CS-C3130 Information security
Examination 2016-12-14
Lecturer: Tuomas Aura

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

1. Security terminology

Give an example of each of the following concepts:

a) trusted path
b) low water mark policy
c) separation of duty
d) covert channel
e) parameterized role
f) principle of least privilege

Note: No definitions! Give an example that is clearly related to a real system or application.

2. Authentication

A mechanical combination lock has between 3 and 6 wheels, each with the digits 0–9. To open the lock, one needs to align the right numbers on one line.

a) What is the entropy of the secret key information for 3-wheel and 6-wheel locks?
b) If it takes one second for a brute-force attacker to try one combination, how long will it take to open the 3-wheel and 6-wheel locks?
c) The mechanical combination lock is replaced with a new electronic design, which has the same physical form but an electronic mechanism inside. How could the security of the electronic lock be improved compared to the mechanical one?

It is sufficient to perform the numerical calculations approximately but please write down your calculations.

Please turn the paper for the remaining problems.

3. Identity management

Aalto university uses Shibboleth 2.0 for authenticating students and staff to online services such as MyCourses and Oodi. Alice, who is a student at Aalto, starts a web browser and logs into a new service at *https://noob.aalto.fi/*. Explain how the Shibboleth 2.0 authentication works in this case. The explanation should cover the communication channels, protocol messages, trust relations and security mechanisms and link them to what the user sees.

Explain just one possible login process; no need to cover many variations. Note that you can get points for explaining the operating principle in an understandable way even if you don't remember the exact terminology or all details.

4. Threat analysis

Many computer users have started to cover the built-in camera on their mobile computer with a piece of opaque adhesive tape. You work at the IT services department of a medium-size technology company. Your boss asks you to analyze the threats created by the cameras on computers and mobile devices in the workplace. Present a summary of your analysis.

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 protocol.)

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
:6B: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
:BA: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
:B8: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
:81:2F
            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
:98:90:9F:D4

            X509v3 Subject Key Identifier:

C0:7A:98:68:8D:89:FB:AB:05:64:0C:11:7D:AA:7D:65:B8:CA
:CC: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
```