CS-C3130 Information security
Examination 2019-10-24
Lecturer: Tuomas Aura

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

0. Please give the following information honestly. It will not affect the grading.

(a) How many of the 12 lectures did you attend?
(b) How many of the 12 lecture videos did you watch?

1. Access control

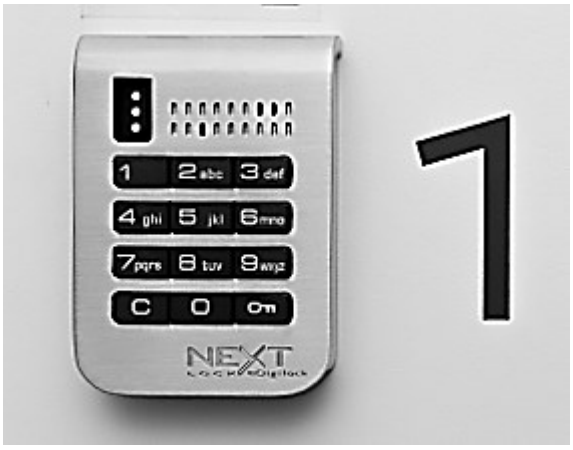
The project computer has the following four users and their files:

```
$ groups alice bob carol david
alice : users team-a
bob : users team-b
carol : users team-a
david : users sudo team-b

$ ls -l project
total 8
-rwxr--r-x 1 alice users   129 Oct 22 02:55 beep.sh
-r--r----- 1 bob   team-a 4113 Oct 22 02:55 doc.txt
-rw-r--r-- 1 carol team-a 5442 Oct 22 02:55 notes.txt
-rwsr-x--x 1 bob   team-b 8168 Oct 22 02:55 run
```

Show the protection state for the above objects in the form of an access control matrix. If the matrix does not give a complete picture of who has or can gain access to the objects, add an explanation. (6p)

2. Authentication



Posti Parcel Lockers are a popular way to receive packets from online stores. Posti sends the locker location and a 6-digit code in a text message to the recipient's phone. To open the locker, the recipient enters the code on a keypad in the locker door. The lock itself if a simple battery-operated code lock with no network connection. The postman uses a programming device to set a new code for every delivered packet.

(a) What is the entropy of the code? Please include the unit in your answer. (2p)

(b) Analyze the difficulty of code-guessing attacks against the code locks. (2p)

(c) How could you improve the security of the code lock with software changes, without connecting the lock to the Internet or making other physical changes? (2p)

The exam continues on pages 2-4.

3. Security protocols

In one of the course exercises, an IoT device accepted commands of the following format:

<user>;<command>;<hmac>

where the <hmac> is a hexadecimal representation of the HMAC-SHA256 hash value computed from the following string concatenation:

hmac("ClientCmd|" + user + "|" + command)

Let us assume that the software vulnerabilities present in the exercise have been fixed.

(a) Explain how an attacker can exploit a flaw in the protocol design to send unauthorized commands to the device. (3p)

(b) Present an improved protocol that prevents the attacks. Explain also the costs and limitations of your solution. (3p) Note: There are many possible solutions. Explain only one of them.

4. Data encryption

In your role as a penetration tester, you have been asked to infiltrate the Euro Shopper factory and retrieve the secret energy drink formula from a computer in the factory control room. You have taken a job in the factory as cleaner. This allows you to roam the facility with relative freedom in the evenings, after everyone else goes home. You cannot enter during work hours. So far, you have discovered the location of the computer. It is a desktop PC that runs Windows, and the factory employees power down the computer before leaving work. Next, you sneak into the office in the evening and power up the computer. The following text appears on the screen: "*BitLocker – Enter the PIN to unlock this drive*".

Problem: What different ways are there for you to get access to the secret files, preferably without getting caught? (6p)

You may also get some points for explaining why certain methods do not work.

5. Web security

In Appendix 1, there is a pretty-printed certificate chain. Explain in detail how the web browser checks the certificate chain and how the browser uses it to authenticate the website in TLS. (6p)

Notes: You do not need to explain the details of the TLS handshake protocol. Also, "rsaEncryption" in this context means the RSA algorithm for any purpose, which may be encryption or signature.

Appendix 1

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:06:00:09:c7:d9:5f:d1:22:f9:29:e8:58:ea:00:f5:ff:c3
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3
        Validity
            Not Before: Aug 28 17:12:50 2019 GMT
            Not After : Nov 26 17:12:50 2019 GMT
        Subject: CN = infosec1.vikaa.fi
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:de:f5:b0:3b:25:31:50:a8:03:93:31:98:d2:82:
                    5a:74:27:5a:fc:c0:39:0a:22:11:62:f5:53:34:ad:
                    c9:2f:4e:9c:df:42:42:2c:6c:6c:74:67:e4:c0:39:
                    c0:2e:8f:3f:0d:bc:75:b3:9d:7b:ce:bf:0c:b9:5b:
                    8c:3e:59:dc:76:b4:47:72:60:6b:33:89:f9:28:29:
                    9c:49:a7:09:56:73:52:a7:6c:d5:20:e1:c2:33:c4:
                    66:c4:5a:65:98:d5:5e:84:b2:7e:34:e3:ef:58:b6:
                    a4:77:14:52:4c:66:79:2d:b5:98:a5:af:c9:8c:04:
                    92:57:d6:7d:0d:99:79:37:78:85:8e:29:bc:42:0d:
                    18:dc:f4:a4:9b:78:46:b9:82:89:7a:82:7c:0b:b7:
                    e7:3b:1a:f7:2c:64:36:14:67:95:10:47:e0:3d:74:
                    ef:08:ac:3e:2f:64:ab:4c:62:06:ee:23:6c:46:a9:
                    ad:70:e9:b9:9d:b5:7f:21:8d:68:59:64:38:b8:f0:
                    cd:30:0e:b9:13:6c:94:1f:54:65:e9:39:3d:8c:4a:
                    d8:8d:20:38:33:70:4b:1b:07:9d:1d:06:46:f3:a8:
                    32:d2:26:c6:d4:8b:19:51:e0:4d:99:a8:63:a4:13:
                    38:41:fb:ce:a2:72:0f:af:0b:0f:50:e7:6f:0c:1a:
                    95:73
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Key Identifier:
                FE:FF:02:B8:79:36:3F:E7:06:09:0D:24:EA:0A:AD:B3:B3:C4:27:35
            X509v3 Authority Key Identifier:
                keyid:A8:4A:6A:63:04:7D:DD:BA:E6:D1:39:B7:A6:45:65:EF:F3:A8:EC:A1

            Authority Information Access:
                OCSP - URI:http://ocsp.int-x3.letsencrypt.org
                CA Issuers - URI:http://cert.int-x3.letsencrypt.org/

            X509v3 Subject Alternative Name:
                DNS:infosec1.vikaa.fi, DNS:potplants1.vikaa.fi
            X509v3 Certificate Policies:
                Policy: 2.23.140.1.2.1
                Policy: 1.3.6.1.4.1.44947.1.1.1
                  CPS: http://cps.letsencrypt.org
            CT Precertificate SCTs:
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : 63:F2:DB:CD:E8:3B:CC:2C:CF:0B:72:84:27:57:6B:33:
                                A4:8D:61:77:8F:BD:75:A6:38:B1:C7:68:54:4B:D8:8D
                    Timestamp : Aug 28 18:12:50.812 2019 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:44:02:20:03:76:31:7D:1F:F4:88:A2:F9:A2:A0:AB:
                                FD:ED:AC:A8:6E:69:83:D4:90:10:F8:AF:37:0E:6F:42:
                                AF:C9:75:0D:02:20:2C:D6:23:5C:84:F0:6F:C0:29:FB:
                                D6:99:18:17:90:46:AD:17:4A:2D:21:2B:40:EA:7E:C0:
                                02:C1:55:60:52:19
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : 6F:53:76:AC:31:F0:31:19:D8:99:00:A4:51:15:FF:77:
                                15:1C:11:D9:02:C1:00:29:06:8D:B2:08:9A:37:D9:13
                    Timestamp : Aug 28 18:12:51.227 2019 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:46:02:21:00:A4:2C:16:35:94:37:F0:7B:59:E0:B9:
                                54:01:2E:5A:A9:87:83:3B:15:4D:E7:14:59:DE:A8:EC:
                                CB:5C:BD:B5:5E:02:21:00:CF:66:68:11:24:3A:6A:51:
                                40:87:5A:4D:A8:F1:FC:1F:D3:76:2C:03:BC:63:69:47:
                                32:16:24:96:50:85:98:F6
    Signature Algorithm: sha256WithRSAEncryption
         53:30:e5:e8:8a:cb:b5:dd:0d:0c:2a:94:f6:0b:0a:ab:ff:14:
```

```
          0d:2b:c0:a6:99:6d:50:bd:61:a1:4f:17:50:f0:7b:bb:83:b2:
          0f:0d:f1:d7:bf:f5:7a:ea:f8:38:b7:41:73:56:25:84:00:30:
          99:35:59:ad:2b:c6:91:f6:e3:ae:3d:ed:2c:f0:2d:64:4a:38:
          c9:8a:88:aa:ab:5a:1f:e2:b8:e8:8f:cc:37:86:93:74:cd:84:
          60:34:6b:fb:e0:70:e0:8a:c7:b8:72:e9:c1:13:fc:a4:05:f8:
          6e:f9:6c:fa:20:84:e6:e5:49:69:54:e6:f2:22:4e:8c:02:cb:
          50:8b:37:02:85:0f:66:13:64:97:fb:d7:c2:60:2b:e9:d4:22:
          cc:75:6d:fe:ec:70:dc:e5:33:03:f7:f6:38:a1:41:50:d9:0b:
          6a:7b:05:56:ec:2b:7d:2e:39:40:58:0a:3e:65:08:0f:f6:a2:
          32:8c:e0:49:32:3d:b1:c3:19:03:a2:ef:2e:9b:58:f8:f0:14:
          fd:a5:eb:25:4d:b8:f9:87:a7:28:6c:db:07:c9:f6:8f:94:6c:
          79:dc:34:fe:3b:76:5c:15:9a:f4:12:45:36:97:fb:a3:44:1b:
          e1:6c:87:80:42:4a:c5:64:98:b5:62:06:59:01:c9:fd:5d:6b:
          78:65:40:52


Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0a:01:41:42:00:00:01:53:85:73:6a:0b:85:ec:a7:08
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: O = Digital Signature Trust Co., CN = DST Root CA X3
        Validity
            Not Before: Mar 17 16:40:46 2016 GMT
            Not After : Mar 17 16:40:46 2021 GMT
        Subject: C = US, O = Let's Encrypt, CN = Let's Encrypt Authority X3
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:9c:d3:0c:f0:5a:e5:2e:47:b7:72:5d:37:83:b3:
                    68:63:30:ea:d7:35:26:19:25:e1:bd:be:35:f1:70:
                    92:2f:b7:b8:4b:41:05:ab:a9:9e:35:08:58:ec:b1:
                    2a:c4:68:87:0b:a3:e3:75:e4:e6:f3:a7:62:71:ba:
                    79:81:60:1f:d7:91:9a:9f:f3:d0:78:67:71:c8:69:
                    0e:95:91:cf:fe:e6:99:e9:60:3c:48:cc:7e:ca:4d:
                    77:12:24:9d:47:1b:5a:eb:b9:ec:1e:37:00:1c:9c:
                    ac:7b:a7:05:ea:ce:4a:eb:bd:41:e5:36:98:b9:cb:
                    fd:6d:3c:96:68:df:23:2a:42:90:0c:86:74:67:c8:
                    7f:a5:9a:b8:52:61:14:13:3f:65:e9:82:87:cb:db:
                    fa:0e:56:f6:86:89:f3:85:3f:97:86:af:b0:dc:1a:
                    ef:6b:0d:95:16:7d:c4:2b:a0:65:b2:99:04:36:75:
                    80:6b:ac:4a:f3:1b:90:49:78:2f:a2:96:4f:2a:20:
                    25:29:04:c6:74:c0:d0:31:cd:8f:31:38:95:16:ba:
                    a8:33:b8:43:f1:b1:1f:c3:30:7f:a2:79:31:13:3d:
                    2d:36:f8:e3:fc:f2:33:6a:b9:39:31:c5:af:c4:8d:
                    0d:1d:64:16:33:aa:fa:84:29:b6:d4:0b:c0:d8:7d:
                    c3:93
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            Authority Information Access:
                OCSP - URI:http://isrg.trustid.ocsp.identrust.com
                CA Issuers - URI:http://apps.identrust.com/roots/dstrootcax3.p7c
            X509v3 Authority Key Identifier:
                keyid:C4:A7:B1:A4:7B:2C:71:FA:DB:E1:4B:90:75:FF:C4:15:60:85:89:10
            X509v3 Certificate Policies:
                Policy: 2.23.140.1.2.1
                Policy: 1.3.6.1.4.1.44947.1.1.1
                  CPS: http://cps.root-x1.letsencrypt.org
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl.identrust.com/DSTROOTCAX3CRL.crl
            X509v3 Subject Key Identifier:
                A8:4A:6A:63:04:7D:DD:BA:E6:D1:39:B7:A6:45:65:EF:F3:A8:EC:A1
    Signature Algorithm: sha256WithRSAEncryption
         dd:33:d7:11:f3:63:58:38:dd:18:15:fb:09:55:be:76:56:b9:
         70:48:a5:69:47:27:7b:c2:24:08:92:f1:5a:1f:4a:12:29:37:
         24:74:51:1c:62:68:b8:cd:95:70:67:e5:f7:a4:bc:4e:28:51:
         cd:9b:e8:ae:87:9d:ea:d8:ba:5a:a1:01:9a:dc:f0:dd:6a:1d:
         6a:d8:3e:57:23:9e:a6:1e:04:62:9a:ff:d7:05:ca:b7:1f:3f:
         c0:0a:48:bc:94:b0:b6:65:62:e0:c1:54:e5:a3:2a:ad:20:c4:
         e9:e6:bb:dc:c8:f6:b5:c3:32:a3:98:cc:77:a8:e6:79:65:07:
         2b:cb:28:fe:3a:16:52:81:ce:52:0c:2e:5f:83:e8:d5:06:33:
         fb:77:6c:ce:40:ea:32:9e:1f:92:5c:41:c1:74:6c:5b:5d:0a:
         5f:33:cc:4d:9f:ac:38:f0:2f:7b:2c:62:9d:d9:a3:91:6f:25:
         1b:2f:90:b1:19:46:3d:f6:7e:1b:a6:7a:87:b9:a3:7a:6d:18:
         fa:25:a5:91:87:15:e0:f2:16:2f:58:b0:06:2f:2c:68:26:c6:
         4b:98:cd:da:9f:0c:f9:7f:90:ed:43:4a:12:44:4e:6f:73:7a:
         28:ea:a4:aa:6e:7b:4c:7d:87:dd:e0:c9:02:44:a7:87:af:c3:
         34:5b:b4:42
```