CS-C3130 Information Security
Examination 2021-10-28
Lecturer: Tuomas Aura

No reference materials, pocket calculators, or other auxiliary equipment are allowed in this examination.

1. Access control models

A government agency plans to implement access control strictly based on the mandatory Bell-LaPadula model. Here is some test data for evaluating the plan:

Operations: read, write

Labels: top secret > secret > confidential > unclassified

Clearances of employees:

Alice	secret
Bob	confidential
Carol	no clearance (=unclassified)

Classification of objects:

article.pdf	unclassified
project.doc	confidential
report.txt	top secret

(a) Present the protection state (i.e., current access rights) of the above test system in the form of an access-control matrix. Only include the subjects and objects listed above. (4p)

(b) Why is this model not entirely realistic to be deployed to production? (2p)

2. Password cracking

Acme Inc. has created a cloud-based online service where the users can register and set up a username and password. So far, they have one million (1000 000) registers users. The passwords are machine-generated random 12-character strings with the following character set:

```
01234  56789  ABCDE  FGHIJ  KLMNO  PQRST
UVWXY  Zabcd  efghi  jklmn  opqrs  tuvwx yz+/
```

The passwords are stored as hash values that are truncated to 128 bits:

```
hash = truncate(SHA-256(password), 128)
```

Sadly, the password database has leaked to the deep web where Wile E., a notorious hacker, has found it. He now plans do brute-force cracking on his new GPU.

Problem: How much does it cost, on average, for the attacker to crack at least one password? The attacker does not care which user's password it finds. (6p)

In addition to the result, show the calculation steps.

Useful data: Wily's gaming GPU can compute 4000 million SHA-256 hash values per second. One day (24h) of GPU usage costs about $1 considering that the price of the GPU is spread over a three-year lifetime. One day is 24*60*60 = 86400 seconds.

3. Trusted path

Alice keeps secret data on a well-managed web server in her office. She connects to the server address `https//alice.vikaa.fi/` from a web browser on her notebook computer. She authenticates herself by entering her username `alice` and a very strong password. She can then browse the secret data on the server.

Problem: Explain possible security vulnerabilities related to *trusted path* (or *secure path*) in this system. (6p)

Definition from lecture notes: Trusted path is any mechanism that ensures direct and secure communication between the user and a trusted part of the system.

4. Threat analysis

Student dormitory plans to change all door locks to be electronic and centrally managed. Access control lists in the locks are updated over a wireless network. Each person receives a RFID key fob. When the key is placed near the lock (less than 5 cm), the lock first authenticates the key and then checks the access control list. If both steps are successful, the door can be opened by turning the handle.

Problem: Analyze the threats against the electronic lock system. 6p

Photo: Abloy

5. Web security

In Appendix 1, there is a pretty-printed certificate chain. Explain in detail how the web browser checks this specific 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.

Appendix 1

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:67:06:55:ab:72:81:9c:45:49:52:91:fa:75:66:c7:0e:41
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = Let's Encrypt, CN = R3
        Validity
            Not Before: Sep 19 02:50:12 2021 GMT
            Not After : Dec 18 02:50:11 2021 GMT
        Subject: CN = tietokilta.fi
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:b5:29:4e:76:e6:9f:cc:0c:86:d8:4b:5b:54:cd:
                    88:18:86:cb:c1:11:a8:08:ce:01:38:36:08:43:35:
                    56:df:78:07:d1:aa:fb:66:4d:48:34:ac:e7:08:6b:
                    64:9d:4e:ca:5d:b7:13:a7:ee:ab:e4:96:08:aa:7c:
                    bd:03:58:31:22:a5:51:fc:b3:c1:cb:06:75:af:ff:
                    3d:d9:fc:03:06:4c:60:01:b6:ca:57:bf:8c:46:23:
                    1f:4c:a0:f4:95:ab:19:fb:f9:aa:7d:18:12:d4:1b:
                    ce:ea:11:3c:74:34:56:94:55:7c:72:56:71:86:cb:
                    35:e0:7c:76:61:8c:00:7e:f9:6d:21:27:31:7a:2d:
                    69:f9:22:a2:fa:5a:a1:63:68:1f:9f:66:4e:d7:b5:
                    38:eb:b0:9e:ae:d3:0f:71:48:4c:31:a7:cc:00:c1:
                    3c:9e:23:31:fc:b6:77:a4:73:e7:97:e6:b5:9c:f9:
                    81:b3:56:db:71:c0:2c:8b:65:44:16:6e:c6:d3:78:
                    d7:76:cb:46:92:e1:2d:46:a0:bd:4e:c6:54:48:d9:
                    81:63:6c:cd:59:a8:f8:78:15:b4:bd:23:d2:89:78:
                    ee:98:c1:fe:37:7c:48:62:e0:bd:47:94:c4:cc:bb:
                    fa:89:b0:cd:21:35:11:d8:2d:5b:f4:d2:10:ac:0c:
                    83:4d
                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:
                6E:CA:C3:E3:34:41:29:70:C8:F8:21:1A:90:27:7D:A6:61:64:DF:0B
            X509v3 Authority Key Identifier:
                keyid:14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6

            Authority Information Access:
                OCSP - URI:http://r3.o.lencr.org
                CA Issuers - URI:http://r3.i.lencr.org/

            X509v3 Subject Alternative Name:
                DNS:tietokilta.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    : 44:94:65:2E:B0:EE:CE:AF:C4:40:07:D8:A8:FE:28:C0:
                                DA:E6:82:BE:D8:CB:31:B5:3F:D3:33:96:B5:B6:81:A8
                    Timestamp : Sep 19 03:50:12.544 2021 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:44:02:20:5E:40:35:45:4A:62:53:A0:CF:85:DA:83:
                                3D:D9:14:29:DC:23:6C:EA:8F:F2:9D:A7:C4:02:2A:B2:
                                BA:56:7B:A0:02:20:24:A4:9F:4F:C2:39:AA:90:9C:68:
                                3D:2F:BE:D7:06:94:E5:CD:E8:F6:76:21:0E:65:8E:4B:
                                DF:58:C7:D6:D3:B9
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : 7D:3E:F2:F8:8F:FF:88:55:68:24:C2:C0:CA:9E:52:89:
                                79:2B:C5:0E:78:09:7F:2E:6A:97:68:99:7E:22:F0:D7
                    Timestamp : Sep 19 03:50:12.581 2021 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:45:02:21:00:EA:07:95:A6:A7:C5:16:80:27:6B:F7:
                                3E:BE:BC:EC:C2:04:F4:7B:70:5F:56:9D:BB:52:F8:4C:
                                25:39:F3:B5:2A:02:20:55:0E:2F:BE:F4:9C:FC:D6:73:
                                C6:BE:19:EF:0E:89:0F:99:9B:78:73:32:95:7C:B9:BF:
                                92:66:E1:33:1F:FD:1D
    Signature Algorithm: sha256WithRSAEncryption
         7f:98:82:44:07:65:b9:01:49:f8:da:f4:5f:b3:d6:79:9c:7a:
         19:74:26:e5:a1:50:3f:ec:53:a1:ce:7a:12:4d:15:b6:10:23:
         e4:1c:18:f9:6d:95:9c:6a:3e:b2:94:c1:6e:3d:e2:c8:7c:d8:
         eb:f1:08:8a:74:f5:0a:21:be:cb:30:e3:c3:6a:a5:c7:76:1b:
         34:fa:a4:13:aa:67:c9:3e:cf:9a:c8:3d:c8:35:4a:8a:f3:62:
         ee:c1:0b:6c:fc:d6:46:72:29:7d:0a:12:76:2b:b1:7b:12:bd:
         22:af:bb:d5:ef:52:47:bb:c3:7d:61:c2:08:f4:0a:10:73:06:
```

```
        58:14:ae:69:2b:8d:45:ef:62:02:58:3e:68:5b:b6:a6:b4:1d:
        c2:a2:48:98:e9:65:a2:ce:a9:1c:ba:17:bf:29:c0:c9:a7:f6:
        e0:28:c4:eb:c0:94:5e:d5:14:46:d9:d0:23:c5:27:d2:f8:d3:
        48:95:d7:ed:16:2f:08:24:57:7b:b6:7c:f6:91:39:57:08:9e:
        88:92:ae:91:14:76:53:78:46:67:4b:31:a1:a1:a0:4e:9a:df:
        f5:e1:c4:09:0b:ce:08:0b:03:16:bb:c1:cd:03:70:40:18:ee:
        fe:3a:81:c8:23:04:d5:85:87:69:e3:4f:cc:71:7e:8e:04:43:
        f5:8e:06:1a
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            91:2b:08:4a:cf:0c:18:a7:53:f6:d6:2e:25:a7:5f:5a
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = Internet Security Research Group, CN = ISRG Root X1
        Validity
            Not Before: Sep  4 00:00:00 2020 GMT
            Not After : Sep 15 16:00:00 2025 GMT
        Subject: C = US, O = Let's Encrypt, CN = R3
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:bb:02:15:28:cc:f6:a0:94:d3:0f:12:ec:8d:55:
                    92:c3:f8:82:f1:99:a6:7a:42:88:a7:5d:26:aa:b5:
                    2b:b9:c5:4c:b1:af:8e:6b:f9:75:c8:a3:d7:0f:47:
                    94:14:55:35:57:8c:9e:a8:a2:39:19:f5:82:3c:42:
                    a9:4e:6e:f5:3b:c3:2e:db:8d:c0:b0:5c:f3:59:38:
                    e7:ed:cf:69:f0:5a:0b:1b:be:c0:94:24:25:87:fa:
                    37:71:b3:13:e7:1c:ac:e1:9b:ef:db:e4:3b:45:52:
                    45:96:a9:c1:53:ce:34:c8:52:ee:b5:ae:ed:8f:de:
                    60:70:e2:a5:54:ab:b6:6d:0e:97:a5:40:34:6b:2b:
                    d3:bc:66:eb:66:34:7c:fa:6b:8b:8f:57:29:99:f8:
                    30:17:5d:ba:72:6f:fb:81:c5:ad:d2:86:58:3d:17:
                    c7:e7:09:bb:f1:2b:f7:86:dc:c1:da:71:5d:d4:46:
                    e3:cc:ad:25:c1:88:bc:60:67:75:66:b3:f1:18:f7:
                    a2:5c:e6:53:ff:3a:88:b6:47:a5:ff:13:18:ea:98:
                    09:77:3f:9d:53:f9:cf:01:e5:f5:a6:70:17:14:af:
                    63:a4:ff:99:b3:93:9d:dc:53:a7:06:fe:48:85:1d:
                    a1:69:ae:25:75:bb:13:cc:52:03:f5:ed:51:a1:8b:
                    db:15
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, TLS Web Server Authentication
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Subject Key Identifier:
                14:2E:B3:17:B7:58:56:CB:AE:50:09:40:E6:1F:AF:9D:8B:14:C2:C6
            X509v3 Authority Key Identifier:
                keyid:79:B4:59:E6:7B:B6:E5:E4:01:73:80:08:88:C8:1A:58:F6:E9:9B:6E

            Authority Information Access:
                CA Issuers - URI:http://x1.i.lencr.org/

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://x1.c.lencr.org/

            X509v3 Certificate Policies:
                Policy: 2.23.140.1.2.1
                Policy: 1.3.6.1.4.1.44947.1.1.1

    Signature Algorithm: sha256WithRSAEncryption
         85:ca:4e:47:3e:a3:f7:85:44:85:bc:d5:67:78:b2:98:63:ad:
         75:4d:1e:96:3d:33:65:72:54:2d:81:a0:ea:c3:ed:f8:20:bf:
         5f:cc:b7:70:00:b7:6e:3b:f6:5e:94:de:e4:20:9f:a6:ef:8b:
         b2:03:e7:a2:b5:16:3c:91:ce:b4:ed:39:02:e7:7c:25:8a:47:
         e6:65:6e:3f:46:f4:d9:f0:ce:94:2b:ee:54:ce:12:bc:8c:27:
         4b:b8:c1:98:2f:a2:af:cd:71:91:4a:08:b7:c8:b8:23:7b:04:
         2d:08:f9:08:57:3e:83:d9:04:33:0a:47:21:78:09:82:27:c3:
         2a:c8:9b:b9:ce:5c:f2:64:c8:c0:be:79:c0:4f:8e:6d:44:0c:
         5e:92:bb:2e:f7:8b:10:e1:e8:1d:44:29:db:59:20:ed:63:b9:
         21:f8:12:26:94:93:57:a0:1d:65:04:c1:0a:22:ae:10:0d:43:
         97:a1:18:1f:7e:e0:e0:86:37:b5:5a:b1:bd:30:bf:87:6e:2b:
         2a:ff:21:4e:1b:05:c3:f5:18:97:f0:5e:ac:c3:a5:b8:6a:f0:
         2e:bc:3b:33:b9:ee:4b:de:cc:fc:e4:af:84:0b:86:3f:c0:55:
         43:36:f6:68:e1:36:17:6a:8e:99:d1:ff:a5:40:a7:34:b7:c0:
         d0:63:39:35:39:75:6e:f2:ba:76:c8:93:02:e9:a9:4b:6c:17:
         ce:0c:02:d9:bd:81:fb:9f:b7:68:d4:06:65:b3:82:3d:77:53:
         f8:8e:79:03:ad:0a:31:07:75:2a:43:d8:55:97:72:c4:29:0e:
         f7:c4:5d:4e:c8:ae:46:84:30:d7:f2:85:5f:18:a1:79:bb:e7:
         5e:70:8b:07:e1:86:93:c3:b9:8f:dc:61:71:25:2a:af:df:ed:
         25:50:52:68:8b:92:dc:e5:d6:b5:e3:da:7d:d0:87:6c:84:21:
         31:ae:82:f5:fb:b9:ab:c8:89:17:3d:e1:4c:e5:38:0e:f6:bd:
         2b:bd:96:81:14:eb:d5:db:3d:20:a7:7e:59:d3:e2:f8:58:f9:
         5b:b8:48:cd:fe:5c:4f:16:29:fe:1e:55:23:af:c8:11:b0:8d:
         ea:7c:93:90:17:2f:fd:ac:a2:09:47:46:3f:f0:e9:b0:b7:ff:
         28:4d:68:32:d6:67:5e:1e:69:a3:93:b8:f5:9d:8b:2f:0b:d2:
         52:43:a6:6f:32:57:65:4d:32:81:df:38:53:85:5d:7e:5d:66:
         29:ea:b8:dd:e4:95:b5:cd:b5:56:12:42:cd:c4:4e:c6:25:38:
         44:50:6d:ec:ce:00:55:18:fe:e9:49:64:d4:4e:ca:97:9c:b4:
```

```
        5b:c0:73:a8:ab:b8:47:c2
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            40:01:77:21:37:d4:e9:42:b8:ee:76:aa:3c:64:0a:b7
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: O = Digital Signature Trust Co., CN = DST Root CA X3
        Validity
            Not Before: Jan 20 19:14:03 2021 GMT
            Not After : Sep 30 18:14:03 2024 GMT
        Subject: C = US, O = Internet Security Research Group, CN = ISRG Root X1
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (4096 bit)
                Modulus:
                    00:ad:e8:24:73:f4:14:37:f3:9b:9e:2b:57:28:1c:
                    87:be:dc:b7:df:38:90:8c:6e:3c:e6:57:a0:78:f7:
                    75:c2:a2:fe:f5:6a:6e:f6:00:4f:28:db:de:68:86:
                    6c:44:93:b6:b1:63:fd:14:12:6b:bf:1f:d2:ea:31:
                    9b:21:7e:d1:33:3c:ba:48:f5:dd:79:df:b3:b8:ff:
                    12:f1:21:9a:4b:c1:8a:86:71:69:4a:66:66:6c:8f:
                    7e:3c:70:bf:ad:29:22:06:f3:e4:c0:e6:80:ae:e2:
                    4b:8f:b7:99:7e:94:03:9f:d3:47:97:7c:99:48:23:
                    53:e8:38:ae:4f:0a:6f:83:2e:d1:49:57:8c:80:74:
                    b6:da:2f:d0:38:8d:7b:03:70:21:1b:75:f2:30:3c:
                    fa:8f:ae:dd:da:63:ab:eb:16:4f:c2:8e:11:4b:7e:
                    cf:0b:e8:ff:b5:77:2e:f4:b2:7b:4a:e0:4c:12:25:
                    0c:70:8d:03:29:a0:e1:53:24:ec:13:d9:ee:19:bf:
                    10:b3:4a:8c:3f:89:a3:61:51:de:ac:87:07:94:f4:
                    63:71:ec:2e:e2:6f:5b:98:81:e1:89:5c:34:79:6c:
                    76:ef:3b:90:62:79:e6:db:a4:9a:2f:26:c5:d0:10:
                    e1:0e:de:d9:10:8e:16:fb:b7:f7:a8:f7:c7:e5:02:
                    07:98:8f:36:08:95:e7:e2:37:96:0d:36:75:9e:fb:
                    0e:72:b1:1d:9b:bc:03:f9:49:05:d8:81:dd:05:b4:
                    2a:d6:41:e9:ac:01:76:95:0a:0f:d8:df:d5:bd:12:
                    1f:35:2f:28:17:6c:d2:98:c1:a8:09:64:77:6e:47:
                    37:ba:ce:ac:59:5e:68:9d:7f:72:d6:89:c5:06:41:
                    29:3e:59:3e:dd:26:f5:24:c9:11:a7:5a:a3:4c:40:
                    1f:46:a1:99:b5:a7:3a:51:6e:86:3b:9e:7d:72:a7:
                    12:05:78:59:ed:3e:51:78:15:0b:03:8f:8d:d0:2f:
                    05:b2:3e:7b:4a:1c:4b:73:05:12:fc:c6:ea:e0:50:
                    13:7c:43:93:74:b3:ca:74:e7:8e:1f:01:08:d0:30:
                    d4:5b:71:36:b4:07:ba:c1:30:30:5c:48:b7:82:3b:
                    98:a6:7d:60:8a:a2:a3:29:82:cc:ba:bd:83:04:1b:
                    a2:83:03:41:a1:d6:05:f1:1b:c2:b6:f0:a8:7c:86:
                    3b:46:a8:48:2a:88:dc:76:9a:76:bf:1f:6a:a5:3d:
                    19:8f:eb:38:f3:64:de:c8:2b:0d:0a:28:ff:f7:db:
                    e2:15:42:d4:22:d0:27:5d:e1:79:fe:18:e7:70:88:
                    ad:4e:e6:d9:8b:3a:c6:dd:27:51:6e:ff:bc:64:f5:
                    33:43:4f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            Authority Information Access:
                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:
                79:B4:59:E6:7B:B6:E5:E4:01:73:80:08:88:C8:1A:58:F6:E9:9B:6E
    Signature Algorithm: sha256WithRSAEncryption
         0a:73:00:6c:96:6e:ff:0e:52:d0:ae:dd:8c:e7:5a:06:ad:2f:
         a8:e3:8f:bf:c9:0a:03:15:50:c2:e5:6c:42:bb:6f:9b:f4:b4:
         4f:c2:44:88:08:75:cc:eb:07:9b:14:62:6e:78:de:ec:27:ba:
         39:5c:f5:a2:a1:6e:56:94:70:10:53:b1:bb:e4:af:d0:a2:c3:
         2b:01:d4:96:f4:c5:20:35:33:f9:d8:61:36:e0:71:8d:b4:b8:
         b5:aa:82:45:95:c0:f2:a9:23:28:e7:d6:a1:cb:67:08:da:a0:
         43:2c:aa:1b:93:1f:c9:de:f5:ab:69:5d:13:f5:5b:86:58:22:
         ca:4d:55:e4:70:67:6d:c2:57:c5:46:39:41:cf:8a:58:83:58:
         6d:99:fe:57:e8:36:0e:f0:0e:23:aa:fd:88:97:d0:e3:5c:0e:
         94:49:b5:b5:17:35:d2:2e:bf:4e:85:ef:18:e0:85:92:eb:06:
         3b:6c:29:23:09:60:dc:45:02:4c:12:18:3b:e9:fb:0e:de:dc:
         44:f8:58:98:ae:ea:bd:45:45:a1:88:5d:66:ca:fe:10:e9:6f:
         82:c8:11:42:0d:fb:e9:ec:e3:86:00:de:9d:10:e3:38:fa:a4:
         7d:b1:d8:e8:49:82:84:06:9b:2b:e8:6b:4f:01:0c:38:77:2e:
         f9:dd:e7:39
```