УДК 004.056

ВРАЗЛИВІСТЬ ПРОТОКОЛУ HTTPS ДО АТАК ТИПУ LOGJAM

Султанова С.Ф.

Гриник Р.О., ЛДУ БЖД, викладач КУІБ

ЛДУ БЖД

Як правило, обмін даними між абонентами в інтернеті відбувається по протоколу HTTP, цей протокол не тільки встановлює правила обміну інформацією, а й служить транспортом для передачі даних - з його допомогою браузер завантажує вміст сайту на ваш комп'ютер або смартфон. Протокол HTTP має один суттєвий недолік, він передає інформацію у відкритому вигляді, що дає змогу зловмиснику перехопити дані котрі передаються. Для встановлення безпечного з'єднання використовується протокол HTTPS з підтримкою шифрування. Захист даних в протоколі HTTPS забезпечує криптографічній протокол SSL/TLS, який використовує асиметричну криптографію для встановлення з'єднання, симетричну криптографію для шифрування повідомлення та коди автентифікації повідомлення для забезпечення цілісності інформації. Проте на даний час використання протоколу HTTPS не гарантує високої ступені захищеності, оскільки він вразливий на транспортному рівні.

На транспортному рівні безпеку забезпечує протокол TLS який в 2008 році замінив протокол SSL v.3.0. Вразливість протоколу полягає в тому, що ще в середині дев'яностих років на вимогу США розробники протоколу ввели обмеження щодо алгоритму Діффі-Хеллмана, а протокол TLS використовує даний алгоритм для захисту спільного секретного ключа підчас передачі його по незахищеним каналам зв'язку. Дана вразливість отримала назву Logjam, вона дає змогу зловмиснику підключитись до каналу зв'язку і стати посередником між абонентом мережі та сервером з підтримкою обміну секретними ключами по алгоритму Діффі-Хеллмана. Для цього зловмиснику необхідно надсилати на сервер модифіковані запити для того, щоб заставити сервер використовувати у всіх з'єднаннях слабкий ключ довжиною 512 біт. Після цього атака зводиться до алгоритмів факторизації великих цілих чисел, для цього можна використати як загальний метод решета числового поля, так і інтелектуальні моделі факторизації великих простих чисел побудовані на еволюційних алгоритмах [1,2].

Особливість атаки Logjam полягає втому, що вона протягом довгого часу залишається непомітною і може виконуватись у режимі реального часу. По оцінкам Надії Хенінджер з Пенсільванського університету атака на протокол HTTPS зачіпає приблизно 8,4 % з першого мільйона найпопулярніших сайтів і трохи більший процент поштових серверів. Зокрема, ті з них, які підтримують протокол StartTLS, а також безпечну авторизацію POP3 або IMAP, за її

оцінками, серед них зараз уразливі відповідно 14,8%, 8,9% і 8,4% поштових серверів [3].

Проблема полягає ще і в тому, що подібний спосіб компрометації ключів може використовуватися проти будь-яких серверів, які підтримують обмін ключами по протоколу Діффі-Хеллмана (DH). У теорії він дозволяє двом сторонам передати секретний ключ по незахищеному каналу зв'язку, але на практиці не повинен використовуватися як самодостатній метод. Для високої надійності систем передачі даних рекомендується додатково використовувати двосторонню автентифікацію або реалізовувати DH на еліптичних кривих (ECDHE). Перевірити сайт на уразливість до атаки Logjam можна на сайті WeakDH.

ЛІТЕРАТУРА

1. Гриник Р.О., Застосування генетичного алгоритму для вирішення задач криптоаналізу, Інформаційно-комунікаційні технології в сучасній освіті: досвід, проблеми, перспективи : IV Міжнар. наук.-практ. конф., 21-22 жовт. 2015 р. : зб. наук. пр. – Ч. 1. – Львів, Вид-во ЛДУ БЖД, 2015. – С. 168-170

2. Гриник Р.О., Шадий В.І. Побудова моделі інтелектуальної системи на базі генетичного алгоритму для криптоаналізу RSA, "Захист інформації в інформаційно-комунікаційних системах": збірник тез доповідей І Міжвузівської науково-практичної конференції. – Львів: ЛДУ БЖД, 2015. С. 23-24.

3. HTTPS-crippling attack threatens tens of thousands of Web and mail servers [Електронний ресурс]. Режим доступу: http://arstechnica.com/security/2015/05/https-crippling-attack-threatens-tens-of-thousands-of-web-and-mail-servers/