Міністерство освіти і науки України
Національний Технічний Університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

Комп'ютерний практикум 3
з дисципліни
«Проектування, розробка і реалізація криптографічних систем»
Тема:
«Дослідження криптографічних протоколів
систем WebMoney, PayPal»

Виконав:
Студент групи ФІ-22мн
Кушнір Олександр
Перевірив:
Селюх П. В.

Київ – 2023

WebMoney

Окрім стандартних протоколів, які актуальні для будь-яких сучасних сервісів та платіжних систем, WebMoney наділений досить унікальною процедурою. E-num – це система авторизації, що надає доступ до сервісів WebMoney Transfer за допомогою секретного ключа (унікального шифроблокнота), який зберігається в мобільному пристрої (телефон, смартфон, планшет) учасника. Система дозволяє зберігати ключі програми WM Keeper у своїй базі даних (E-num Storage), що дозволяє безпечно користуватися своїми електронними гаманцями, а також сервісами WebMoney практично на будь-якому комп'ютері.

Авторизація відбувається за схемою "Питання-відповідь" наступним чином:

- На сторінці сайту (або у програмі), яка передбачає захищений доступ, учасник бачить свій email, далі відображається число-питання;
- Учасник запускає у своєму телефоні мобільний клієнт E-num, програму WM Keeper для Android або WM Keeper для iOS та вводить число-питання. Після введення на дисплеї телефону відображається число-відповідь;
- Учасник вводить число-відповідь у полі авторизації на сайті (або у програмі WM Keeper) та отримує доступ до захищених розділів сайтів або підтверджує виконання операції (переведення коштів, додавання кореспондента та ін.).

Сервіс E-num надає учасникам такі можливості:

- Реєструватися у системі, проводити налаштування, відновлювати доступ;
- Використовувати додатковий безпечний спосіб входу до WM Keeper;
- Підтверджувати авторизацію на сервісах WebMoney під час виконання важливих операцій;
- Підтверджувати перекази коштів, оплату послуг та проведення інших операцій у WM Keeper;

Також WebMoney використовує систему персональних сертифікатів. Персональний (особистий, клієнтський) цифровий сертифікат X.509 у системі WebMoney Transfer призначений для захисту, ідентифікації та передачі даних при інтернет-з'єднаннях WM Keeper WebPro. Використовуються сертифікати стандарту X.509.

Ідентифікація забезпечується шляхом застосування закритого ключа, що генерується на комп'ютері користувача в процесі реєстрації, зберігається лише у власника персонального цифрового сертифіката WM Keeper WebPro і ніколи не передається через мережу.

Персональний цифровий сертифікат засвідчує власника WM-ідентифікатора на сайтах сервісів WebMoney Transfer, а також на інших сайтах, на яких встановлена система авторизації WebMoney Transfer.

Встановлення персонального сертифіката є частиною процесу реєстрації WM Keeper WebPro і можливе у різних браузерах:

- Microsoft Internet Explorer
- Mozilla Firefox ESR
- macOS Safari

Після успішної реєстрації можливе використання персонального сертифіката WM Keeper WebPro у наступних браузерах:

- Google Chrome
- Opera
- Safari
- Konqueror
- K-Meleon

Також можливе отримання клієнтського сертифіката після реєстрації WM Keeper WebPro з використанням логіну та пароля з E-num або SMS підтвердженням, а також після зміни основного способу керування WM Keeper Standard на WM Keeper WebPro. Персональний сертифікат діє два роки, після чого його необхідно оновлювати (продовжувати).

PayPal

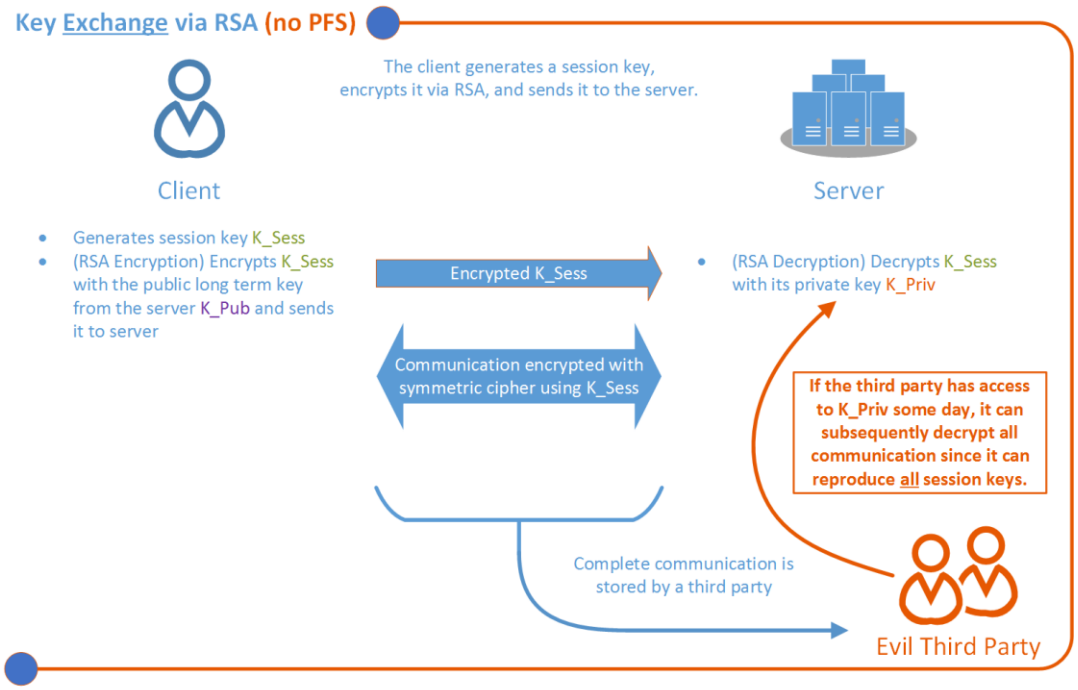
Аналогічно окрім звичайних SSL/TLS є ще й унікальні системи захисту. Perfect Forward Secrecy (PFS) розроблений для запобігання компрометації довгострокового секретного ключа та впливу на конфіденційність минулих чи майбутніх розмов. Ми рекомендуємо вам реалізувати PFS у вашій інтеграції.

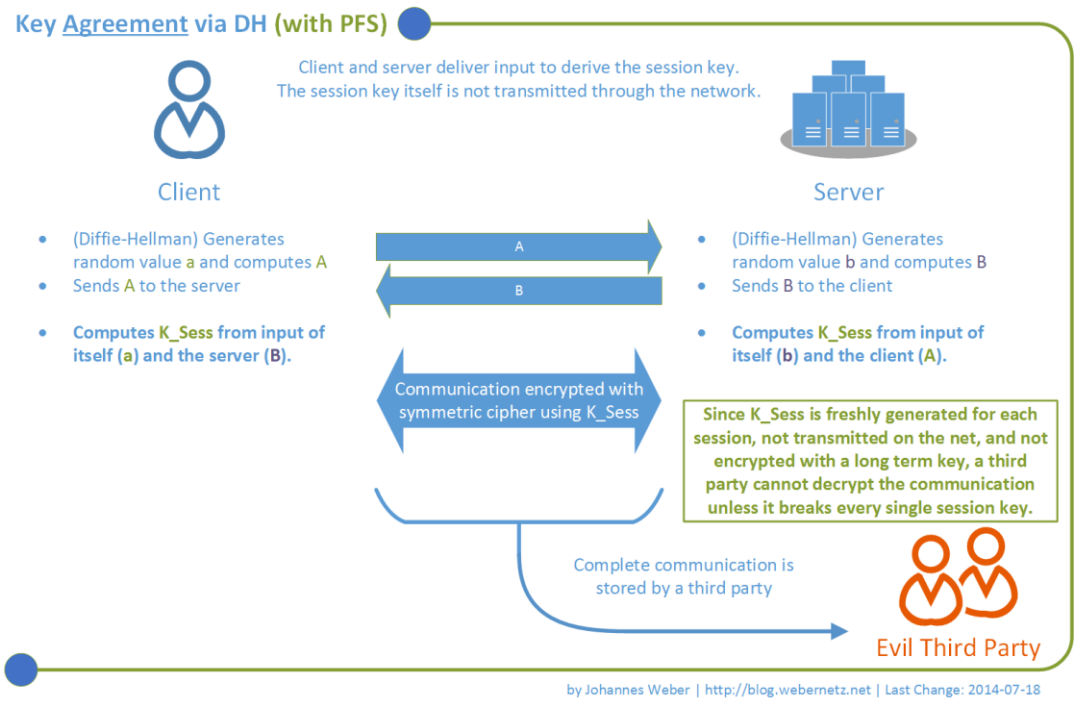
Завдяки впровадженню PFS будь-які захищені передачі, записані вами в минулому, як і раніше, безпечні і не можуть бути скомпрометовані, навіть якщо поточний ключ скомпрометований. Те саме справедливо і для майбутніх передач. Без PFS, якщо одна передача буде скомпрометована, всі попередні та майбутні передачі можуть бути скомпрометовані.

При реалізації PFS вам необхідно дозволити протоколу узгоджувати найвищу версію TLS і ніколи не використовувати жорстко закодовані спеціальні шифри. Коли PFS увімкнено, узгодження протоколу TLS здійснюється на стороні PayPal. Обов'язково не обмежуйте у своїй інтеграції шифри Діффі-Хеллмана з обміном ключами (DHE) або еліптичною кривою Діффі-Хеллмана (ECDHE).

Perfect Forward Secrecy (PFS) Overview

Difference between no PFS (with RSA) and PFS (with DH) in TLS/SSL/IPsec Connections





by Johannes Weber | http://blog.webernetz.net | Last Change: 2014-07-18

PayWord and MicroMint

PayWord працює на основі кредитів. Користувач створює обліковий запис у брокера, який видає йому сертифікат PayWord із цифровим підписом, що містить ім'я брокера, ім'я та IP-адресу користувача, відкритий ключ користувача, термін дії та іншу інформацію. Сертифікат має бути поновлений брокером (наприклад, щомісяця), який зробить це, якщо обліковий запис користувача має добру репутацію. Цей сертифікат дає користувачеві право створювати ланцюжки Payword і гарантує постачальникам, що брокер може використати Paywords.

Фундаментальна конструкція PayWord полягає в тому, щоб звести до мінімуму спілкування (особливо в режимі онлайн) з брокером. Ми припускаємо, що буде лише кілька загальнонаціональних брокерів; щоб запобігти тому, щоб вони стали вузьким місцем, важливо, щоб їхнє обчислювальне навантаження було розумним і «офлайновим». Таким чином, PayWord надзвичайно ефективний, коли користувач робить повторні запити від того самого постачальника, але в будь-якому випадку досить ефективний. Операції з відкритим ключем, які вимагає V, це лише перевірка підпису, яка є відносно ефективною. Зауважимо, що ймовірнісні методи скринінгу сигнатур Шаміра можна використовувати тут, щоб ще більше зменшити обчислювальне навантаження на постачальника. Ще одна програма, для якої добре підходить PayWord, — це придбання фільмів з оплатою за перегляд; користувач може платити кілька центів за кожну хвилину часу перегляду.

MicroMint розроблено для забезпечення розумної безпеки за дуже низькою ціною та оптимізовано для непов'язаних платежів малої вартості. MicroMint взагалі не використовує операції з відкритим ключем. «Монети» MicroMint виготовляються брокером, який продає їх користувачам. Користувачі віддають ці монети постачальникам як оплату. Продавці повертають монети брокеру в обмін на оплату іншими способами. Монета — це бітовий рядок, дійсність якого може легко перевірити будь-хто, але яку важко створити. Це схоже на вимоги до підпису відкритого ключа, складність якого робить його надмірним для транзакції, вартість якої становить один цент. (PayWord використовує підписи, але не для кожної транзакції.)