CS-C3130 Information Security
Examination 2024-04-15
Teachers: Tuomas Aura, Lachlan Gunn

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 concepts in the context of a chocolate factory. The example can be about human workflows or computer systems used in the chocolate production.

(a) principle of minimum privilege (2p)
(b) separation of roles (2p)
(c) covert channel (2p)

Please answer each item with one sentence. Points will be given for examples, not for definitions. It is a civilian chocolate factory; do not give military examples.

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 one million (1 000 000) registered users. The passwords are machine-generated random 15-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:

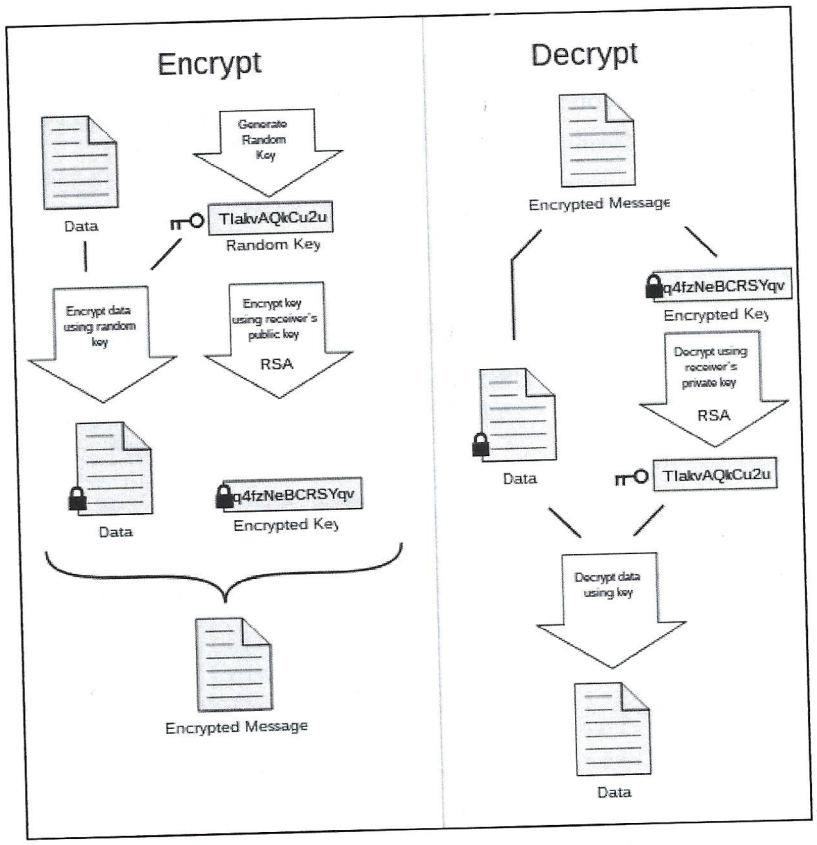
(a) How much does it cost, on average, for the attacker to crack at least one password? The attacker does not care which user's password it finds. Show the calculation steps and give an approximate numerical result. 4p
(b) What is the major weakness in this password hashing method, and how can it be 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. Security protocols

Published in 1991, PGP was the first widely available open-source cryptographic tool for strong encryption. It is still sometimes used to encrypt confidential documents emailed between companies. The picture below describes the encryption process: the data is encrypted with a random key and symmetric encryption, and the key is encrypted with the recipient's public key. The sender must have learned the recipient's public key via some secure method.



[Picture: Wikipedia]

A teacher decides that programming exercise solutions (a Python code file) must be encrypted with PGP, as in the picture above, and then submitted to the teacher by email. The teacher knows some students are hacking the school computer network or email server, so that they can read, spoof, and modify emails. The teacher believes that PGP encryption will prevent:

(a) interception, i.e., unauthorized reading of the message when it is in transit from the student through the computer network and email server to the teacher,
(b) unauthorized modification of other student's submissions, and
(c) plagiarism, where one student intercepts and copies another student's solution.

Problem: How well does the encryption protect against these three threats? 2p each

The examination continues on the following page

4. Software security

Consider the following piece of C code:

```
void vulnerable() {
  char str[12];
  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 0x11223344. What input should the attacker provide? 2p

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

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 information learned from the certificates to authenticate the website https://effi.org/. 6p

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

Appendix 1

Certificate 1:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            04:fd:d5:89:89:c4:63:13:1b:8c:96:28:8e:fa:1b:2a:e3:de
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, O = Let's Encrypt, CN = R3
        Validity
            Not Before: Feb 20 03:55:09 2024 GMT
            Not After : May 20 03:55:08 2024 GMT
        Subject: CN = effi.org
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d3:e4:54:54:48:8c:ed:ab:74:d6:f6:66:50:4e:
                    2d:f9:5c:32:c4:94:b9:50:a3:de:51:5c:7e:63:59:
                    2d:85:c7:db:99:d7:5a:fa:cd:42:1a:1b:cd:77:52:
                    b5:7f:50:dc:b9:86:4f:94:42:78:ba:b3:a2:e7:7f:
                    2d:33:7c:0d:63:09:d5:6f:1b:24:c7:c2:f3:27:15:
                    b8:9b:5f:7e:a8:c7:2e:06:ac:e8:e5:f3:d2:ef:64:
                    23:34:a8:34:64:26:74:a9:79:68:b7:65:06:72:91:
                    6c:82:9b:77:d8:57:16:83:54:c2:30:69:0c:e7:4f:
                    68:9f:20:16:ec:ed:11:e0:b6:0a:d8:d8:b9:fc:9b:
                    9d:da:21:c3:39:04:c8:e2:c3:f2:b8:d5:ed:be:ee:
                    5d:24:d4:69:c7:66:24:33:52:21:93:5d:35:4b:47:
                    3c:a1:91:b5:fa:6a:59:31:40:0e:38:8e:9a:87:9d:
                    41:af:d1:35:8a:16:d9:06:9a:e6:43:21:24:ab:40:
                    fc:f1:d5:8d:82:ef:22:a3:77:f0:04:7b:31:ca:40:
                    b6:8a:5b:2d:7e:01:13:ed:c3:f6:3f:a7:e2:6c:57:
                    43:14:03:cb:6f:25:c3:ac:77:ad:15:71:de:5b:d7:
                    68:83:b7:ea:53:7d:c6:49:9d:07:31:2b:8d:90:53:
                    ec:8b
                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:
                1E:D2:74:95:97:AE:CF:EB:65:AC:4E:F1:9A:2D:40:BC:74:AF:DF:07
            X509v3 Authority Key Identifier:
                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:effi.org, DNS:www.effi.org
            X509v3 Certificate Policies:
                Policy: 2.23.140.1.2.1
            CT Precertificate SCTs:
                Signed Certificate Timestamp:
                    Version   : v1 (0x0)
                    Log ID    : 3B:53:77:75:3E:2D:B9:80:4E:8B:30:5B:06:FE:40:3B:
                                67:D8:4F:C3:F4:C7:BD:00:0D:2D:72:6F:E1:FA:D4:17
                    Timestamp : Feb 20 04:55:09.993 2024 GMT
```

```
            Extensions: none
            Signature : ecdsa-with-SHA256
                        30:45:02:20:68:0D:AF:46:3F:79:B9:48:A6:25:9C:83:
                        A7:F2:08:F2:1B:55:15:21:4E:48:C5:B6:DC:C7:37:98:
                        67:E4:FF:99:02:21:00:C4:D5:75:FA:18:E4:71:32:38:
                        50:7C:2C:2B:C4:C4:40:58:28:D8:74:AA:8B:9F:BA:E9:
                        C4:60:5A:90:CF:2F:68
        Signed Certificate Timestamp:
            Version   : v1 (0x0)
            Log ID    : 48:B0:E3:6B:DA:A6:47:34:0F:E5:6A:02:FA:9D:30:EB:
                        1C:52:01:CB:56:DD:2C:81:D9:BB:BF:AB:39:D8:84:73
            Timestamp : Feb 20 04:55:10.001 2024 GMT
            Extensions: none
            Signature : ecdsa-with-SHA256
                        30:45:02:20:73:02:20:25:97:4E:85:50:AF:B6:7E:C4:
                        B0:15:BF:6F:BA:E0:05:BD:97:FE:C1:9A:DF:0A:E5:AD:
                        2B:99:59:00:02:21:00:B4:F5:93:90:8A:D6:D0:BB:52:
                        08:FE:CE:5B:5D:79:9D:22:75:49:B9:33:A0:42:E7:79:
                        38:63:6D:19:59:37:6F
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        1f:90:cc:3b:ce:f5:65:b6:a4:20:b8:ea:9f:2c:26:c4:d8:b0:
        3c:e6:1c:ff:cc:a2:63:7d:60:9a:60:06:a9:42:79:0d:4b:2f:
        53:98:01:fe:21:b5:a7:88:2a:39:9f:c9:3d:8f:d5:9d:76:6c:
        0b:c5:c3:52:c7:46:77:e1:78:15:ab:12:d5:c8:a2:0a:e8:da:
        af:5a:a1:1b:71:10:55:ff:08:df:ad:13:5b:4c:ac:71:2c:c5:
        83:85:bb:57:18:62:18:1c:2c:b7:1e:46:6e:f5:7f:f6:18:e9:
        a4:b9:9d:47:0a:71:e9:2b:bb:00:20:4c:43:00:e8:96:3f:7a:
        52:7f:ad:f6:8b:51:61:6b:6a:11:48:4e:75:1e:52:20:4e:35:
        3d:d1:c1:aa:a9:69:e1:0a:a3:4a:79:0e:83:8a:a9:79:a2:37:
        df:f2:57:7a:06:79:11:4e:c4:88:99:9f:2c:84:c8:82:c9:b8:
        14:01:9b:c3:78:c6:f0:9a:14:9d:af:f1:66:f6:86:90:e1:58:
        8e:3c:6d:8d:84:2c:30:48:73:34:96:0c:58:28:05:9c:a5:b1:
        50:6b:81:e6:af:84:d3:59:79:be:b9:b4:d8:b7:b0:55:4c:c2:
        78:a6:fb:8b:1d:0b:0d:f4:cd:03:00:74:13:17:de:0c:9a:f5:
        ae:f4:2b:3d
```

Certificate 2:

```
    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
                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:
            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
Signature Value:
    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
```