CSE-C3400 Information security
Examination 2015-10-22
Lecturer: Tuomas Aura

No electronic equipment or reference material is allowed in the examination.

1. Access control

The family Linux computer has five users: the parents Alice and Bob, and the children Carol, David and Emil. Alice is the system administrator. She has set up user groups for the parents and children. Here is the output of the `ls -l` command on some folder on the computer:

```
-rw-r-----   1 alice  parents      22136 21 Jun 05:06 abc.doc
-rw-r-----   1 bob    children      5408 26 Mar  2013 jokes.txt
-rw-r-----   1 david  children  71224238 10 Jul 20:52 party.mpeg
-rw----r--   1 carol  children   1943593 14 Aug 10:11 selfie.jpg
-r--r--r--   1 bob    parents      1022 18 Aug 12:55 test.txt
```

Problem:

(a) Show the protection state for the above objects in the form of access control lists where the subjects are the individual users.

(b) How can David prevent little Emil from watching the movie from his party, without making other changes?

2. Encrypted storage

Consider disk encryption solutions that do not require user interaction or input during a reboot, for example, after a security update or power outage. Compare such solutions based on (a) encryption built into the disk drive hardware or firmware, (b) solution where the master key is sealed by a TPM, and (c) purely software-based solution. In your answer, explain briefly the threats and attack scenarios that are significant for the comparison. You can base your answer on BitLocker.

3. User authentication

Our immensely popular *potplant* service has one million users, who have to select 12-character passwords. The character set for the passwords is the following:

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890-+

The service stores the passwords in a database as hash values. The hash function is SHA-256, which is computed on the concatenation of string "potplant" and the password and then truncated to 16 bytes:

$$hash = leftmostbytes(\ SHA\text{-}256\ (\text{“potplant”} \mid password),\ 16\ )$$

The attacker has obtained the user and password database with an SQL injection attack and mounts a brute-force attack on the hashes. The attacker is using an array of top-end GPUs, which each can compute 1000 million (10^9) SHA-256 hashes per second. The price of a GPU day is approximately $1 including the hardware, electricity and other costs. Based on this information, how much does it cost to crack:

Please turn the paper for the remaining parts of the examination.

(a) the password of the user *alice,*
(b) the password of at least one user,
(c) all the passwords?

Later, we decide to improve the password hash function by adding the username to the hash input and by saving the full 32-byte hash values, and we require all users to log in once so that the hashes can be upgraded to the new version.

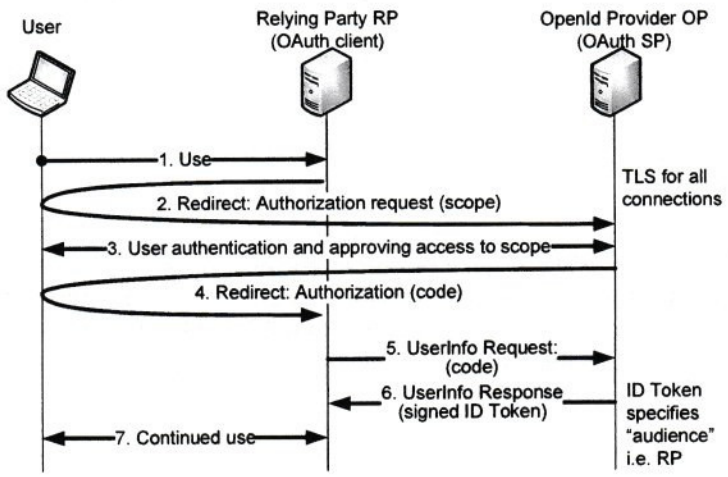
hash = SHA-256 ("potplant" | username | password)

(d) How does the cost of the attack change for cases (a)–(c) as the result of this improvement?

Since you do not have a pocket calculator, a rough estimate is ok. However, please write down the intermediate steps of the calculation. (1 day = 86 400 s)

4. Identity management

The picture below shows the message flow in OpenId Connect:



Answer the following questions:

(a) How would the security be affected if TLS were not used for the connection between User and OP?
(b) How would the security be affected if TLS were not used for the connection between User to RP?
(c) How would the security be affected if the ID Token did not contain an RP identifier (the "audience" information)?
(d) How does the meaning of "open" in OpenId Connect compare with the earlier versions of OpenId?

5. X.509 PKI

The certificate chain below (see the third page) was received by a web browser from gmail. It has been pretty-printed with the *openssl* tool. Explain in detail how the web browser checks the certificate chain and how it is used to authenticate the web site in SSL or TLS. Please refer to the specific certificate fields in your answer. For clarity, refer to the three certificates as C1, C2 and C3. (Note: You do not need to write out the messages of the SSL/TLS handshake.)

Certificate C1:

```
    Data:
        Version: 3 (0x2)
        Serial Number: 5034357460863282341
(0x45dda16fff17eca5)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Google Inc, CN=Google Internet
Authority G2
        Validity
            Not Before: Oct  7 11:10:51 2015 GMT
            Not After : Jan  5 00:00:00 2016 GMT
        Subject: C=US, ST=California, L=Mountain View,
O=Google Inc, CN=mail.google.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
00:96:db:37:d0:56:cf:f9:1d:76:74:eb:f3:b1:ed:
...many more bytes...
01:db
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web
Client Authentication
            X509v3 Subject Alternative Name:
                DNS:mail.google.com,
DNS:inbox.google.com
            Authority Information Access:
                CA Issuers -
URI:http://pki.google.com/GIAG2.crt
                OCSP -
URI:http://clients1.google.com/ocsp

            X509v3 Subject Key Identifier:

37:DB:18:BA:07:20:3C:DA:A6:B1:9F:C2:5C:4C:6C:85:7C:B2:6
B:E0
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Authority Key Identifier:

keyid:4A:DD:06:16:1B:BC:F6:68:B5:76:F5:81:B6:BB:62:1A:B
A:5A:81:2F

            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.11129.2.5.1
                Policy: 2.23.140.1.2.2

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://pki.google.com/GIAG2.crl

    Signature Algorithm: sha256WithRSAEncryption

64:be:a0:00:54:57:c3:32:0f:c0:3e:63:19:e4:b4:96:56:8b:

ea:66:98:96:38:47:f5:85:cd:cf:da:25:19:a7:ba:5b:
...many more bytes...
8c:e8:ad:b9:21:67:ed:85:45:8a:a1:94:5d:04
```

Certificate C2:

```
    Data:
        Version: 3 (0x2)
        Serial Number: 146051 (0x23a83)
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=GeoTrust Inc., CN=GeoTrust
Global CA
        Validity
            Not Before: Apr  5 15:15:56 2013 GMT
            Not After : Dec 31 23:59:59 2016 GMT
        Subject: C=US, O=Google Inc, CN=Google Internet
Authority G2
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:

00:9c:2a:04:77:5c:d8:50:91:3a:06:a3:82:e0:d8:
...many more bytes...
72:69
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
keyid:C0:7A:98:68:8D:89:FB:AB:05:64:0C:11:7D:AA:7D:65:B
8:CA:CC:4E

            X509v3 Subject Key Identifier:

4A:DD:06:16:1B:BC:F6:68:B5:76:F5:81:B6:BB:62:1A:BA:5A:8
1:2F
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            Authority Information Access:
                OCSP - URI:http://g.symcd.com

            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 CRL Distribution Points:

                Full Name:

URI:http://g.symcb.com/crls/gtglobal.crl

            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.11129.2.5.1

    Signature Algorithm: sha256WithRSAEncryption

aa:fa:a9:20:cd:6a:67:83:ed:5e:d4:7e:de:1d:c4:7f:
...many more bytes...
7e:c8:35:d8
```

Certificate C3:

```
    Data:
        Version: 3 (0x2)
        Serial Number: 1227750 (0x12bbe6)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=Equifax, OU=Equifax Secure
Certificate Authority
        Validity
            Not Before: May 21 04:00:00 2002 GMT
            Not After : Aug 21 04:00:00 2018 GMT
        Subject: C=US, O=GeoTrust Inc., CN=GeoTrust
Global CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:

00:da:cc:18:63:30:fd:f4:17:23:1a:56:7e:5b:df:
...many more bytes...
e4:f9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:

keyid:48:E6:68:F9:2B:D2:B2:95:D7:47:D8:23:20:10:4F:33:9
8:90:9F:D4

            X509v3 Subject Key Identifier:

C0:7A:98:68:8D:89:FB:AB:05:64:0C:11:7D:AA:7D:65:B8:CA:C
C:4E
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 CRL Distribution Points:

                Full Name:

URI:http://crl.geotrust.com/crls/secureca.crl

            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS:
https://www.geotrust.com/resources/repository

    Signature Algorithm: sha1WithRSAEncryption

76:e1:12:6e:4e:4b:16:12:86:30:06:b2:81:08:cf:f0:
...many more bytes...
3f:12
```