CSE-C3400 Information security
Examination 2015-10-09
Lecturer: Tuomas Aura

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

1. Access control

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

(a) Reference monitor
(b) Covert channel
(c) Bell-LaPadula *-property
(d) Chinese wall policy
(e) Access token (in Windows processes)
(f) SUID bit (in Linux file system)

2. Payment systems

Explain the technical reasons for the following:

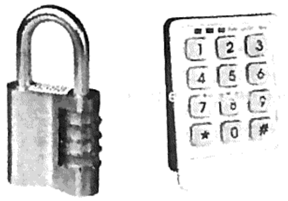
(a) *Static data authentication* (SDA) as payment-card authentication method is not considered secure, and Finnish banks require *dynamic data authentication* (DDA) to be used.
(b) The idea of contactless payment is to make the transactions really fast and smooth: the card holder just taps the NFC-enabled payment terminal with the payment card. Nevertheless, the terminals must have a PIN pad.
(c) If Bitcoin replaces all or most of the world's currencies, deflation is inevitable.

(Background information: Deflation is defined as a decrease in the general price level of goods and services. Note that the European Central Bank currently sees deflation as one of the biggest threats to economy. Advocates of Bitcoin or gold standard naturally disagree.)

3. Authentication

A mechanical combination lock has 3 to 6 wheels, each with digits 0–9. In order 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? Give an approximate numerical answer including the unit.
b) The mechanical combination locks are replaced with a new electronic lock, which has a PIN pad and a connection to a backend server. You are asked to help designing the new lock system. How can the security of the electronic lock be improved compared to the mechanical one?

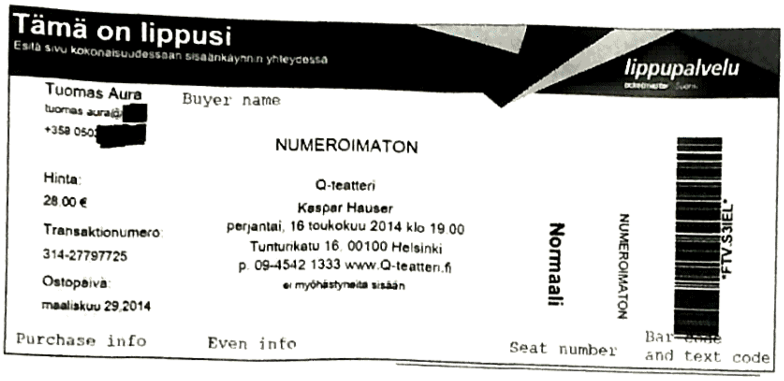


Notes for part (b): You do *not* need to consider mechanical or software flaws in your answer. There are many potential improvements, and you need to cover many of most significant ones for full points.

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

4. Threat analysis

Theater and concert tickets can be bought in an online shop and printed at home. The most important part of the ticket is a bar code or a short text code. At the entrance to the event, this code is scanned electronically by the security personnel. The ticket has the buyer's name on it, but it is acceptable to give the ticket to another person. Analyze the threats against such tickets.



Tämä on lippusi

Esitä sivu kokonaisuudessaan sisäänkäynnin yhteydessä

lippupalvelu

ticketmaster Suomi

Tuomas Aura

tuomas.aura@[redacted]

+358 050[redacted]

Buyer name

NUMEROIMATON

Hinta:

28.00 €

Transaktionumero:

314-27797725

Ostopäivä:

maaliskuu 29.2014

Q-teatteri

Kaspar Hauser

perjantai, 16 toukokuu 2014 klo 19.00

Tunturikatu 16, 00100 Helsinki

p. 09-4542 1333 www.Q-teatteri.fi

ei myöhästyneitä sisään

Normaali

NUMEROIMATON

FTV.S3IEL

Purchase info

Even info

Seat number

Bar code and text code

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: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
```