**Львівський національний університет імені Івана Франка**

**Факультет електроніки та комп’ютерних технологій**

*Кафедра радіоелектронних і комп’ютерних систем*

**Звіт**

про виконання лабораторної роботи №7

*«SSL-сертифікати»*

**Виконав:**

студентки групи ФеІ-31

Зьола О.П.

Викладач:  
Сінькевич О.О.

Львів

2020

**Мета роботи:** ознайомитися із SSL-сертифікатами, їх змістом та різновидами.

**Завдання:** проаналізувати літературу та винести основні тези про SSL-сертифікати, їх вміст та різновиди.

**Порядок виконання роботи:**

1. Проаналізувавши літературу в інтернеті, я ознайомилася із із SSL-сертифікатами, їх змістом та різновидами. Виділила наступні теоретичні дані:

***Протокол SSL*** (від англ. Secure Sockets Layer –рівень захищених сокетів) використовується мільйонами сайтів для захисту даних в Інтернеті. Він гарантує безпечне з'єднання між браузером користувача та сервером. При використанні SSL-протоколу інформація передається в закодованому вигляді по HTTPS і розшифрувати її можна тільки за допомогою спеціального ключа на відміну від звичного протоколу HTTP. Для роботи SSL-протоколу потрібно, щоб на сервері був встановлений SSL-сертифікат.

*Що таке SSL-сертифікат?*

*SSL-сертифікат* – це свого роду унікальна цифровий підпис вашого сайту. Такий сертифікат потрібен, в першу чергу, банкам, платіжним системам і іншим організаціям, що працюють з персональними даними, - для захисту транзакцій і запобігання несанкціонованого доступу до інформації.

SSL-сертифікат містить наступну інформацію:

* доменне ім'я, на яке оформлено SSL-сертифікат;
* юридична особа, яка володіє сертифікатом;
* фізичне місцезнаходження власника сертифіката (місто, країна);
* термін дії сертифіката;
* реквізити компанії-постачальника SSL-сертіфікатa.

SSL-Сертифікат підтверджує, що домен належить реальній компанії і що його власник має право користуватися секретним ключем на законних підставах.

Протокол SSL надає «безпечний канал», який має три основні властивості:

* Канал є приватним. Шифрування використовується для всіх повідомлень після простого діалогу, який служить для визначення секретного ключа.
* Канал аутентифікований. Серверна сторона діалогу завжди аутентифицирующей, а клієнтська робить це опціонально.
* Канал надійний. Транспортування повідомлень включає в себе перевірку цілісності.

Перевагою SSL є те, що він незалежний від прикладного протоколу. Протоколи додатків ( HTTP , FTP , TELNET і т. Д.) Можуть працювати над протоколом SSL абсолютно прозоро, тобто SSL може погоджувати алгоритм шифрування і ключ сесії, а також аутентифікувати сервер до того, як додаток прийме або передасть перший байт повідомлення.

*Яка різниця між HTTP і HTTPS?*

HTTPS (HyperText Transfer Protocol Secure) - це розширення протоколу HTTP, що підтримує шифрування. Дані, що передаються по протоколу HTTP, «упаковуються» в криптографічний протокол SSL або TLS. За замовчуванням HTTPS використовує 443 TCP-порт (для незахищеного HTTP - 80).

Щоб підготувати веб-сервер для обробки HTTPS-з'єднань, адміністратор повинен отримати і встановити в систему сертифікат для цього веб-сервера. Сертифікат складається з двох частин (двох ключів) - public і private. Public-частина сертифіката використовується для шифрування трафіку від клієнта до сервера в захищеному з'єднанні; private-частина - для розшифрування отриманого від клієнта зашифрованого трафіку на сервері.

Після того як пара ключів приватний / публічний згенеровані, на основі публічного ключа формується запит на SSL-сертифікат в Центр сертифікації.

Існує можливість створити такий сертифікат, не звертаючись до Центру сертифікації. Підписуються такі сертифікати цим же сертифікатом і називаються самоподпісанного (self-signed).

*Різновиди SSL-сертифікатів*

Існує кілька типів SSL-сертифікатів:

1. SSL-сертифікати з перевіркою домену (Domain Validation) - це сертифікати початкового рівня, є найпоширенішими в світі, а швидкість видачі таких сертифікатів варіюється від 2 до 10 хвилин, залежить від бренду. Щоб отримати такий сертифікат, не потрібно спеціальних документів. Такі сертифікати підійдуть для невеликих сайтів і маленьких проектів, коли немає необхідності у великій довірі з боку клієнтів та відвідувачів сайту. Потрібно підтвердити володіння доменом:

* перевірка через електронну пошту (DCV Email) - центр сертифікації висилає верифікаційного лист, в якому буде посилання для підтвердження володінням домену. Вислати такий лист можуть або на пошту, вказану у Whois вашого домену, або на один із золотої п'ятірки: admin @ , administrator @ , hostmaster @ , postmaster @ , webmaster @ вашого сайту;
* перевірка за допомогою DNS-записи (DNS CNAME) - спосіб для тих, у кого налаштований мейл-сервер, а пошта у Whois закрита приватній реєстрацією. Необхідно створити особливу запис у вашому DNS, і центр сертифікації його перевірить. Метод повністю автоматичний;
* перевірка за допомогою хеш-файлу (HTTP CSR Hash) - користувачеві буде надано спеціальний .txt файл, який необхідно завантажити на свій сервер, при цьому центр сертифікації переконається в його наявності та сертифікат буде виданий. Метод повністю автоматичний.

1. SSL-сертифікати з перевіркою компанії (Business Validation) - такі сертифікати актуальні для тих, хто думає про довіру до своїх продуктів, компанії і сервісів, так як центр сертифікації проводить більш ретельну перевірку. Необхідно вислати документи компанії, пройти процес «віддзвонили» на корпоративний телефон.
2. SSL-сертифікати з розширеною перевіркою (Extended validation) - тільки EV сертифікати забезпечать сайт зеленої адресним рядком в браузері. Найчастіше такі сертифікати можна зустріти у банків, онлайн-систем з великою кількістю відвідувачів.
3. SSL-сертифікати c підтримкою субдоменів (Wildcard) -це дуже зручний сертифікат, коли мова йде про захист великої кількості субдоменів в рамках одного домена. Він може захистити будь-яку кількість субдоменів на необмеженій кількості серверів.
4. SAN SSL-сертифікати - єдині сертифікати зв'язку, які здатні захищати безліч доменів, субдоменів, локальних доменів і серверів. Дані сертифікати працюють як із зовнішніми, так і внутрішніми доменними іменами. SGC SSL-сертифікати - застарілі сертифікати, які примусово збільшують рівень шифрування для старих браузерів з 40 біт до повноцінних 256 біт.
5. SSL-Сертифікати для ПО (CodeSigning SSL) -такі сертифікати можуть допомогти, коли ваші користувачі отримують попередження та помилки при скачуванні програмного коду з ваших ресурсів. Це ідеальний продукт для розробників програмного забезпечення, він використовується для захисту програмних продуктів розповсюджуваних в мережі.

*Формат заголовка записів SSL*

Всі дані в SSL пересилаються у вигляді записів (рекордів) - об'єктів, які складаються з заголовка і деякої кількості даних. Кожен заголовок рекорду містить 2 або 3 байти коду довжини. Якщо старший біт в першому байті коду довжини рекорду дорівнює 1, тоді рекорд не має заповнювач і повна довжина заголовка дорівнює 2 байтам, в іншому випадку рекорд містить заповнювач, і повна довжина заголовка дорівнює 3 байтам. У разі довгого (3 байта) заголовка другий за старшинством біт першого байта обмежене спеціальним значенням. Якщо він дорівнює 0 - рекорд є інформаційним, якщо він дорівнює 1 - рекорд є security escape. Код довжини рекорду не включає в себе число байт заголовка. Для 2-байтового заголовка його довжина обчислюється так:

RECORD-LENGTH = ((byte [0] & 0x7F) << 8) | byte [1];

Тут byte [0] - перший отриманий байт, а byte [1] - другий отриманий байт.

Для 3-байтового заголовка довжина рекорду обчислюється таким чином:

RECORD-LENGTH = ((byte [0] & 0x3F) << 8) | byte [1];

IS-ESCAPE = (byte [0] & 0x40)! = 0;

PADDING = byte [2];

Значення PADDING специфікує число байтів, доданих відправником до вихідного рекорду. Дані заповнювач використовуються для того, щоб зробити довжину рекорду кратною розміру блоку шифру. Відправник додає PADDING після наявних даних, а потім шифрує все це, так як довжина цього масиву кратна розміру блоку використовуваного шифру. Оскільки відомий обсяг переданих даних, заголовок повідомлення може бути сформований з урахуванням обсягу PADDING . Одержувач повідомлення дешифрує все поле даних і отримує вихідну інформацію, потім обчислює справжнє значення RECORD-LENGTH , при цьому PADDING з поля «дані» видаляється.

*Формат інформаційних записів SSL*

Частина даних рекорду SSL складається з 3 компонентів:

MAC-DATA [MAC-SIZE]

ACTUAL-DATA [N]

PADDING-DATA [PADDING]

MAC-DATA - код аутентифікації повідомлення

MAC-SIZE - функція використовуваного алгоритму обчислення хеш-суми

ACTUAL-DATA - реально передані дані або поле даних повідомлення

PADDING-DATA - дані PADDING (при блочному шифруванні)

MAC-DATA = HASH [ SECRET , ACTUAL-DATA , PADDING-DATA , SEQUENCE-NUMBER ]

Тут SECRET передається хеш-функції першим, потім слід ACTUAL-DATA і PADDING-DATA , за якими передається SEQUENCE-NUMBER - порядковий номер.

Значення SECRET залежить від того, хто саме посилає повідомлення. Якщо це робить клієнт, то SECRET дорівнює CLIENT-WRITE-KEY . Якщо ж клієнт отримує повідомлення, SECRET дорівнює CLIENT-READ-KEY .

Порядковий номер представляє собою 32-бітовий код, який передається хеш-функції у вигляді 4 байт, використовуючи мережевий порядок передачі «від старшого до молодшого». Порядковий номер - лічильник для сервера або клієнта. Для кожного напрямку передачі використовується пара лічильників - для відправника і для одержувача; кожен раз, коли відправляється повідомлення, лічильник збільшує своє значення на 1.

Одержувач повідомлення використовує очікуване значення порядкового номера для передачі MAC (тип хеш-функції визначається параметром CIPHER-CHOICE ). Обчислення значення MAC-DATA має збігатися з переданим значенням. Якщо порівняння не пройшло, повідомлення вважається пошкодженим, що призводить до виникнення помилки, яка викликає закриття з'єднання.

Остаточна перевірка відповідності виконується, коли використовується блоковий шифр. Обсяг даних в повідомленні ( RECORD-LENGTH ) повинен бути кратний розміру блоку шифру. Якщо ця умова не виконана, повідомлення вважається пошкодженим, що призводить до розриву з'єднання.

Для 2-байтового заголовка максимальна довжина повідомлення одно 32767 байтів, для 3-байтового 16383 байтів. Повідомлення протоколу діалогу SSL повинні відповідати поодиноким рекордів протоколу SSL, а повідомлення прикладного протоколу можуть займати кілька рекордів SSL.

*Протокол діалогу SSL*

Протокол діалогу SSL містить 2 основні фази.

Перша фаза використовується для встановлення конфіденційного каналу комунікацій.Ця фаза ініціалізує з'єднання, коли обидва партнери обмінюються повідомленнями «hello». Клієнт посилає повідомлення CLIENT-HELLO . Сервер отримує це повідомлення, обробляє його і посилає у відповідь повідомлення SERVER-HELLO .У цей момент і сервер і клієнт мають достатньо інформації, щоб знати, чи потрібен новий master key. Якщо ключ не потрібен, сервер і клієнт переходять у фазу 2. Коли виникає необхідність створення нового master key , повідомлення сервера SERVER-HELLO вже містить достатньо даних для того, щоб клієнт міг згенерувати master key. У ці дані входять підписаний сертифікат сервера, список базових шифрів і ідентифікатор з'єднання (випадкове число, сгенерированное сервером, яке використовується протягом всієї сесії). Після генерації клієнтом master key він посилає серверу повідомлення CLIENT-MASTER-KEY або ж повідомлення про помилку, коли клієнт і сервер не можуть узгодити базовий шифр.Після визначення master key сервер посилає клієнтові повідомлення SERVER-VERIFY , яке аутентифікує сервер.

Фаза 2 називається фазою аутентифікації. Так як сервер вже аутентифікований на першій фазі, то на другій фазі здійснюється аутентифікація клієнта. Сервер відправляє запит клієнта, і якщо у клієнта є необхідна інформація - він надсилає позитивний відгук, якщо ж ні - повідомлення про помилку. Коли один партнер виконав аутентифікацію іншого партнера - він посилає повідомлення finished . У разі клієнта повідомлення CLIENT-FINISHED містить зашифровану форму ідентифікатора CONNECTION-ID , яку повинен верифікувати сервер. Якщо верифікація була невдалою, сервер посилає повідомлення ERROR .

Коли один з партнерів послав повідомлення finished- він повинен приймати повідомлення до тих пір, поки не отримає повідомлення finished від іншого партнера, і тільки коли обидва партнери послали і отримали повідомлення finished , протокол діалогу SSL закінчить свою роботу. З цього моменту починає роботу прикладної протокол.

*Де отримати SSL-сертифікат?*

Для отримання сертифікату необхідно звернутися в компанії, які видають SSL-сертифікати. Наприклад, SSL.com.ua – один із найпопулярніших сервісів видачі SSL-сертифікатів. Вартість SSL-сертифіката на 1 рік може становити від 400 до 7000 гривень. Часто SSL-сертифікат може входити у вартість хостингу сайту.

**Висновок:** Виконуючи цю лабораторну роботу, я проаналізувала літературу та винесла основні тези про SSL-сертифікати, їх вміст та різновиди.