Introduction to Cryptography

Homework 6

0510002 袁鈺勛

A. Overview

在取得他人的公鑰進行加密或簽章確認時，不一定能確認拿到的就是想要的使用者的公鑰，所以要透過一個可信任的 CA，以 CA 的私鑰對使用者的公鑰簽章，將此簽章和使用者的公鑰組成憑證，當我們想要用此使用者的公鑰時，就可以透過 CA 的公鑰解開憑證來比對取得的使用者公鑰和 CA 簽的公鑰是不是同一個，以確認公鑰是不是來自正確的使用者，而不是中間的攻擊者。

B. Certificates

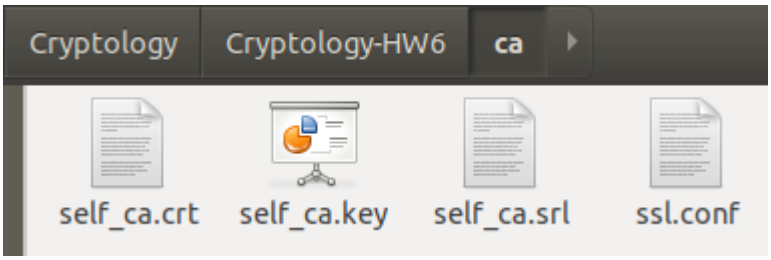
1. 建立 CA 的金鑰

```
user@user-VirtualBox:~/Cryptology/Cryptology-HW6/ca$ openssl genrsa -des3 -out self_ca.key 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
.........................++++
.....................................................++++
e is 65537 (0x010001)
Enter pass phrase for self_ca.key:
Verifying - Enter pass phrase for self_ca.key:
```

2. CA 自簽憑證

```
user@user-VirtualBox:~/Cryptology/Cryptology-HW6/ca$ openssl req -x509 -new -nodes -key self_ca.key -sha256 -days 3650 -out self_ca.crt -config ssl.conf
Enter pass phrase for self_ca.key:
```

3. 目前 CA 的文件



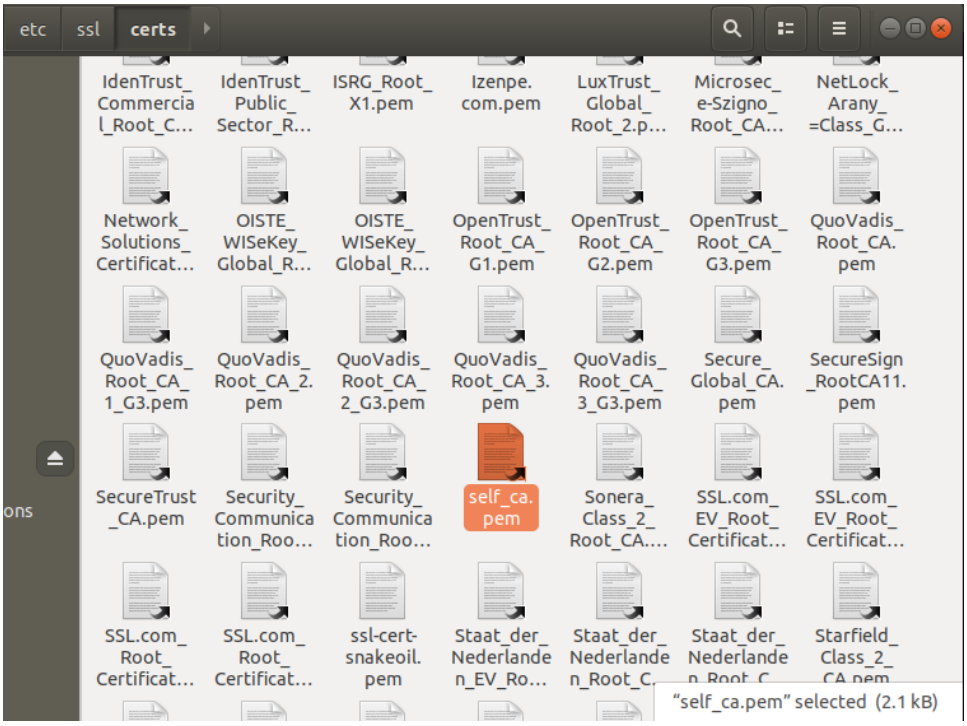
4. 查看 CA 憑證內容

```
user@user-VirtualBox:~/Cryptology/Cryptology-HW6/ca$ openssl x509 -text -noout -in self_ca.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            5a:49:e0:19:3e:ed:8c:31:49:39:5f:18:2b:e5:f4:12:6e:ac:00:c9
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = TW, ST = Hsinchu, L = Hsinchu City, O = National Chiao Tung University, OU = EECS, emailAddress = steven112163@gmail.com, CN = Yu-Hsun Yuan
        Validity
            Not Before: Jun 17 08:08:22 2019 GMT
            Not After : Jun 14 08:08:22 2029 GMT
        Subject: C = TW, ST = Hsinchu, L = Hsinchu City, O = National Chiao Tung University, OU = EECS, emailAddress = steven112163@gmail.com, CN = Yu-Hsun Yuan
```

5. 安裝 CA 的憑證到電腦中

```
user@user-VirtualBox:~/Cryptology/Cryptology-HW6/ca$ sudo cp self_ca.crt /usr/share/ca-certificates/
[sudo] password for user:
user@user-VirtualBox:~/Cryptology/Cryptology-HW6/ca$ sudo dpkg-reconfigure ca-certificates
Updating certificates in /etc/ssl/certs...
1 added, 0 removed; done.
Processing triggers for ca-certificates (20180409) ...
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
```

6. 可以在電腦中確認到已安裝的 CA 憑證



7. 建立使用者的金鑰

```
user@user-VirtualBox:~/Cryptology/Cryptology-HW6/user$ openssl genrsa -des3 -out self_my.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
..+++++
....+++++
e is 65537 (0x010001)
Enter pass phrase for self_my.key:
Verifying - Enter pass phrase for self_my.key:
```

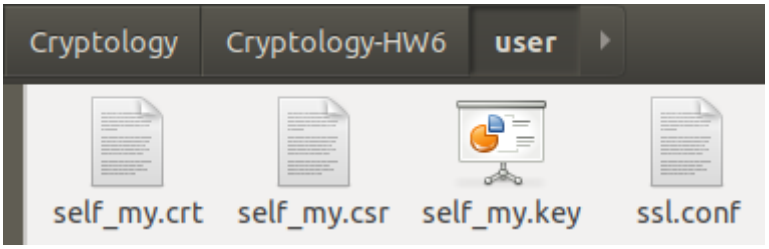
8. 產生使用者的憑證簽署要求

```
user@user-VirtualBox:~/Cryptology/Cryptology-HW6/user$ openssl req -new -key self_my.key -out self_my.csr -config ssl.conf
Enter pass phrase for self_my.key:
```

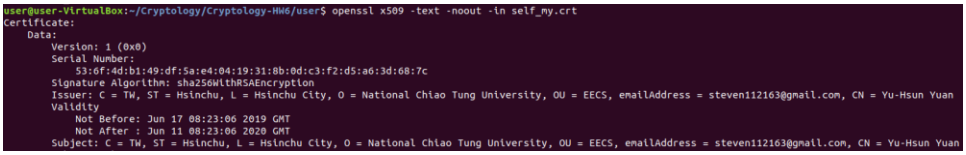
9. CA 簽屬使用者憑證

```
user@user-VirtualBox:~/Cryptology/Cryptology-HW6/user$ openssl x509 -req -days 360 -in self_my.csr -CA ../ca/self_ca.crt -CAkey ../ca/self_ca.key -CAcreateserial -out self_my.crt
Signature ok
subject=C = TW, ST = Hsinchu, L = Hsinchu City, O = National Chiao Tung University, OU = EECS, emailAddress = steven112163@gmail.com, CN = Yu-Hsun Yuan
Getting CA Private Key
Enter pass phrase for ../ca/self_ca.key:
```

10. 目前使用者的文件



11. 確認 CA 簽屬使用者憑證的內容



C. Application

最常見使用憑證的協定便是 HTTPS，他是在 TLS/SSL 上傳輸的 HTTP，但在上面傳輸的資料會經過加密。在使用者一開始連到網站時，網站要將自己的憑證傳給使用者，瀏覽器會以此憑證去驗證這網站的公鑰，如果通過，瀏覽器才會用這把公鑰進行接下來的加密，如果不通過，瀏覽器會認為這個網站是不安全的，並警告使用者。