УДК 004.7

К. О. Паламарчук
О. В. Войцеховська

ДОДАВАННЯ ЦИФРОВОГО ПІДПИСУ ДО ПРОТОКОЛУ ARP ДЛЯ ЗАПОБІГАННЯ ARP-SPOOFING

Вінницький національний технічний університет

Анотація

У роботі проведено дослідження використання цифрового підпису як засобу захисту протоколу ARP від атак типу ARP-spoofing. Запропоновано модифікацію обміну ARP-повідомленнями шляхом додавання криптографічного підпису, що забезпечує автентичність джерела та цілісність переданих даних, а також передбачає оптимізацію процесу підписування шляхом використання симетричних алгоритмів, що зменшує обчислювальні витрати. Проведено оцінювання впливу підпису на продуктивність мережевої взаємодії та визначено доцільність запропонованого підходу у запобіганні підробці ARP-відповідей.

***Ключові слова**: Address Resolution Protocol, захист локальних мереж, ARP-спуфінг, цифровий підпис.*

Abstract

This paper investigates the use of a digital signature as a means of protecting the ARP protocol from ARP-spoofing attacks. A modification of the ARP message exchange is proposed by adding a cryptographic signature that ensures the authenticity of the source and the integrity of the transmitted data, while also providing an optimization of the signing process through the use of symmetric algorithms, which reduces computational overhead. An assessment of the impact of the signature on network performance was conducted, and the feasibility of the proposed approach in preventing forged ARP replies was determined.

***Keywords**: Address Resolution Protocol, local network security, ARP-spoofing, digital signature.*

Вступ

У сучасних локальних мережах питання забезпечення надійної та безпечної передачі даних набуває особливої важливості, оскільки зростання кількості взаємодіючих пристроїв підвищує ризики несанкціонованого втручання. Безпека мережевих протоколів – це основа стабільної роботи інфраструктури, а їхні вразливості можуть призвести до суттєвих порушень конфіденційності та втрати важливих даних.

Одним із базових компонентів локальних комп’ютерних мереж є протокол Address Resolution Protocol (ARP), основне призначення якого полягає у встановленні відповідності між IP-адресою та MAC-адресою вузла в межах однієї мережі. Отримана інформація зберігається у кеші ARP, що дозволяє уникнути повторних запитів і забезпечує швидкий обмін даними між пристроями.

Протокол ARP не має вбудованих механізмів перевірки достовірності отриманих відповідей. Це робить його вразливим до атак типу ARP-spoofing, під час яких зловмисник надсилає підроблені ARP-відповіді, змінюючи відповідність між IP- та MAC-адресами у кеші жертви. У результаті мережний трафік може бути перенаправлений через пристрій атакуючого, що створює умови для перехоплення даних, атак «людина посередині» (MITM) або порушення доступності мережних ресурсів [1]. Зловмисник зможе змінювати вміст повідомлень (фільтрувати, вводити команди або шкідливий код тощо), захоплювати з'єднання. Тому питання захисту ARP-протоколу та запобігання підміні мережевих адрес є актуальним і потребує нових досліджень та рішень.

Результати дослідження

Для запобігання ARP спуфінгу, в роботі [2] було запропоновано додавання цифрового підпису до протоколу ARP, з метою усунення основної вразливості класичного ARP – відсутності автентифікації відправника. У базовому варіанті Secure Address Resolution Protocol (S-ARP) кожній IP-адресі в мережі ставиться у відповідність не лише відповідна MAC-адреса, але й цифровий підпис. Структуру пакету протоколу S-ARP показано на рисунку 1.

На відміну від стандартного ARP, пакет S-ARP містить спеціальний заголовок з унікальним ідентифікатором (magic), часовою міткою (timestamp) для запобігання атакам повторного відтворення,

цифровим підписом (signature), що генерується власником IP-адреси за допомогою приватного ключа і поля siglen для визначення його довжини.

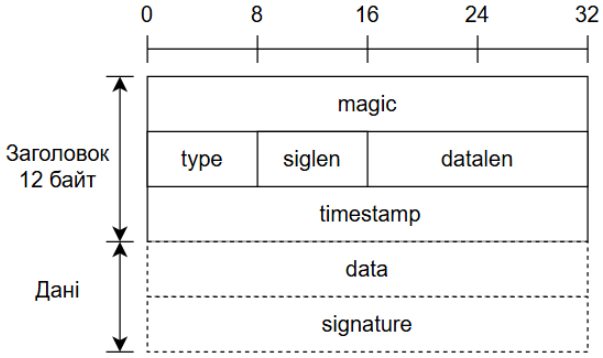


Рисунок 1 — Структура пакету S-ARP

Для централізованого керування довірою в системі використовується довірчий центр сертифікації, який підтверджує право хоста використовувати конкретну IP-адресу. Приватний ключ зберігається локально на пристрої, тоді як публічний ключ передається до центру разом з IP- та MAC-адресами вузла. Після перевірки отриманих даних центр сертифікації підписує публічний ключ власним приватним ключем, створюючи сертифікат. Під час формування S-ARP-запиту комп'ютер генерує відповідь, підписує її своїм приватним ключем і додає сертифікат, що підтверджує його публічний ключ. Поки криптографічна перевірка не завершена, вміст пакету ігнорується. Спочатку перевіряється валідність сертифіката за допомогою публічного ключа центру сертифікації. Після цього з сертифіката отримують публічний ключ відправника, який застосовується для перевірки підпису всередині ARP-повідомлення.

Однак, S-ARP має кілька суттєвих недоліків. Асиметрична криптографія потребує складних обчислень і призводить до помітного збільшення розміру ARP-повідомлень через включення сертифіката і підпису. У великих або завантажених мережах перевірка підпису для кожної отриманої ARP-відповіді може створювати значні затримки, що може впливати на загальну продуктивність мережі [3].

Виправити зазначені недоліки та водночас зберегти належний рівень захисту ARP-протоколу можливо завдяки застосуванню комбінованого підходу. Він полягає в тому, що складні асиметричні алгоритми використовуються лише на етапі первинного встановлення довіри між двома хостами, тоді як подальша взаємодія відбувається з використанням простіших симетричних механізмів. Цей спосіб дозволяє значно зменшити обчислювальне та мережеве навантаження, не втрачаючи цілісність та автентичність обміну ARP-повідомленнями.

При первинній взаємодії два вузли застосовують асиметричний криптоалгоритм RSA. Цей крок забезпечує захищений обмін службовою інформацією, у межах якого сторони узгоджують та встановлюють спільний сеансовий ключ.

Подальші обміни ARP-відповідями здійснюються за допомогою симетричного механізму — HMAC, що значно пришвидшує обробку кадрів і знижує навантаження на мережеві пристрої, оскільки обчислення геш-коду з ключем набагато швидші, ніж операції з відкритими та закритими ключами RSA. При цьому рівень захисту залишається високим, оскільки підробити HMAC без відомого сеансового ключа практично неможливо.

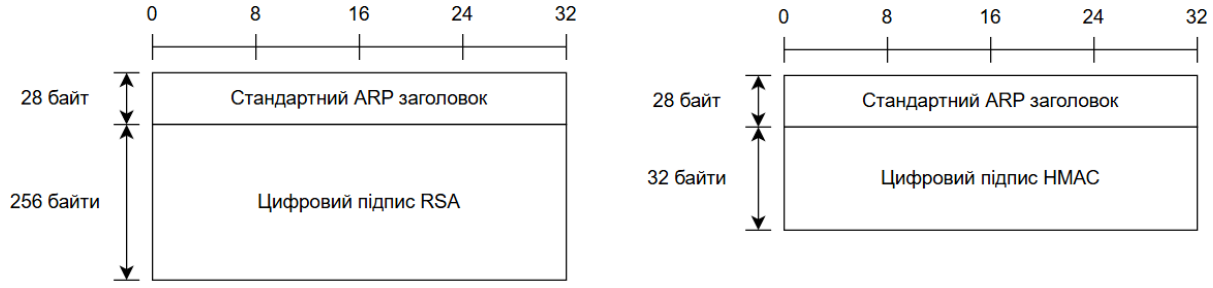
Будь-який ARP-пакет, що не проходить криптографічну перевірку або надходить без криптографічного підпису, автоматично відкидається отримувачем. Така поведінка блокує спроби отруєння ARP-кешу та унеможливлює підміну MAC-адрес зловмисником.

Реалізація механізму цифрового підпису не потребує зміни базового формату ARP пакету. Стандартний ARP-заголовок, що має фіксований розмір 28 байт, доповнюється спеціальним полем навантаження (payload), у якому передається криптографічний підпис. Під час первинного встановлення довіри між вузлами застосовується алгоритм RSA-2048 розміром 256 байт. Загальний розмір ARP-пакета становитиме 284 байт (рисунок 2, а).

Для подальших запитів і відповідей, коли довіра вже встановлена, використовується алгоритм HMAC-SHA256. Він додає лише 256 біт, тобто 32 байти додаткової інформації. У підсумку загальний

розмір ARP-повідомлення із захистом на основі HMAC становить 60 байт (рисунок 2, б), що практично не впливає на пропускну здатність мережі та затримки під час обміну.

Максимальний розмір Ethernet-кадру, становить 1500 байт. Найбільший пакет ARP з криптографічним підписом і з урахуванням заголовка Ethernet-кадру менший за встановлений ліміт, що гарантує відсутність фрагментації та забезпечує коректну доставку пакетів у локальній мережі.



а) б)

Рисунок 2 — Структура ARP-пакета
а) з RSA-підписом; б) з HMAC-підписом

Додатковим рівнем захисту у запропонованій схемі є поведінкова детекція, яка відстежує нетипові зміни співвідношень IP – MAC та аномалії у часових інтервалах відповідей, що вказують на спроби спуфінгу або повторного відтворення. Наявність такого модуля дозволяє відкинути пакети, що не проходять криптографічну перевірку.

Висновки

Таким чином, удосконалення ARP за допомогою впровадження механізму цифрового підпису усуває головну вразливість протоколу до атаки ARP-spoofing — відсутність автентифікації відправника. Запропоновано комбінований криптографічний підхід, який поєднує сильну асиметричну криптографію для початкового встановлення довіри та швидкі симетричні алгоритми для подальшого обміну ARP-повідомленнями.

Такий метод захисту усуває недоліки, пов’язані з великими обчислювальними витратами та затримками під час перевірки підписів. Він використовує асиметричну криптографію лише під час первинного встановлення довіри між вузлами, що дозволяє узгодити сеансовий ключ. Подальша обробка ARP-повідомлень відбувається з використанням HMAC, який забезпечує швидку перевірку автентичності без втрати рівня захисту, що суттєво знижує навантаження на мережеве обладнання.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What Is ARP Spoofing? [Електронний ресурс] — Режим доступу до ресурсу: https://jumpcloud.com/it-index/what-is-arp-spoofing

2. D. Bruschi, A. Ornaghi, and E. Rosti, «S-ARP: A secure address resolution protocol» in Proc. 19th Annu. Comput. Secur. Appl. Conf., 2003, pp. 66–74

3. S. Oei, Y. Suyanto and R. Pulungan, «A Comprehensive Approach for Detecting and Handling MitM-ARP Spoofing Attacks,» in IEEE Access, vol. 13, 2025, pp. 115503-115519

Паламарчук Катерина Олександрівна — студентка групи 1КІ-24м, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, katerina_854@ukr.net.

Войцеховська Олена Валеріївна — кандидат технічних наук, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця.

Palamarchuk Kateryna O. — student, 1KI-24ms, Faculty of information Technologies and Computer Engeneering, Vinnytsa National Technical University, Vinnytsia, katerina_854@ukr.net.

Voitsekhovska Olena V. — Candidate of Technical Sciences, Associate Professor of the Department of Computer Techniques, Vinnytsia National Technical University, Vinnytsia.