Висновки

Передовий досвід інформатизації та комп'ютеризації освіти показує явно виражену тенденцію – навчання студентів практичним аспектам новітніх інформаційних технологій та їхньому застосуванню у майбутній професійній діяльності. Притому розвиток інформаційних технологій дає широку можливість для винаходу нових методів та методик в освіті, поліпшуючи її якість. Викладачі, використовуючи у своїй роботі контролюючі програмні засоби під час оцінювання рефератів, курсових, дипломних робіт, не тільки отримують обґрунтований висновок щодо самостійності досліджень студента, але й виховують шанобливе ставлення до чужої інтелектуальної власності та привчають дотримуватися Закону про авторське право. Вибір зручної програми для цього є складним процесом. Проаналізовані технології тестування текстів свідчать про доцільність використання в оцінюванні студентських робіт творчого або дослідницького характеру, в навчальному процесі під час організації самостійної діяльності студентів таких програм контролю, як Distortion. Простота у використанні, швидкість роботи, можливість інтерпретації результатів відповідно до бальної шкали оцінок, візуалізація результатів перевірки студентських робіт за допомогою гістограм, на наш погляд, є істотними перевагами у виборі програмних засобів.

1. Болілий В.О., Копотій В.В. Перевірка унікальності тексту при оцінюванні студентських робіт творчого або дослідницького характеру // Наукові записки. Серія "Психолого-педагогічні науки". – Ніжин: Видавництво НДУ ім. М. Гоголя, 2011. – № 7. – С. 134–145. 2. Капіца Ю. Спеціальні механізми захисту авторського права і суміжних прав в Інтернеті / Ю. Капіца, О. Рассомахіна, К. Шахбазян // Інтелектуальна власність. – К.: Держ. департ. інтелектуальної власності, 2012. – № 4. – С. 12– 24. 3. Ковальова А. Проблеми академічного плагіату та авторського права у цифровому просторі України / Спеціальні історичні дисципліни: питання теорії та методики. Електронні інформаційні ресурси // зб. наук. праць / Відп. ред. Г.В. Боряк. – К.: НАН України, Інститут історії України, 2013. – С. 61-71.

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

Здійснено аналіз захищеного протоколу SSL, використання його вразливостей спільно з елементами соціальної інженерії. Подано методи боротьби з такою вразливістю.

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

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.

Key words: SSL, vulnerability, social engineering, methods of defend, the man in the middle.

Вступ

Динаміка розвитку комп'ютерних технологій надала кіберпростір для ведення бізнесу, розширивши тим самим 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 оперативнішим, що дає змогу також диференційовано працювати із замовником залежно від індивідуальних переваг, схильності до ризику та формування портфеля клієнта. А розвиток інформаційних технологій дозволяє істотно скоротити дистанцію між виробником і споживачем банківських послуг.

Інтернет-банкінг – це загальна назва технологій дистанційного банківського обслуговування, за якого доступ до рахунків і операцій надається в будь-який час і з будь-якого комп'ютера, що має доступ в мережу Інтернет. Цей напрям 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 не потрібно встановлювати клієнтську частину 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 нескладно перехопити, модифікувати і навіть підмінити їх. Ось чому логіни і паролі, а також інші конфіденційні дані за звичайним HTTP протоколом 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 цій технології ?

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

Практичні аспекти реалізації

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

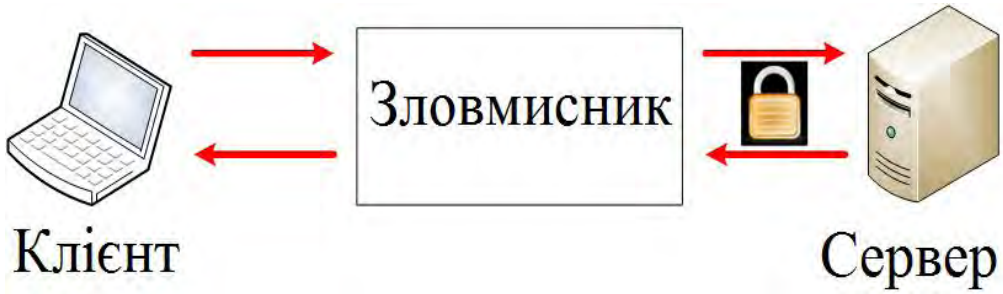

Рис. 1. Схема атаки "зловмисник посередині", також відома як MitM (Man-in-the-Middle)

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 через захищений канал, бачить зловмисника як клієнта, від якого приходить під'єднання, 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, використовують 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 недостатньо зосереджує увагу, використовуючи власну конфіденційну інформацію [3].

Під час такої атаки активно використовують логотипи захищених веб-сторінок, такі як піктограми замків золотистого або зеленого кольору, залежно від того, який браузер використовує жертва. Такі піктограми можна створити власноруч (рис. 2).

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

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

Дистрибутив Back-Track має бути налаштований на пересилання IP. Для цього виконується команда:

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

Після цього потрібно спрямувати весь трафік HTTP, який буде перехоплюватися, на порт, який прослуховуватиметься за допомогою інструменту SSLstrip. Для цього потрібно змінити конфігурацію міжмережевого екрана iptables так:

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 відбуватиметься 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 під'єднання 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 цього досліду вибрано 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 логіна та пароля, які, в цьому 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 відмінностей (рис.3).

а *б*

Рис. 3. Відмінності між захищеним оригінальним з'єднанням (а) та з'єднанням, яке створив зловмисник (б)

В результаті здійснення цієї атаки, через вразливість протоколу SSL, зловмисник отримує в режимі реального часу конфіденційні дані (тут логін та пароль) (рис. 4).

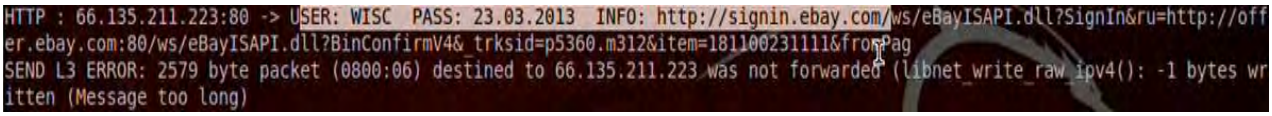

Рис.4. Отримання конфіденційних даних (логін та пароль) за допомогою дистрибутива Back-Track

Висновки

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

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

- Необхідно переконатися в тому, що використовується саме захищене HTTPS під'єднання для інтернет-банкінгу. Якщо використовується протокол HTTP замість HTTPS, висока ймовірність того, що щось не так.
- Незалежно від моделі браузера, необхідно вміти розрізняти захищені під'єднання і незахищені.
- Рекомендується виконувати свої мережеві банківські операції вдома – шанси того, що хтось перехопить трафік у 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, переходячи на захищені веб-сторінки – набирати повний URL вручну.

1. Воронін А. Електронний банкінг та ризики його використання // Фінансовий ринок України – 2009. – № 1. – С. 8–9. 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.