communiquer avec des hôtes non

sécurisés. En revanche, les hôtes fonctionnant avec le protocole ARP classique peuvent accepter des messages authentifiés.

Comment ça marche : Protocole S-ARP en action

Identification de l'AKD et Distribution des Clés : Au début de la configuration, l'Autorité Distributrice de Clés (AKD) est identifiée, et sa clé publique ainsi que son adresse MAC sont distribuées à tous les hôtes de manière sécurisée. En parallèle, chaque hôte activé pour S-ARP est distinctement identifié par son adresse IP et équipé d'une paire de clés publique/privée pour une communication sécurisée. Cette approche en deux couches établit un cadre de confiance fondamental.

Connexion de l'Hôte au LAN et Soumission du Certificat à l'AKD : Lorsqu'un hôte rejoint le LAN, il génère une paire de clés publique/privée. Par la suite, l'hôte transmet son certificat signé, encapsulant la clé publique et l'adresse IP, à l'AKD. Agissant comme un référentiel de clés de confiance, l'AKD vérifie ces certificats, assurant l'exactitude des informations. Simultanément, la clé publique et l'adresse IP de l'hôte sont intégrées à la base de données locale du référentiel AKD. Les auteurs mentionnent l'utilisation de l'Algorithme de Signature Numérique (DSA) pour les signatures numériques, en raison de son efficacité avec une clé de 512 bits, tout en reconnaissant qu'il n'est pas entièrement sécurisé.

Processus de Changement de Clé : Si un hôte souhaite modifier sa clé, il transmet la nouvelle clé à l'AKD, signant la demande avec l'ancienne clé. Ce processus garantit une transition fluide des clés, l'AKD mettant à jour son infrastructure de clés tout en préservant les associations nécessaires.

Attribution Dynamique des Adresses IP : Dans les scénarios avec des attributions dynamiques d'adresses IP facilitées par DHCP, l'association dynamique des clés se produit, renouvelée à chaque attribution d'une nouvelle adresse IP à un hôte. Cette attribution dynamique des clés est orchestrée par un serveur S-DHCP personnalisé, favorisant la communication entre le serveur DHCP et le serveur S-ARP pour s'adapter au paysage réseau en constante évolution.

Synchronisation de l'Horloge Après la Connexion : Après la connexion, chaque hôte synchronise son horloge locale S-ARP avec la référence temporelle reçue de l'AKD. Cette synchronisation fournit non seulement un contexte temporel partagé, mais sert également de mesure préventive contre les attaques de rejeu.

Processus d'Authentification des Messages :

- ***Anneau de Clés Publiques :***

Chaque hôte maintient un anneau de clés publiques, abritant les clés publiques et leurs adresses IP correspondantes provenant de l'AKD.

- ***Gestion des Réponses S-ARP :***

À la réception d'une réponse S-ARP, l'hôte examine son anneau de clés publiques pour l'IP de l'expéditeur et la clé publique correspondante. Une identification réussie conduit à la vérification de la signature numérique, tandis que les entités non reconnues incitent l'hôte à demander le certificat nécessaire à l'AKD.

- ***Demande de Certificat à l'AKD :***

L'AKD répond avec une réponse signée, fournissant la clé publique demandée et l'horodatage actuel. À la réception, l'hôte subit un processus complet : resynchronisation de l'horloge, stockage de la clé acquise et vérification de la signature de la réponse à l'aide de la clé nouvellement acquise.

Gestion des Changements de Clé : Si l'ancienne clé dans l'anneau local devient obsolète, l'hôte vérifie la nouvelle clé reçue de l'AKD avec la clé mise en cache. Toute divergence entraîne le rejet de la réponse pour prévenir une utilisation non autorisée. À l'inverse, une correspondance incite la mise à jour du cache, assurant une transition fluide.

Considérations sur l'Horodatage :

- ***Horodatage dans la Réponse S-ARP :***

Chaque réponse S-ARP encapsule un horodatage, indiquant l'heure locale de l'expéditeur.

- ***Rejet des Anciennes Réponses :***

Les réponses portant des horodatages obsolètes sont promptement rejetées, servant de mesure protectrice contre les attaques de rejeu.

- ***Différence de Temps Acceptable :***

Les hôtes intègrent une différence de temps acceptable, généralement autour de 30 secondes, entre l'horodatage et leur horloge locale. Cette approche adaptative prend en compte les variations temporelles du réseau et renforce la sécurité.

- ***Prévention des Attaques de Rejeu :***

La différence de temps acceptable agit comme une fenêtre temporelle, rendant les réponses obsolètes invalides. Cette mesure proactive protège contre les attaques de rejeu, où les attaquants tentent de réutiliser des réponses S-ARP précédemment interceptées et valides.

L'Authentification ARP (ARP-A) par Osama S. Younes

Osama S. Younes présente une approche novatrice pour contrer les attaques de détournement ARP, abordant les limitations observées dans les techniques existantes qui souvent ne parviennent pas à protéger contre l'usurpation d'identité des hôtes et les attaques par déni de service (DoS). Younes se concentre sur plusieurs défis clés et propose une solution complète qui renforce la sécurité du Protocole de Résolution d'Adresses (ARP) dans un environnement réseau.

Les objectifs principaux d'ARP-A comprennent l'assurance de l'intégrité des messages ARP, la mise en place d'une authentification robuste pour les entités et les messages ARP, la transformation d'ARP

d'un protocole sans état à un protocole étatique pour une adaptabilité dynamique, la réduction des risques liés à un point de défaillance unique, le maintien de la simplicité et de la compatibilité avec les protocoles ARP standards, la minimisation des coûts de calcul pour l'efficacité, et l'assurance de la scalabilité pour répondre aux demandes évolutives des infrastructures réseau.

ARP-A se compose de deux schémas : le schéma d'Authentification Centralisée ARP (ARP-CA) et le schéma d'Authentification Décentralisée ARP (ARP-DA).

Le schéma **ARP-CA** fonctionne comme un protocole client/serveur, exploitant un serveur central appelé serveur ARP-A situé sur le réseau local (LAN) pour effectuer des authentifications pour les clients et les messages ARP. Ce serveur stocke et maintient les paires IP/MAC pour tous les clients dans une base de données locale.

Lorsqu'un nouvel hôte intègre le réseau et obtient son adresse IP du serveur DHCP ou utilise une adresse IP statique, il interagit rapidement avec le serveur ARP-A pour enregistrer sa paire IP/MAC. Le serveur examine le message d'enregistrement et, après vérification, envoie un accusé de réception sous la forme d'un message de Ticket, accompagné d'un ticket encodé. Ce ticket sert à authentifier les associations IP-MAC en cas de défaillance du serveur. Simultanément, le serveur diffuse un message de mise à jour à tous les clients, les incitant à actualiser leurs caches ARP avec la dernière entrée. Le ticket et le message de mise à jour sont encodés à l'aide de la clé privée du serveur pour renforcer la sécurité.

Lorsqu'un hôte, désigné comme A, souhaite communiquer avec un autre hôte, B, il envoie un message ARP-A Request unicast au serveur, encodé avec la clé de sécurité du client. Après réception du message ARP-A Request, le serveur effectue un processus de vérification méticuleux, recherchant dans sa base de données locale la paire IP/MAC de l'hôte B. Ensuite, le serveur encode la paire IP/MAC identifiée dans un message de Reply et le transmet à l'hôte A. L'hôte A, après vérification, met à jour son cache ARP avec les informations contenues dans le message de Reply valide. La communication entre les hôtes et le serveur est protégée par l'application de la cryptographie symétrique, garantissant un échange sécurisé d'informations.

En cas de défaillance du serveur, le schéma ARP-CA se désactive élégamment, laissant place au schéma ARP-DA.

ARP-DA, un protocole pair-à-pair, authentifie de manière experte les messages ARP Request et Reply, assurant la continuité de la communication sécurisée en l'absence du serveur central. Dans un scénario ARP-DA, lorsqu'un client, A, tente de communiquer avec un autre client, B, il diffuse un message ARP-DA Request accompagné de son ticket préalablement obtenu auprès du serveur à tous les clients. À la réception du message ARP-DA Request, le client B, ainsi que d'autres clients, vérifient rigoureusement le ticket et l'authenticité du message. Après vérification réussie, le client B transmet le ARP Reply, accompagné de son propre ticket, à l'hôte A. Le ticket du client, contenant le mappage des adresses IP/MAC et signé par le serveur, sert de mécanisme robuste de validation de l'identité de l'expéditeur et du mappage des adresses IP/MAC associées.

II. Les approches non cryptographiques

Ces approches se concentrent principalement sur le développement de méthodes permettant de détecter et/ou de prévenir les menaces de sécurité ARP sans recourir fortement à des mesures cryptographiques.

Approche logicielle

Les outils de détection comme ARP Watch et ARP Guard... sont utilisés pour surveiller les activités ARP sur Ethernet et vérifier ces activités par rapport à une base de données de couplages (adresse IP, adresse matérielle). Ainsi, si un couplage est modifié ou ajouté, un e-mail est envoyé pour alerter. l'administrateur du réseau. Cependant, ces outils servent uniquement à détecter les attaques ARP, plutôt qu'à les atténuer.

Approche matérielle

Les solutions "Hardware" pour la sécurité ARP fournissent une couche de protection supplémentaire au niveau matériel et impliquent souvent la mise en œuvre de fonctionnalités fournies par les commutateurs réseau, telles que l'inspection dynamique ARP (DAI) et la surveillance DHCP... **L'inspection dynamique ARP (DAI)** fonctionne en inspectant les paquets ARP au sein du réseau et en validant le mappage entre les adresses IP et les adresses MAC. Il maintient une base de données fiable de liaisons d'adresses IP à MAC légitimes et, lorsqu'il détecte des incohérences ou des paquets ARP non autorisés, il peut prendre des actions prédéfinies, telles que l'abandon ou la journalisation du trafic suspect. De même, **la surveillance DHCP "Snooping"** examine le processus DHCP, où elle surveille et vérifie les messages DHCP échangés entre les clients et les serveurs. En gardant une trace des attributions d'adresses IP valides, la surveillance DHCP aide à prévenir les serveurs DHCP malveillants et atténue les vulnérabilités potentielles liées à l'ARP. **L'activation de la sécurité des ports sur un commutateur** est également utile en agissant comme un contrôleur d'accès, permettant aux administrateurs de spécifier quels appareils sont autorisés à se connecter à des ports de commutateur spécifiques en fonction de leurs adresses MAC, empêchant ainsi tout accès non autorisé.

Entrées ARP statiques

Une autre mesure préventive robuste contre l'usurpation d'identité ARP consiste à stocker et à **configurer des entrées statiques permanentes** pour les hôtes de confiance dans les caches ARP de tous les ordinateurs. Ce faisant, la transmission des messages ARP sur Ethernet est éliminée, empêchant les attaquants de modifier le cache ARP et contrecarrant efficacement les tentatives d'usurpation d'identité ARP. Bien que cette solution soit très efficace, elle pose des problèmes dans les réseaux vastes et dynamiques, car elle peut entraîner une complexité et des frais administratifs accrus.

Segmentation et isolation du réseau

Lorsqu'un réseau est bien segmenté, l'impact d'une attaque par empoisonnement du cache ARP est limité à un sous-réseau spécifique, empêchant son accès aux appareils d'autres sous-réseaux. Ce confinement est obtenu car les messages ARP sont limités au sous-réseau local et ne traversent pas au-delà.

Conclusion

Le protocole de résolution d'adresse, en tant que composant essentiel des réseaux locaux, nécessite une protection solide, car il opère en tant que protocole sans état dépourvu de mécanismes de sécurité intégrés. Les solutions cryptographiques mises en avant dans cette présentation, telles que ARP-A, redéfinissent le paysage en incorporant des contrôles d'intégrité, des mécanismes d'authentification et une adaptabilité dynamique. L'utilisation de clés asymétriques, de signatures numériques et de synchronisation temporelle sécurisée renforce la défense contre les attaques d'usurpation d'identité, élevant ainsi la sécurité ARP à de meilleurs niveaux. D'un autre côté, les solutions non cryptographiques apportent une dimension pratique à la stratégie de défense. Les commutateurs d'inspection ARP dynamique et la surveillance DHCP apparaissent comme une excellente couche de protection supplémentaire centrée sur le matériel, surveillant et authentifiant le trafic ARP en temps réel. La mise en place d'entrées ARP statiques sert de rempart, prévenant toute altération non autorisée des caches ARP et contrant les risques potentiels d'empoisonnement du cache. Chaque nouvelle publication de recherche s'appuie sur des travaux antérieurs avec une approche légèrement différente, cherchant à renforcer la sécurité, à améliorer le rapport coût-sécurité/performance, tout en comblant les lacunes des solutions précédemment proposées.

Références

- *Gouda, M. G., & Huang, C.-T. (2003). A secure address resolution protocol. Computer Networks, 41(1), 57–71. doi:10.1016/s1389-1286(02)00326-2*

10.1016/s1389-1286(02)00326-2

- *Bruschi, D., Ornaghi, A., & Rosti, E. (n.d.). S-ARP: a secure address resolution protocol. 19th Annual Computer Security Applications Conference, 2003. Proceedings. doi:10.1109/csac.2003.1254311*

10.1109/csac.2003.1254311

- *Younes, O. S. (2017). Modeling and performance analysis of a new secure address resolution protocol. International Journal of Communication Systems, 31(1), e3433. doi:10.1002/dac.3433*

10.1002/dac.3433