УДК 004.056.53

ЗАСТОСУВАННЯ В КОМП'ЮТЕРНИХ МЕРЕЖАХ АТАК ТИПУ «MAN-IN-THE-MIDDLE» ТА ЗАХИСТ ВІД НИХ

Костенецький К.В.
Науковий керівник– к. т. н., ст. викладач Никитенко О.Д.

Проблема інформаційної безпеки стає перед нами щодня. З кожним заходом в Інтернет через публічні Wi-Fi мережі, користувачі піддають себе такими небезпеками як крадіжка даних, особистої інформації, паролів, а також крадіжка грошей. Подібні атаки реалізовані за допомогою техніки ARP-spoofing, що дозволяє перехоплювати інформацію між вузлами завдяки недолікам ARP (Address Resolution Protocol) протоколу. Найпоширеніша з них має назву «Man in the middle» (MITM-атака), за допомогою якої криптоаналітик здатний читати і видозмінювати повідомлення, якими обмінюються користувачі. Для реалізації такої атаки зловмисник ставить себе в ланцюг між двома користувачами, що спілкуються в мережі Інтернет, щоб перехоплювати їх повідомлення. При цьому зловмисник видає себе за кожну з протилежних сторін. Ці атаки є достатньо ефективними і їх важко відстежити.

Одним із способів захисту від такої атаки є використання стійкого шифрування між клієнтом і сервером. У такому випадку сервер може ідентифікувати себе за допомогою надання цифрового сертифікату, після чого між користувачем і сервером встановлюється шифрований канал для обміну конфіденційними даними.

Ще один спосіб що б убезпечити себе, використовувати захищений HTTPS протокол, в якому дані «упаковуються» в криптографічний протокол SSL (Secure Sockets Layer). Більшість сайтів пов'язаних з електронною поштою, банками використовують його за замовчуванням.

Один з можливих способів реалізації MITM-атаки на захищене з'єднання SSL це використання спеціалізованих програм, наприклад, програми SSLStrip. Проте використання таких програм має і «недолік», який полягає в тому, що атакуючий не зможе надати підписані цифрові сертифікати і користувач буде бачити попередження про ненадійний сертифікат, коли така атака відбудеться.

Інший більш надійний спосіб захистити себе від такої атаки, це зробити статичний запис MAC і IP адреси роутера в ARP таблицю. Зробити це можна командою arp-s <IP-адрес> <MAC-адрес> в операційній системі Windows. Тоді при спробі зловмисником оголосити себе роутером, користувач звірить його IP і MAC адресу з адресами з ARP таблиці і відхилить його запит.

Виходячи з проведеного аналізу, проблема атаки «Man in the middle» все ще відкрита і немає універсального способу захисту. Тому є необхідність пошуку рішення проблеми інформаційної безпеки в комп'ютерних мережах при таких атаках.