DOI https://doi.org/10.36059/978-966-397-479-8-130

АНАЛІЗ ПОТОЧНОГО СТАНУ КРИПТОГРАФІЧНИХ ПРОТОКОЛІВ

Петков Є. І.
аспірант за спеціальністю 125 – Кібербезпека та захист інформації
Міжнародний гуманітарний університет
Науковий керівник: ***Йона Л. Г.***
кандидат технічних наук,
завідувач, доцент кафедри комп'ютерної інженерії
та інноваційних технологій
Міжнародний гуманітарний університет
м. Одеса, Україна

На сьогодні TLS/SSL – це один із ключових протоколів забезпечення безпеки передачі даних в Інтернеті та в корпоративних мережах. Він гарантує конфіденційність, цілісність та автентичність переданих даних, що робить його незамінним для захисту онлайн-комунікацій. Зазвичай він працює між клієнтом (наприклад, веб-браузер) та сервером (веб-сервер).

TLS є більш сучасною і безпечною версією протоколу SSL. Історично SSL був розроблений компанією Netscape у 1990-х роках, а TLS став його вдосконаленим і стандартизованим варіантом після того, як SSL був визнаний небезпечним через виявлені вразливості. Тому в сучасній практиці зазвичай використовується саме TLS (чинні версії TLS 1.2 та TLS 1.3), хоча термін SSL все ще часто використовується для позначення цього типу захисту.

Найбільш розповсюджене використання TLS/SSL – це протокол HTTPS (як SSL/TLS в комбінації з HTTP). Також цей протокол використовується в інших сервісах, а саме:

– протоколи SMTPS, POP3S, IMAPS, використовують TLS для захищеного поштового трафіку;

– протокол FTPS (FTP Secure) використовує TLS для захищеного трансферу файлів;

– для шифрування даних у VPN-з'єднаннях.

Протокол SSH забезпечує безпечний спосіб підключення користувачів до віддалених систем (серверів), виконання команд, керування мережевими пристроями і, навіть, передачу файлів через зашифрований канал. Протокол працює в клієнт-серверній моделі, з встановленням підключення SSH-клієнтом до SSH-сервера.

Перша версія протоколу (SSH-1), розроблена в 1995 році фінським дослідником Тату Ілоненом з Технологічного університету Гельсінкі. SSH-2 – поточна та безпечніша версія протоколу, в якій виправлено деякі архітектурні проблеми та вразливості першого. Вона підтримує надійніші алгоритми шифрування та протоколи обміну ключами.

Найбільш розповсюдженим є використання протоколу SSH:

– для віддаленого підключення до серверів та передачі команд для керування системою;

– для захищеного передавання файлів за допомогою протоколів SCP (Secure File Copy), або SFTP (SSH File Transfer Protocol).

Клієнт SSH керує процесом встановлення з'єднання до сервера та ініціює встановлення TCP-з'єднання (як правило по порту 22, але це може бути і не стандартний порт). На стадії обміну ключами, клієнт та сервер домовляються про використання алгоритму шифрування та обмінюються криптографічними ключами для встановлення спільного сеансового ключа, що буде використовуватись далі для шифрування даних. На стадії аутентифікації клієнт може підтвердити свою особу перед сервером двома способами:

– за допомогою введення персонального пароля при парольній аутентифікації;

– за допомогою пари ключів (публічного і приватного) при без-парольній аутентифікації.

Після вдалої аутентифікації встановлюється зашифроване з'єднання (як правило вже симетричним шифруванням), для безпечної передачі команд або даних між клієнтом і сервером.

IPSec – це сучасний протокол (або набір протоколів) для створення VPN-з'єднань, захисту корпоративних мереж при передачі конфіденційної інформації через відкритий незахищений канал зв'язку (як Інтернет, або будь-який інший). IPsec працює на мережевому рівні (Layer 3 OSI) і використовується для захищеної комунікацій між двома віддаленими пристроями в мережі (як то маршрутизатори, або файєрволи), забезпечуючи шифрування, автентифікацію та цілісність даних.

Основні компоненти IPSec:

– протокол AH (Authentication Header). Призначений для автентифікації даних та їх цілісності. AH не шифрує дані, але додає заголовок для перевірки автентичності та цілісності переданого;

– протокол ESP (Encapsulating Security Payload). Призначений для шифрування, автентифікації даних та їх цілісност;

– протокол IKE (Internet Key Exchange). Призначений для обміну ключами та аутентифікації між двома сторонами перед створенням захищеного з'єднання IPSec. Протокол IKE працює раніше протоколів AH

та ESP, узгоджує параметри обох кінцевих сторін, встановлює між двома сторонами логічне з'єднання, яке в IPSec носить назву «безпечна асоціація» (Security Association, SA). Остання та вдосконалена версія протоколу з покращенною безпекою – це IKEv2.

WPA3 (Wi-Fi Protected Access 3) – протокол безпеки для бездротових мереж, це третя та остання наразі версія стандарту, розробленого Wi-Fi Alliance. Він був анонсований у 2018 році для заміни попереднього стандарту WPA2 разом зі своїми недоліками. В WPA3 додані нові функції безпеки в персональних та корпоративних мережах завдяки підвищенню криптографічної стійкості та підвищення безпеки автентифікації для всіх кінцевих користувачів WPA3. Стандарт WPA3 використовує останні методи та протоколи безпеки, забороняє використання застарілих протоколів, та робить обов'язковим використання технології PMF (Protected Management Frames). Остання технологія додатково захищає бездротовий канал від таких атак, як відмова в обслуговуванні (DoS), honeypots (пастка або приманка) та прослуховування трафіка.

Таблиця 1

Порівняння характеристик криптографічних протоколів

Протокол	SSL/TLS	SSH	IPSec	WPA
Актуальна версія	TLS 1.2, TLS 1.3	SSH-2	IKEv2, ESP/AH	WPA3
Використання	HTTPS, SMTPS, POP3S, IMAPS, FTPS	SSH, SFTP, SCP	VPN-з'єднання між віддаленими мережами	Бездротові Wi-Fi мережі 802.11ac, 802.11ax (Wi-Fi 6)
Шифрування	AES (Advanced Encryption Standard): AES-CCM, AES-GCM; ChaCha20-Poly1305	AES: AES-128, AES-256; ChaCha20	AES: AES-128, AES-192 AES-256; ChaCha20	AES CCMP (Counter Cipher Block Chaining Message Authentication Code Protocol); GCMP (Galois/Counter Mode Protocol)
Автентифікація	RSA (Rivest–Shamir–Adleman), ECDSA (Elliptic Curve Digital Signature Algorithm)	RSA, DSA (Digital Signature Algorithm), ECDSA, Ed25519	HMAC (Hash-Based Message Authentication Code)	SAE (Simultaneous Authentication of Equals) для WPA3-Personal; 802.1X для WPA3-Enterprise
Обмін ключами	ECDH (Elliptic Curve Diffie-Hellman), RSA, Pre-Shared Keys (PSK)	DH (Diffie-Hellman), ECDH, RSA	IKEv2 включає: DH з різними групами (Group 1, 2, 5, 14, 15, 16, тощо); ECDH	SAE, SAE з Diffie-Hellman

Оскільки Wi-Fi Alliance відрізняє мережі Wi-Fi за своїми цілями використання та потребами безпеки, WPA3 містить додаткові можливості як для персональних, так і для корпоративних мереж. Користувачі WPA3-Personal отримали посилений захист від повторюваних спроб вгадування пароля, а користувачі WPA3-Enterprise мають можливість скористатися перевагами протоколів безпеки вищого рівня для конфіденційних мереж.

WPA3-Personal надала посилений захист окремим користувачам, забезпечуючи більш надійну автентифікацію на основі пароля, навіть якщо користувачі вибирають прості паролі, які не відповідають рекомендаціям щодо своєї складності. Цю функцію забезпечує технологія Simultaneous Authentication of Equals (SAE). Технологія стійка до так званих «словникових атак» в режимі оффлайн, коли зловмисник намагається визначити пароль, пробуючи можливі паролі без подальшої взаємодії з мережею. Відповідно, користувачам дозволяється обрати паролі, які легше запам'ятати. У табл. 1 представлено порівняльні характеристики криптографічних протоколів

Для кожного із розглянутих протоколів є своє ключове призначення. Для SSL/TLS – це переважно, захист клієнт-серверних з'єднань веб трафіку, а також захисту даних для інших відомих протоколів передачі даних. Для SSH першочергова місія – це безпечний доступ до віддалених систем та передача команд керування, а також захищена передача файлів. Для IPSec – захист каналу зв'язку на мережевому рівні між віддаленими мережами (VPN технологія). Для WPA3 – це безпека підключення користувачів та обміну даних в бездротових Wi-Fi мережах. В основі більшості розглянутих вище протоколів лежать відомі базові криптографічні протоколи, наприклад, AES (симетричне шифрування), RSA (автентифікація), DH (обмін ключів) та їх більш сучасні модифікації.

Література:

1. Encryption Consulting. What are Encryption Protocols and How Do They Work? URL: https://www.encryptionconsulting.com/what-are-encryption-protocols-and-how-do-they-work/

2. F5. What is SSL/TLS Encryption? URL: https://www.f5.com/glossary/ssl-tls-encryption

3. Wikipedia. Transport Layer Security. URL: https://en.wikipedia.org/wiki/Transport_Layer_Security

4. SSH Protocol – Secure Remote Login and File Transfer. URL: https://www.ssh.com

5. Introduction to Cisco IPsec Technology. URL: https://www.cisco.com/c/en/us/td/docs/net_mgmt/vpn_solutions_center/2-0/ip_security/provisioning/guide/IPsecPG1.html

6. Understand IPsec IKEv1 Protocol. URL: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/217432-understand-ipsec-ikev1-protocol.html
7. Wi-Fi Alliance. URL: https://www.wi-fi.org/

DOI https://doi.org/10.36059/978-966-397-479-8-131

ДОСЛІДЖЕННЯ МЕТОДІВ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ПРИСТРОЇВ МОБІЛЬНОГО ЗВ'ЯЗКУ

Потапальський К. В.
здобувач вищої освіти другого (магістерського) рівня
за спеціальністю 172 – Електронні комунікації та радіотехніка
Міжнародний гуманітарний університет

Бублик М. І.
здобувач вищої освіти другого (магістерського) рівня
за спеціальністю 172 – Електронні комунікації та радіотехніка
Міжнародний гуманітарний університет
Науковий керівник: ***Вакарчук А. О.***
кандидат технічних наук,
доцент кафедри комп'ютерної інженерії та інноваційних технологій
факультету кібербезпеки, програмної інженерії та комп'ютерних наук
Міжнародний гуманітарний університет
м. Одеса, Україна

У сучасному світі мобільні пристрої стали невід'ємною частиною життя людей, забезпечуючи не лише зв'язок, але й доступ до інформації, розваг та послуг. Зі зростанням обсягів використання мобільних технологій виникають нові виклики, пов'язані з ефективністю роботи пристроїв, зокрема зі зменшенням енергоспоживання, підвищенням продуктивності, покращенням якості зв'язку та забезпеченням стійкої роботи в умовах високого навантаження на мережі.

Актуальність теми полягає в тому, що зростаючий попит на мобільні пристрої та технології створює потребу у впровадженні нових підходів до їх оптимізації. Ефективне використання мобільних пристроїв стає критичним як для кінцевих користувачів, так і для операторів мобільного зв'язку. Покращення технічних характеристик пристроїв та оптимізація використання мережевих ресурсів сприятиме розвитку галузі та