УДК 004

А.З.Піскозуб, С.Т.Шикеринець
Національний університет «Львівська політехніка»
кафедра захисту інформації

ПРОТОКОЛ SSL, ВИКОРИСТАННЯ ЙОГО ВРАЗЛИВОСТІ СПІЛЬНО З ЕЛЕМЕНТАМИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

The analysis of secure SSL protocol, the usage of its vulnerabilityy together with elements of social engineering, methods of protection against this vulnerability are been discussed in this paper.

Keywords – SSL, vulnerability, social engineering, methods of defend, the man in the middle.

В даній статті обговорюються аналіз захищеного протоколу SSL, використання його вразливостей спільно з елементами соціальної інженерії. Представлені методи боротьби з даною вразливістю.

Ключові слова – SSL, вразливість, соціальна інженерія, методи боротьби, людина посередині.

Вступ

Динаміка розвитку комп’ютерних технологій надала кібер-простір для ведення бізнесу, розширивши таким чином його можливості. З’явились туристичні агентства, Інтернет-магазини, Інтернет-банки, які ведуть розрахунки прямо через свої сайти. А там де є гроші - завжди знайдуться охочі їх отримати. Тому про безпеку фінансових операцій в мережі потрібно подумати заздалегідь..

Завдяки Інтернету взаємозв'язок клієнт-банк стає більш оперативним, що дозволяє також диференційовано працювати із замовником у залежності від індивідуальних переваг, схильності до ризику та формування портфеля клієнта. А розвиток інформаційних технологій дозволяє в значній мірі скоротити дистанцію між виробником і споживачем банківських послуг .

Інтернет-банкінг – це загальна назва технологій дистанційного банківського обслуговування, при якому доступ до рахунків і операцій надається в будь-який час і з будь-якого комп'ютера, що має доступ в мережу Інтернет. Цей напрямок в Україні в останні роки активно розвивається і вдосконалюється. Банки постійно проводять дослідження і впроваджують нові технології та розробляють нові способи захисту та кодування інформації про рахунки і паролі користувачів [1].

Для виконання операцій Інтернет-банкінгу використовується браузер, тобто відсутня необхідність установки клієнтської частини програмного забезпечення системи.

У цьому випадку постає надзвичайно важливе питання, чи може звичайний браузер гарантувати надійність та захищеність з’єднання між клієнтом та сервером. Передавати дані у відкритому вигляді – небезпечно, вони легко можуть стати здобиччю зловмисника, якому не складе труднощів перехопити, модифікувати і навіть підмінити їх. Ось чому логіни і паролі, а також інші конфіденційні дані по звичайному HTTP протоколу не передаються. Замість цього використовується захищений протокол HTTPS, який працює повільніше, але упаковує дані в криптографічний протокол SSL, і ті передаються вже в зашифрованому вигляді. SSL — криптографічний протокол, який забезпечує встановлення безпечного з'єднання між клієнтом і сервером, та забезпечує конфіденційність обміну даними між ними. Але чи можна повністю довіритися даній технології ?

Мета даної статті – показати недоліки протоколу SSL, який, використовується для Інтернет-банкінгу, зокрема використання його вразливості спільно з елементами соціальної інженерії, навести можливий сценарій несанкціонованого використання персональних даних, то розробити рекомендації, які можна виконати на стороні клієнта для виявлення і запобігання такої атаки.

Практичні аспекти реалізації

В даному випадку, найпоширенішим типом атак є атака зловмисник посередині, також відома як MitM (Man-in-the-Middle). Передбачається участь трьох сторін: сервера, клієнта і зловмисника, що знаходиться між ними. У даній ситуації зловмисник може перехоплювати всі повідомлення, які слідують в обох напрямках, і модифікувати їх. Зловмисник представляється сервером для клієнта і клієнтом для сервера (рис.1).

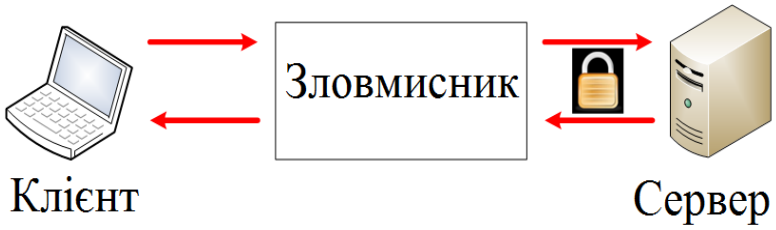

Рис. 1. Схема атаки зловмисник посередині, також відома як MitM (Man-in-the-Middle)

Під час виконання такої атаки зловмисник отримує контент HTTPS веб-сторінки і віддає його клієнту, але вже з розширенням HTTP. У результаті клієнт отримує оригінальну веб-сторінку. Сервер, що віддає весь контент по захищеному каналу, бачить зловмисника як клієнта, від якого приходить підключення, а справжній клієнт не отримує жодних попереджень і навіть не підозрює, що використовує незахищене з'єднання. Отже зловмисник перехоплює весь трафік [2].

Для того, щоб змусити клієнта довіритися такому з'єднанню, використовуються елементи соціальної інженерії. Соціальна інженерія – наука, що вивчає можливість отримання інформації, або певного роду вигоди внаслідок людської неуважності, використання простих паролів, ігнорування необхідних заходів безпеки. Для отримання конфіденційних даних застосовуються знання більше з соціології та психології, ніж зі сфери IT. Статистика демонструє, що велика кількість людей не достатньо зосереджує свою увагу при використанні власної конфіденційної інформації [3].

Під час даної атаки, активно використовуються логотипи захищених веб-сторінок, такі як піктограми замків золотистого, або зеленого кольору, в залежності від того, який браузер використовує жертва. Дані піктограми можна створити власноруч (рис.2):

Рис. 2. Різновиди піктограм, які можуть використовуватися для введення жертви в оману

Для практичної реалізації даної атаки можна використати дистрибутив операційної системи Back-Track на платформі Ubuntu 10.04. При цьому використовуватимуться інструменти SSLstip[4], ARPspoof [5]та Ettercap [6].

При цьому, дистрибутив Back-Track має бути налаштований на пересилання IP. Для цього виконується команда:

```
echo "1"> / proc/sys/net/ipv4/ip_forward
```

Після цього потрібно направляти весь трафік HTTP, який буде перехоплюватися, на порт, який буде прослуховуватися за допомогою інструменту SSLstrip. Для цього потрібно змінити конфігурацію міжмережевого екрану iptables наступним чином:

```
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 10000
```

Інструмент SSLstrip запускається з метою запису даних з 10000 порту, на який вони надходитимуть від клієнта до сервера і навпаки, а також буде використовуватись спеціальна захисна піктограма, щоб створити жертві ілюзію захищеного SSL каналу:

sslstrip.py –w login –l 100+600 –a –f

При цьому додатково буде проводитися запис всіх даних у файл login.

Наступним кроком у цьому процесі буде налаштування ARP спуфінгу для перехоплення трафіку з цільового вузла. Для цього потрібно виконати команду :

arpspoof -i <interface> -t <targetIP> <gatewayIP>,

де <interface> - інтерфейс підключення до локальної мережі, через який буде здійснюватись перехоплення, <targetIP> - IP адреса жертви, <gatewayIP> - IP адреса основного шлюзу.

Останньою дією буде використання інструменту ettercap, щоб в режимі реального часу побачити перехоплені дані :

ettercap –T –q –i <interface>

Реалізація

Для даного досліду було обрано захищену веб-сторінку відомого Інтернет-аукціону ”Ebay”. Для доступу до персональних даних, таких як розрахункові номери, домашня адреса, номер телефону, електронна скринька та списки замовлень, необхідно пройти авторизацію за допомогою логіну та паролю, які, в даному випадку, , є ціллю зловмисника.

Спершу жертва входить на звичайну сторінку авторизації, проте не через захищений протокол HTTPS, а через протокол HTTP. Вводить логін та пароль і авторизується як зазвичай, не помітивши різниці (рис.3).

а) б)

Рис. 3. Демонстрація різниці захищеним оригінальним з’єднанням (а) та з’єднанням, яке створене зловмисником (б).

В результаті здійснення даної атаки через вразливість протоклу SSL, зловмисник отримує в режимі реального часу конфіденційні дані (в даному випадку логін та пароль) (рис.4).

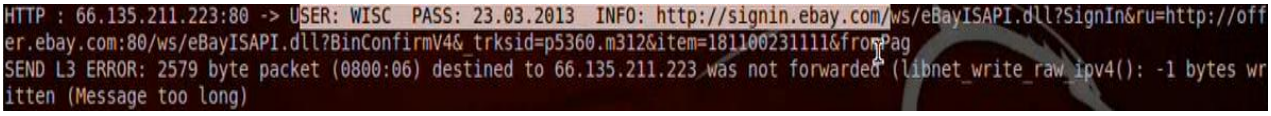

Рис.4. Демонстрація отримання конфіденційних даних (логін та пароль) за допомогою дистрибутиву Back-Track

Висновки

Проведене дослідження дає змогу на практиці переконатися у вразливості захищеного криптографічного протоколу SSL спільно з використанням елементів соціальної інженерії – через звичайну неуважність може відбутися витік конфіденційної інформації щодо банківських рахунків, що може бути використано зловмисниками для власних фінансових вигод, або підриву авторитету особи чи установи.

Відповідно до такої загрози рекомендовано здійснити наступні заходи, які можна виконати на стороні клієнта для виявлення і запобігання такої атаки :

• Необхідно переконатися в тому, що використовується саме захищене HTTPS підключення при використанні Інтернет-банкінгу. При використанні протоколу HTTP замість HTTPS є висока ймовірність того, що щось не так.

• Незалежно від моделі браузера, необхідно вміти розрізняти захищені підключення і незахищені.

• Рекомендується виконувати свої мережеві банківські операції вдома - шанси того, що хтось перехопить трафік в домашній мережі, набагато менші, ніж шанси перехоплення трафіку в корпоративній мережі.

• Необхідно перевіряти сертифікати сайтів, а також весь ланцюг сертифікатів.

• Рекомендується використовувати програми Certificate Search [7] та Certificate Checker [8].

• Регулярно оновлювати свої браузери. При переході на захищені веб-сторінки – набирати повний URL вручну.

Література

1. Воронін А. Електронний банкінг та ризики його використання. Фінансовий ринок України – 2009. - №1. 8-9 с. 2.SSLstrip. // http://www.thoughtcrime.org. 3.Social Engineering: Security Through Education. // http://www.social-engineer.org. 4. SSLstrip .// http://www.thoughtcrime.org/software/sslstrip 5.Ornaghi, Alberto, and Marco Valleri. An Ettercap Primer. // http://www.sans.org/reading_room/whitepapers/tools/ettercap-primer_1406. 6.Lockhart, Andrew .Network security hacks /O'Reilly-2007. 186c. ISBN 978-0-596-52763-1. 7. SSL Certificate Tools. // http://www.sslshopper.com/ssl-certificate-tools.html. 8.Certificate Check Install. // http://www.digicert.com/help.