CS-C3130 Information Security
Examination 2021-12-20
Lecturer: Tuomas Aura

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

1. Access control terminology

Give an example of each of the following in the context of a university or school. The example should clearly demonstrate that you have understood the meaning of the concept. The answer should be an example; no points will be given for a definition. (2p each)

1. attribute-based AC
2. principle of least privilege
3. no-read-down policy

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 ten thousand (10 000) registered users. The passwords are machine-generated random 10-character strings with the following character set:

```
ABCDE FGHIJ KLMNO PQRST UVWXY Z
Abcde fghij klmno pqrst uvwxy z
01234 56789  +=
```

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

```
hash = truncate(SHA256(username+":"+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 GPU. Wily's gaming GPU can compute 1000 million SHA-256 hash values per second.

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)

Give a numerical result and show the calculation steps.

*Useful data: One day (24h) of GPU usage costs about $1 considering that the price of the GPU is amortized over a three-year lifetime. One day is 24*60*60 = 86400 seconds.*

$\frac{10^{18}}{10^9}$ H H/s

10^{18} ~~10^{-9} / 5 10^9~~

The examination continues on the following page.

3. Secure storage

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 the beverage engineers have gone home. You are not allowed to enter when they are at work. So far, you have discovered the location of the computer. It is a Windows PC.

From a security policy pinned on the wall, you learn that all computer disks in the factory must be protected with BitLocker.

You sneak into the control room in the evening and start examining the computer. The user is still logged in and the production process seems to be running, but the screen is locked.

Problem: What realistic ways do you have for getting access to the secret formula on the computer? (6p)

4. Security protocols

The registrar at SKI School receives course results from teachers by insecure email (SMTP). Therefore, the teachers must sign the emails to the registrar with PGP, a widely used software tool for signing emails. The registrar has a list all the teachers' public signature keys, which are used to verify the signatures. Here is one such email:

```
To: registrar@ski.waveuni.fi
From: tuomas@ski.waveuni.fi
Subject: Teemu finally improved his grade
Date: Wed, 15 Dec 2021 16:02:56 +0000

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

Teemu Teekkari (student number 34561278A) successfully completed another bonus
assignment in my course E101 Ether Vortices. Each bonus assignment increases the
grade by one, and they can be submitted within the academic year. Please update
his grade.
Thanks!
Tuomas
-----BEGIN PGP SIGNATURE-----

iQGzBAEBCgAdFiEEnJhA0PZJAdknnRpLrXS6ZraNZ0oFAmG6IHIACgkQrXS6ZraN
Z0o0zAv/Wd1wfA8PB4IuL15REh/OU44c7kGCGgeV8PVXylNHdu3yMmlqt94SQJoo
quQgzbxxqxoov3pzoRFv8dtwRelhI98LqezWEEE8QJ/HsgJmZJmDHebnIVc5Xd0j
yOX5z/yrEKe3jGA5bIzfcVQhvL0xey5QlQe/r23PWKg1sXZ1RTSB/4LsVukVLLYe
VZkC1RxGXSHrxy/ULffX9JCQoPhcZ4RfjBzGxyTgLvDiA8Dbso6GTur6lZcGBsFl
BXyU3o0CpIx6F+aIaoEw+/GhTvz34pFCgl4ePydNvKEHsxJabNyS+zhiXw/lhKcM
+Sr6emgGDGGchlb1XIZn2qCMKhP2XWpiktt9fRoxyewcCDOhBjgTof0sf0afWxI7
lv1+Sw4AxRR4vdwp6s83Yhhjmd4CGkO+RJv4TBS9I9wY3gz5QkFHfQ6LIEXe+btQ
ABLUqCzY1duB/c+6+9UIMm3E5iF+Lj7Bx+22cl+gqrErFIt1dbpFUI2w4ALvPwSq
O/dlaQjw
=clyp
-----END PGP SIGNATURE-----
```

Problem: Analyze the security of this communication protocol. Propose a solution to any serious flaws that you find. (6p)

Note: You do not need to consider software implementation flaws.

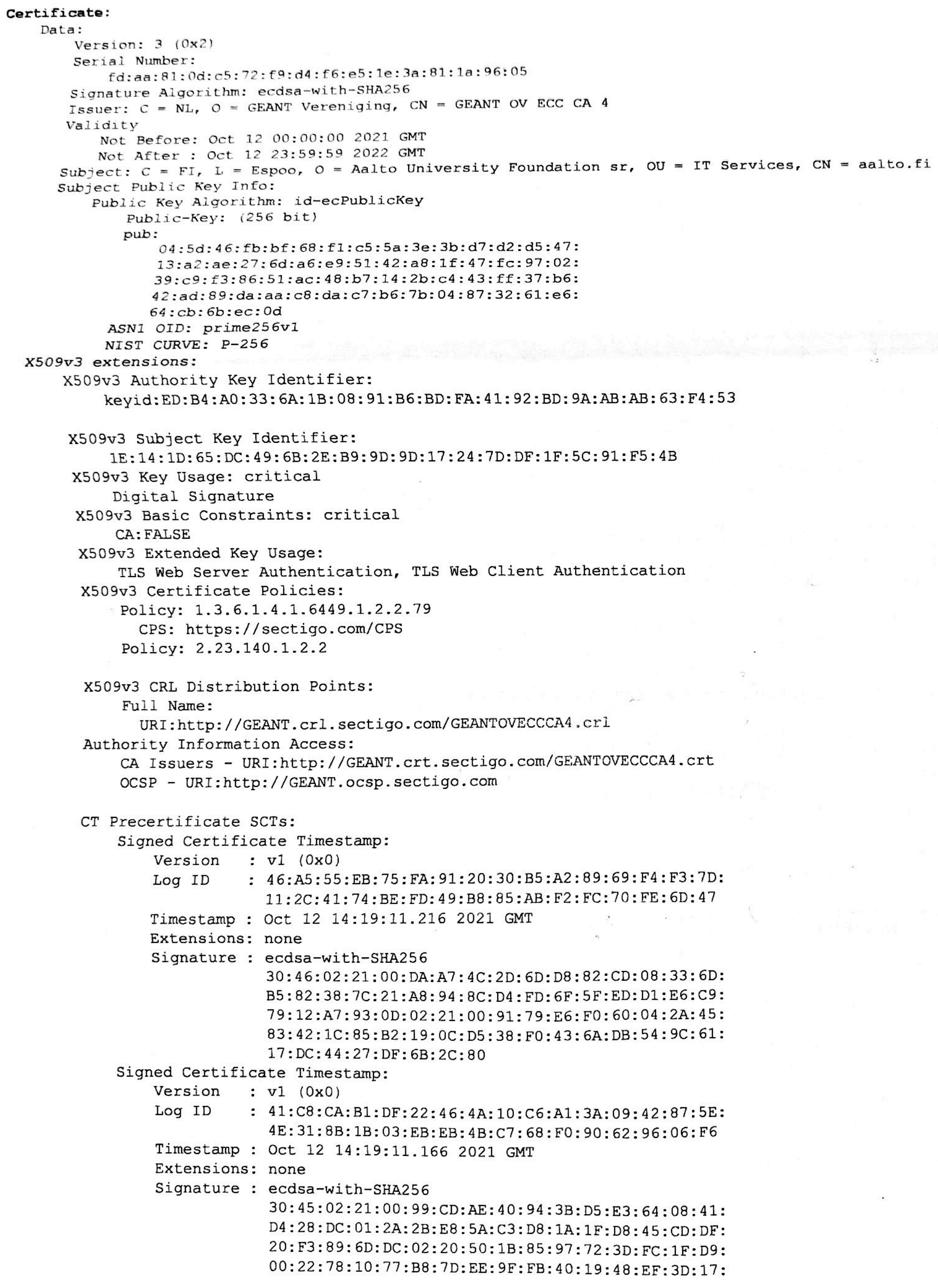
The examination continues on the following page.

5. Web security

In Appendix 1, there is a pretty-printed certificate chain for the website https://cs.aalto.fi. 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)

Note: You do not need to explain the details of the TLS handshake protocol.

Appendix 1



```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            fd:aa:81:0d:c5:72:f9:d4:f6:e5:1e:3a:81:1a:96:05
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = NL, O = GEANT Vereniging, CN = GEANT OV ECC CA 4
        Validity
            Not Before: Oct 12 00:00:00 2021 GMT
            Not After : Oct 12 23:59:59 2022 GMT
        Subject: C = FI, L = Espoo, O = Aalto University Foundation sr, OU = IT Services, CN = aalto.fi
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:5d:46:fb:bf:68:f1:c5:5a:3e:3b:d7:d2:d5:47:
                    13:a2:ae:27:6d:a6:e9:51:42:a8:1f:47:fc:97:02:
                    39:c9:f3:86:51:ac:48:b7:14:2b:c4:43:ff:37:b6:
                    42:ad:89:da:aa:c8:da:c7:b6:7b:04:87:32:61:e6:
                    64:cb:6b:ec:0d
                ASN1 OID: prime256v1
                NIST CURVE: P-256
    X509v3 extensions:
        X509v3 Authority Key Identifier:
            keyid:ED:B4:A0:33:6A:1B:08:91:B6:BD:FA:41:92:BD:9A:AB:AB:63:F4:53

        X509v3 Subject Key Identifier:
            1E:14:1D:65:DC:49:6B:2E:B9:9D:9D:17:24:7D:DF:1F:5C:91:F5:4B
        X509v3 Key Usage: critical
            Digital Signature
        X509v3 Basic Constraints: critical
            CA:FALSE
        X509v3 Extended Key Usage:
            TLS Web Server Authentication, TLS Web Client Authentication
        X509v3 Certificate Policies:
            Policy: 1.3.6.1.4.1.6449.1.2.2.79
              CPS: https://sectigo.com/CPS
            Policy: 2.23.140.1.2.2

        X509v3 CRL Distribution Points:
            Full Name:
              URI:http://GEANT.crl.sectigo.com/GEANTOVECCCA4.crl
        Authority Information Access:
            CA Issuers - URI:http://GEANT.crt.sectigo.com/GEANTOVECCCA4.crt
            OCSP - URI:http://GEANT.ocsp.sectigo.com

        CT Precertificate SCTs:
            Signed Certificate Timestamp:
                Version   : v1 (0x0)
                Log ID    : 46:A5:55:EB:75:FA:91:20:30:B5:A2:89:69:F4:F3:7D:
                            11:2C:41:74:BE:FD:49:B8:85:AB:F2:FC:70:FE:6D:47
                Timestamp : Oct 12 14:19:11.216 2021 GMT
                Extensions: none
                Signature : ecdsa-with-SHA256
                            30:46:02:21:00:DA:A7:4C:2D:6D:D8:82:CD:08:33:6D:
                            B5:82:38:7C:21:A8:94:8C:D4:FD:6F:5F:ED:D1:E6:C9:
                            79:12:A7:93:0D:02:21:00:91:79:E6:F0:60:04:2A:45:
                            83:42:1C:85:B2:19:0C:D5:38:F0:43:6A:DB:54:9C:61:
                            17:DC:44:27:DF:6B:2C:80
            Signed Certificate Timestamp:
                Version   : v1 (0x0)
                Log ID    : 41:C8:CA:B1:DF:22:46:4A:10:C6:A1:3A:09:42:87:5E:
                            4E:31:8B:1B:03:EB:EB:4B:C7:68:F0:90:62:96:06:F6
                Timestamp : Oct 12 14:19:11.166 2021 GMT
                Extensions: none
                Signature : ecdsa-with-SHA256
                            30:45:02:21:00:99:CD:AE:40:94:3B:D5:E3:64:08:41:
                            D4:28:DC:01:2A:2B:E8:5A:C3:D8:1A:1F:D8:45:CD:DF:
                            20:F3:89:6D:DC:02:20:50:1B:85:97:72:3D:FC:1F:D9:
                            00:22:78:10:77:B8:7D:EE:9F:FB:40:19:48:EF:3D:17:
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            56:67:1d:04:ea:4f:99:4c:6f:10:81:47:59:d2:75:94
        Signature Algorithm: sha384WithRSAEncryption
        Issuer: C = GB, ST = Greater Manchester, L = Salford, O = Comodo CA Limited, CN = AAA Certificate Services
        Validity
            Not Before: Mar 12 00:00:00 2019 GMT
            Not After : Dec 31 23:59:59 2028 GMT
        Subject: C = US, ST = New Jersey, L = Jersey City, O = The USERTRUST Network, CN = USERTrust ECC Certification Authority
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:1a:ac:54:5a:a9:f9:68:23:e7:7a:d5:24:6f:53:
                    c6:5a:d8:4b:ab:c6:d5:b6:d1:e6:73:71:ae:dd:9c:
                    d6:0c:61:fd:db:a0:89:03:b8:05:14:ec:57:ce:ee:
                    5d:3f:e2:21:b3:ce:f7:d4:8a:79:e0:a3:83:7e:2d:
                    97:d0:61:c4:f1:99:dc:25:91:63:ab:7f:30:a3:b4:
                    70:e2:c7:a1:33:9c:f3:bf:2e:5c:53:b1:5f:b3:7d:
                    32:7f:8a:34:e3:79:79
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:A0:11:0A:23:3E:96:F1:07:EC:E2:AF:29:EF:82:A5:7F:D0:30:A4:B4

            X509v3 Subject Key Identifier:
                3A:E1:09:86:D4:CF:19:C2:96:76:74:49:76:DC:E0:35:C6:63:63:9A
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy

            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://crl.comodoca.com/AAACertificateServices.crl
            Authority Information Access:
                OCSP - URI:http://ocsp.comodoca.com

Signature Algorithm: sha384WithRSAEncryption
     19:ec:eb:9d:89:2c:20:0b:04:80:1d:18:de:42:99:72:99:16:
     32:bd:0e:9c:75:5b:2c:15:e2:29:40:6d:ee:ff:72:db:db:ab:
     90:1f:8c:95:f2:8a:3d:08:72:42:89:50:07:e2:39:15:6c:01:
     87:d9:16:1a:f5:c0:75:2b:c5:e6:56:11:07:df:d8:98:bc:7c:
     9f:19:39:df:8b:ca:00:64:73:bc:46:10:9b:93:23:8d:be:16:
     c3:2e:08:82:9c:86:33:74:76:3b:28:4c:8d:03:42:85:b3:e2:
     b2:23:42:d5:1f:7a:75:6a:1a:d1:7c:aa:67:21:c4:33:3a:39:
     6d:53:c9:a2:ed:62:22:a8:bb:e2:55:6c:99:6c:43:6b:91:97:
     d1:0c:0b:93:02:1d:d2:bc:69:77:49:e6:1b:4d:f7:bf:14:78:
     03:b0:a6:ba:0b:b4:e1:85:7f:2f:dc:42:3b:ad:74:01:48:de:
     d6:6c:e1:19:98:09:5e:0a:b3:67:47:fe:1c:e0:d5:c1:28:ef:
     4a:8b:44:31:26:04:37:8d:89:74:36:2e:ef:a5:22:0f:83:74:
     49:92:c7:f7:10:c2:0c:29:fb:b7:bd:ba:7f:e3:5f:d5:9f:f2:
     a9:f4:74:d5:b8:e1:b3:b0:81:e4:e1:a5:63:a3:cc:ea:04:78:
     90:6e:bf:f7
```