CS-C3130 Information Security
Examination 2023-10-19
Teachers: Tuomas Aura, Lachlan Gunn

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

1. Cryptographic concepts

(a) A preimage attack against the SHA-256 hash function requires in the order of 2^{256} hash computations. Why is password cracking possible with many fewer computations? 3p
(b) Recall how you connected to an online server with SSH in the course exercises. This process was vulnerable to an impersonation attack. Explain why (or give an example). 3p

Please keep each answer to 10-30 words.

2. Password cracking

Acme Inc. has created a cloud-based online service where users can register and set up a username and password. So far, they have four million (4 000 000) registered users. The passwords are machine-generated random 12-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(password), 128)
```

Sadly, the password database has leaked to the deep web, where Wile E., a notorious hacker, has found it. He plans to perform brute-force cracking on modern GPUs, which can compute 1000 million SHA-256 hash values per second.

Problem:

(a) How much does it cost, <u>on average</u>, for the attacker to crack <u>at least one</u> password? The attacker does not care which user's password it finds. Give a numerical result and show the calculation steps. 4p
(b) What is the major weakness in this password hashing method, and how can it be fixed? 2p

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.

The examination continues on the following page

3. Secure storage

You are traveling with a Windows laptop computer that has BitLocker encryption enabled for the hard disk. The computer has a built-in TPM security module. When not in use, the laptop is in sleep mode. When you start the computer, it shows the Windows lock screen, which can be unlocked with biometric authentication (face recognition) or with your username and password.

At the Elbonian airport, an officer takes the sleeping laptop to a back office to be examined while his colleague interrogates you about your travel plans. After one hour, they return the laptop to you and let you go.

Problem: Analyze how this incident might affect the security of the data stored on the laptop computer.

6p

4. Software security

Consider the following piece of C code:

```
void vulnerable() {
  char str[8];
  gets(&str);
}
```

The code is compiled and running in a 32-bit, big-endian system.

Problem:

(a) Draw a diagram of the function's stack frame, showing what information is stored and where. 2p
(b) This function contains a buffer overrun vulnerability. Explain how an attacker would exploit it. 2p
(c) Suppose the attacker wants to execute code at the memory address 0x41424344. What input should the attacker provide? 2p

Notes: In the C language, `char str[8]` is a byte array. `&str` is the starting address of `str` in the memory. The `gets()` function reads a line of user input and stores it in the memory beginning from the provided address.

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 https://password.aalto.fi/ in TLS. 6p

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

Appendix 1

Certificate 1:

```
    Data:
        Version: 3 (0x2)
        Serial Number:
            95:14:87:2e:56:c1:9c:52:ac:c3:a8:e3:82:f7:33:fe
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = NL, O = GEANT Vereniging, CN = GEANT OV ECC CA 4
        Validity
            Not Before: Apr 21 00:00:00 2023 GMT
            Not After : Apr 20 23:59:59 2024 GMT
        Subject: C = FI, ST = Uusimaa, O = Aalto University Foundation sr, CN =
password.aalto.fi
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:68:bc:45:bd:0d:ca:b1:00:b9:2e:24:93:e3:59:
                    23:c7:40:12:16:7e:d4:5c:f1:1f:e8:1a:76:12:e5:
                    34:40:1a:7b:17:ff:5e:c1:f8:fa:16:7b:62:76:ba:
                    a0:e2:f5:c6:01:66:b3:3c:9d:7c:b4:c1:75:97:a8:
                    b6:ea:ab:ba:38
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                ED:B4:A0:33:6A:1B:08:91:B6:BD:FA:41:92:BD:9A:AB:AB:63:F4:53
            X509v3 Subject Key Identifier:
                EC:B1:FD:B6:4C:7B:5C:B9:A9:E7:5A:BE:EA:57:B7:3B:3B:2A:69:A5
            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    : 76:FF:88:3F:0A:B6:FB:95:51:C2:61:CC:F5:87:BA:34:
                                B4:A4:CD:BB:29:DC:68:42:0A:9F:E6:67:4C:5A:3A:74
                    Timestamp : Apr 21 07:35:22.902 2023 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:45:02:21:00:9F:67:1C:17:28:5D:A2:AB:1C:B7:CC:
                                07:D2:CE:2F:18:EC:CF:2D:5D:95:93:95:17:0F:1F:BD:
                                5C:44:5F:85:AB:02:20:0B:E0:29:5E:17:54:AE:C5:95:
                                6B:58:3E:3D:B9:3F:CE:3C:26:0A:D2:5F:9C:07:3D:27:
                                3A:AB:FB:07:78:05:C8
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
```

```
                    Log ID    : DA:B6:BF:6B:3F:B5:B6:22:9F:9B:C2:BB:5C:6B:E8:70:
                                91:71:6C:BB:51:84:85:34:BD:A4:3D:30:48:D7:FB:AB
                    Timestamp : Apr 21 07:35:22.985 2023 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:45:02:20:41:56:D3:7D:1B:BE:BB:36:FF:94:64:78:
                                B9:58:22:26:00:73:EB:79:05:F9:7A:20:81:8F:3D:BC:
                                C6:FC:BB:A0:02:21:00:9A:57:B3:82:02:4A:96:2E:45:
                                F1:38:B4:92:7B:D7:6A:BB:E4:15:FC:CC:D5:8F:6E:A7:
                                E6:46:BC:32:68:A5:F1
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : EE:CD:D0:64:D5:DB:1A:CE:C5:5C:B7:9D:B4:CD:13:A2:
                                32:87:46:7C:BC:EC:DE:C3:51:48:59:46:71:1F:B5:9B
                    Timestamp : Apr 21 07:35:23.024 2023 GMT
                    Extensions: none
                    Signature : ecdsa-with-SHA256
                                30:46:02:21:00:EC:30:2D:36:C3:FC:8E:F0:DB:6D:9B:
                                E1:F3:4C:79:5D:E7:9E:45:CC:76:4B:19:21:AB:9C:6E:
                                AD:B7:37:D9:A5:02:21:00:B4:E6:07:E5:9F:C1:50:0B:
                                44:E5:5B:CC:2A:F2:87:D2:46:A5:C4:57:59:EC:CA:E1:
                                46:77:82:65:B4:A7:6F:79
            X509v3 Subject Alternative Name:
                DNS:password.aalto.fi, DNS:access.aalto.fi,
DNS:losenord.aalto.fi, DNS:salasana.aalto.fi
    Signature Algorithm: ecdsa-with-SHA256
    Signature Value:
        30:45:02:21:00:de:71:91:72:6e:15:82:97:51:15:f9:d7:9b:
        e7:29:c8:5e:38:a0:af:dd:13:83:53:1a:ad:c3:e7:24:02:ec:
        d5:02:20:28:38:66:ee:07:b0:a7:b4:4d:94:6b:c3:f5:70:63:
        b5:f0:df:7e:65:af:42:22:bf:f8:c6:62:68:5b:e3:77:fd
```

Certificate 2:

```
    Data:
        Version: 3 (0x2)
        Serial Number:
            eb:8e:81:19:71:29:f4:af:64:ef:81:4a:2f:50:ce:e9
        Signature Algorithm: ecdsa-with-SHA384
        Issuer: C = US, ST = New Jersey, L = Jersey City, O = The USERTRUST
Network, CN = USERTrust ECC Certification Authority
        Validity
            Not Before: Feb 18 00:00:00 2020 GMT
            Not After : May  1 23:59:59 2033 GMT
        Subject: C = NL, O = GEANT Vereniging, CN = GEANT OV ECC CA 4
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:5d:89:2f:1a:b7:eb:32:cd:88:c1:d2:39:f8:8c:
                    29:13:03:e1:fa:28:16:fc:13:96:7a:d9:8e:c0:ff:
                    d9:21:70:bc:7c:d7:82:df:f6:58:3c:00:0c:c9:1a:
                    45:4b:4b:f7:fd:ce:79:14:34:c4:db:16:ce:51:9e:
                    73:79:56:58:42
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                3A:E1:09:86:D4:CF:19:C2:96:76:74:49:76:DC:E0:35:C6:63:63:9A
            X509v3 Subject Key Identifier:
                ED:B4:A0:33:6A:1B:08:91:B6:BD:FA:41:92:BD:9A:AB:AB:63:F4:53
            X509v3 Key Usage: critical
```

```
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Certificate Policies:
                Policy: X509v3 Any Policy
                  CPS: https://sectigo.com/CPS
            X509v3 CRL Distribution Points:
                Full Name:

URI:http://crl.usertrust.com/USERTrustECCCertificationAuthority.crl
            Authority Information Access:
                CA Issuers -
URI:http://crt.usertrust.com/USERTrustECCAddTrustCA.crt
                OCSP - URI:http://ocsp.usertrust.com
    Signature Algorithm: ecdsa-with-SHA384
    Signature Value:
        30:65:02:30:1f:b3:d9:ec:33:4a:9a:24:65:6e:e8:3a:56:57:
        2e:2a:a2:38:8e:a7:05:75:87:f3:16:67:91:89:c7:2e:82:2a:
        fd:fe:44:c0:77:49:39:1a:16:1d:3e:1e:27:db:93:6e:02:31:
        00:d1:7f:fb:a3:5c:04:35:6f:89:c5:a5:91:9a:48:82:a5:77:
        28:1c:74:20:c0:c5:b0:1d:f6:d9:71:70:df:fe:27:9d:f8:08:
        90:db:97:37:7f:e3:44:44:cc:65:b0:4b:99
```

Certificate 3:

```
    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:
                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
Signature Value:
    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
```