CSE-C3400 Information security
Examination 2016-04-04
Lecturer: Tuomas Aura

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

1. Security terminology

Explain the meaning of the following terminology (max 15 words each):

(a) Covert channel
(b) Handshake and session protocol
(c) SUID bit (in Linux file system)

2. Access control

Explain the Bell-LaPadula and Biba security models and give examples of where each security property is needed.

3. Data encryption

Design a client-based file encryption system for files stored in Dropbox, OneDrive or a similar cloud storage service. In your design, specify what keys and cryptographic algorithms are used, and what is encrypted or signed. The security goal is to protect confidentiality of the file contents in the cloud storage. It should be possible to share files between users and to revoke access to the shared files. Each user trusts his or her own client computer and the software on it, but the storage server should not be able to learn the file contents.

4. Threat analysis

An amusement park uses wrist band tickets. The tickets are priced differently for under and over 15 year olds. The ticket is valid for unlimited rides during one day within a year from the purchase. Tickets are read with a bar code scanner before each ride. What security threats and potential vulnerabilities there are in this system? Give also your estimate of what are the most serious threats from the point of view of the amusement park business.

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.)

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

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
```