SECURITY SPRING 2018

Examination set, June 1, 2018.

What to answer

1. MSc students (class code KSSECUR1KU) must answer all questions.
2. BSc students (class code BSSECUR1KU) must answer all questions EXCEPT those titled MSC-ONLY-1 through MSC-ONLY-8.

What to hand in

You submit electronically, via LearnIT:

1. A plain-text file `answers.txt` with your answers to multiple choice questions, one line per answer: the question identifier, a colon, and the answer digit (format example below). You can submit only one answer for each question; multiple answers will be awarded zero points.
2. A pdf file `discussion.pdf` containing the answers to discussion questions D1 and D2. It may contain text and figures in any form.

If there are technical or logistical problems with submitting in this way, please turn to available personnel in order to find a backup solution. Feel free to submit a .zip archive containing the above two files.

How to answer

Example multiple choice question:

> **Question 9-7**
>
> This is the question text. It is followed by the possible answers:
>
> 1. The first possible answer.
> 2. The second possible answer.
> 3. The third possible answer.
> 4. The fourth possible answer.

Example answer. You choose "The third possible answer":

```
9-7:3
```

Permissible aids

This examination is A11: Written, on-premise, with access to all aids and internet.

Questions begin on the next page.

Multiple-choice Questions

Your answers to the multiple choice questions counts 60% towards the final grade.

Security principles

Question 1-1

The hotel chain "Atlantic" has decided to implement a system to control access to their rooms. To satisfy the diverse customers needs, they want to offer access by: smartcards, smartcards plus pincode, and pincode-only. This is a violation of the principle of:

1. Open design
2. Generating secrets
3. Simplicity
4. No single point of failure

Question 1-2

For each hotel in the chain, Atlantic generated a master key for the smartcard system that allows access to that particular hotel only. Unfortunately, the program that generated the master keys did not gather enough entropy, hence half of the master keys are the same. This is a violation of the principle of:

1. Compartmentalization
2. Generating secrets
3. Least privilege
4. Minimum exposure

Question 1-3

The cleaning staff of the "Atlantic" are issued special keys that are computer-controlled to: only open rooms allocated for cleaning; only open those rooms from 10am to 1pm; only open each room once; and only work on the days on which the key-holder is on shift. This is an application of the principle of:

1. Minimum exposure
2. Usability
3. Least privilege
4. No single point of failure

Question 1-4

The smartcards for the cleaning personel also give access to the server room, which has an open terminal that allows anybody to change card permissions. This is a violation of:

1. Complete mediation
2. Generating secrets
3. Usability
4. Compartmentalization

Question 1-5

The server that manages access control to the rooms is also hosting the hotel's booking service, customer database and payroll system. This violates the principle of:

1. Compartmentalization
2. No single point of failure
3. Minimum exposure
4. Complete mediation

Question 1-6

During development, the server's database was made accessible from the external network, and it has remained so ever since. This contradicts the principle of:

1. Open design
2. Compartmentalization
3. Minimum exposure
4. Least privilege

Question 1-7

Each access to a room is recorded in a cryptographic, append only log. This is in accordance with the principle of:

1. Open design
2. Complete mediation
3. No single point of failure
4. Traceability

Question 1-8

In case of a power outage all the locks automatically open. In order to improve security, the hotel managers have decided to change the behaviour of the locks to remain closed in case of a power failure, but being anyway openable from inside the rooms as a safety precaution. In their reasoning the managers have applied the principle of:

1. Open design
2. No single point of failure
3. Secure, fail-safe defaults
4. Traceability

Question 1-9

The booking interface of the hotel chain offers different prices according to the customer's region. However, once the region is determined, the room price is stored as a hidden field in the booking form of the web page and is not further validated. This violates:

1. Minimum trust, maximum trustworthiness
2. Complete mediation
3. No single point of failure
4. Traceability

Question 1-10

Only the owner of the "Atlantic" has the "super key" that can create a master key for a hotel in the chain. However, no recovery mechanism has been devised in case the "super key" is lost or stolen. This contradicts the principle of:

1. Complete mediation
2. No single point of failure
3. Usability
4. Compartmentalization

Computer Networks

Question MSC-ONLY-1

What is the repeated pattern in the first 7 bytes (before the start-of-frame delimiter) of an ethernet packet?

1. 10101010
2. 10111010
3. 10101110
4. 10101011

Question MSC-ONLY-2

An 8-way switch has the following internal switching table:

```
LINK MAC
1    ff:78:ad:00:fe:01
2    01:00:5e:00:00:fb
3    fe:01:01:00:5e:00
4    ad:00:fe:01:01:00
```

An ethernet frame where bytes 8-20 are as follows arrives on Link 2:

```
ff78ad00fe0101005e0000fb
```

What should the switch do with the packet?

1. Nothing
2. Forward the packet on Link 1
3. Forward the packet on Link 2
4. Forward the packet on all links but Link 3

Question MSC-ONLY-3

How should the switch in the preceding question update its switching table?

1. Do not update the switching table
2. Add an entry for Link 3, MAC fe:01:01:00:5e:00
3. Remove the entry for Link 1
4. Remove the entry for Link 2

Question MSC-ONLY-4

This is the contents of my routing table:

```
Destination        Gateway            Flags         Refs      Use   Netif Expire
default            10.28.6.1          UGSc            52        0     en0
10.28.6.1/32       link#4             UCS              1        0     en0
192.168.1.1/24     link#3             UCS              5        0     en1
172.18.1.1/30      link#5             UCS              5        0     en2
```

On what network interface should a packet for 172.18.1.7 go?

1. en0
2. en1
3. en2
4. en3

Question MSC-ONLY-5

The Dynamic Host Configuration Protocol is used for

1. Dynamically obtaining an IP address
2. Remote administration
3. Discovering IP/MAC associations
4. Discovering IP/DNS associations

Question MSC-ONLY-6

Complete the three-way handshake:

```
A -> B : SYN seq(2030)
B -> A : SYN ACK(2031) seq(2112)
```

1. `A -> B : ACK(2113) seq(2031)`
2. `A -> B : ACK(2031) seq(2113)`
3. `A -> B : ACK(2032) seq(2112)`
4. `A -> B : ACK(2112) seq(2032)`

Question MSC-ONLY-7

Here is a trace of a recursive DNS lookup for dr.dk:

```
> dig dr.dk A +trace
; <<>> DiG 9.9.7-P3 <<>> dr.dk A +trace
;; global options: +cmd
.                       416479  IN      NS      f.root-servers.net.
.                       416479  IN      NS      g.root-servers.net.
...
;; Received 1097 bytes from 193.162.153.164#53(193.162.153.164) in 26 ms

dk.                     172800  IN      NS      a.nic.dk.
dk.                     172800  IN      NS      b.nic.dk.
...
;; Received 705 bytes from 192.203.230.10#53(e.root-servers.net) in 37 ms

dr.dk.                  86400   IN      NS      ns01.dr.dk.
dr.dk.                  86400   IN      NS      dns101.telia.com.
dr.dk.                  86400   IN      NS      dns102.telia.com.
...
;; Received 875 bytes from 194.0.46.53#53(c.nic.dk) in 48 ms

dr.dk.                  60      IN      A       159.20.6.38
dr.dk.                  60      IN      NS      ns2-usa.global.sonera.net.
dr.dk.                  60      IN      NS      ns1-fin.global.sonera.fi.
...
;; Received 273 bytes from 194.255.56.69#53(dns101.telia.com) in 48 ms
```

Which of the following nameservers is in the above trace responsible for the `.dk` domain?

1. f.root-servers.net
2. b.nic.dk
3. ns01.dr.dk
4. 159.20.6.38

Question MSC-ONLY-8

In the OSI protocol stack model:

1. Payload size goes up when moving down the stack
2. Protocol layers actually form a red-black tree
3. The relative positioning of layers shift dynamically at run-time
4. Payload of higher layers are headers of lower layers

Network Security

Question 3-1

An 8-way switch has the following internal switching table:

```
LINK MAC
1    ff:78:ad:00:fe:01
2    01:00:5e:00:00:fb
3    fe:01:01:00:5e:00
4    ad:00:fe:01:01:00
```

An adversary who wishes to eavesdrop on `fe:01:01:00:5e:00` via a MAC flooding attack would:

1. Repeatedly send packets with source MAC `ff:78:ad:99:fe:01` to the switch
2. Repeatedly send packets with target MAC `ff:78:ad:99:fe:01` to the switch
3. Repeatedly send packets with random source MAC to the switch
4. Repeatedly send packets with random target MAC to the switch

Question 3-2

An adversary with MAC `ad:00:fe:01:01:00/IP 10.173.19.19` who wishes to eavesdrop on MAC `fe:01:01:00:5e:00/IP 10.173.19.20` using an ARP Spoofing attack would broadcast ARP packets:

1. `10.173.19.19 IS-AT ad:00:fe:01:01:00`
2. `10.173.19.19 IS-AT fe:01:01:00:5e:00`

3. `10.173.19.20 IS-AT ad:00:fe:01:01:00`
4. `10.173.19.20 IS-AT ff:78:ad:00:fe:01`

Question 3-3

When portscanning, which of the following scan-techniques requires fewer network packets?

1. SYN
2. XSS
3. CONNECT
4. Idle

Question 3-4

I use nmap to scan the Naive Corp webserver. This is what I find:

```
PORT      STATE   SERVICE
22/tcp    open    ssh
80/tcp    open    http
443/tcp   open    ssl/http
8022/tcp  closed  unknown
8023/tcp  open    mysql
```

Which of the following is a more likely to give me root access?

1. Apply metasploit to port 8022
2. Start a firewall on port 443
3. Launch an idle-scan on port 80
4. Try common passwords on port 22

Question 3-5

I notice a scan on my computer. Scrambling to harden my system, I run `sudo lsof -i | grep LISTEN` on my web application server and see the following:

```
sshd      1623      ssh   08u  IPv4   7269      0t0  TCP *:ssh (LISTEN)
proftpd   8028      ftp   20u  IPv4   4824      0t0  TCP *:8022 (LISTEN)
mysqld    8027            21u  IPv4   4823      0t0  TCP *:8023 (LISTEN)
nginx     8029      ftp   20u  IPv4   4825      0t0  TCP *:http (LISTEN)
nginx     8030      ftp   23u  IPv4   4898      0t0  TCP *:https (LISTEN)
```

I am already running a firewall that disallows incoming traffic on port 8022. What should I do?

1. Filter port 8022
2. Filter port 8023
3. Filter port 23u
4. Filter all ports

Question 3-6

It turns out there is no reason for me to run an ftp server. I leave it running just in case it turns out to be useful. This approach is:

1. Appropriate
2. Violating the principle of minimum exposure
3. Violating the principle of minimising trust
4. Violating the principle of generating secrets

Cryptography

Question 4-1

Salting is a technique that is used for storing passwords:

1. in conjunction with hashing, to prevent single-user brute-force attacks
2. in conjunction with encryption, to prevent single-user brute-force attacks

3. in conjunction with hashing, to prevent multi-user brute-force attacks
4. in conjunction with encryption, to prevent multi-user brute-force attacks

Question 4-2

A mobile banking app does "certificate pinning": that is, it stores the bank's server certificate, and checks that every TLS connection that the app opens is using that certificate. This prevents:

1. The bank from using a self-signed certificate
2. An intruder from performing a Man-in-the-Middle attack with a different but valid certificate
3. An intruder from performing a Man-in-the-Middle attack by stealing the bank's server certificate
4. The bank from using a certificate signed by a recognized CA

Question 4-3

A modern car has about N=100 Electric Control Units (ECUs): resource constrained devices that coordinate and control different aspects of the car. To secure the next generation of ECUs, the designers decide that TLS is too costly to implement, and decide to roll out a new protocol using only symmetric cryptography. If they want a secure channel between each pair of ECUs, how many keys do they need to distribute for each new car?

1. N^2 = 10000
2. 2^(N-1) - 1 = 633825300114114700748351602687
3. N*(N-1)/2 = 4950
4. N = 100

Question 4-4

Signing a document can be achieved by means of:

1. Hashing and then encrypting with the private key (asymmetric encryption)
2. Encrypting with the public key (asymmetric encryption)
3. Hashing and then encrypting with the secret key (symmetric encryption)
4. Encrypting with the public key (asymmetric encryption) and then hashing

Question 4-5

AES in CBC protects data confidentiality because:

1. Given twice the same block, it will produce the same output for the same key
2. Given twice the same block, it will produce two different outputs for the same key
3. Given one input block, it will produce two different outputs for two different keys
4. Given one input block, it will produce the same output for two different keys

System security

Question 5-1

I am trying to login to the ITU Linux server through SSH using my public key, but fail. I then complain to IT support, who reply with a cryptic message showing `ls -la` on the `~/.ssh` directory for my user on the server, as follows:

```
[root@bohr .ssh]# ls -la
total 28
drwx--xr-x  2 brun brun 4096 Jan 16 15:03 .
dr-xr-xr-x 10 brun brun 4096 May 23 16:29 ..
-rw-rw-rw-  1 brun brun 1598 Feb 28 16:00 authorized_keys
-rw-r--r--  1 brun brun 1675 Nov 29 01:31 id_rsa
-rw-r--r--  1 brun brun  391 Nov 29 01:31 id_rsa.pub
-rw-r--r--  1 brun brun 1353 May 24 19:31 known_hosts
```

It also contains this excerpt of the ssh man-page:

```
~/.ssh/authorized_keys
   Lists the public keys (DSA, ECDSA, Ed25519, RSA) that can be used
   for logging in as this user. If this file is writable by others it will be
   ignored by ssh.

~/.ssh/id_rsa
   Contains the private key for authentication.  These files contain
   sensitive data and should be readable by the user but not accessible by
   others (read/write/execute).  ssh will simply ignore a private key file if
   it is accessible by others.  It is possible to specify a passphrase when
   generating the key which will be used to encrypt the sensitive part of
   this file using 3DES.
```

The reason why I can't login remotely is:

1. The folder containing the ssh configuration is readable only by me, thus excluding the SSH daemon
2. The file `authorized_keys` is writable by anybody, thus the SSH server is disabling public-key authentication for my account
3. The file `id_rsa` containing my secret key is readable by anybody, thus the SSH server is disabling access for the corresponding public key
4. The file `known_hosts` is readable by anybody, thus the SSH server is disabling my account for fear of impersonation

Question 5-2

Realizing the security mistakes I have done from the IT support email, I should:

1. Kindly ask everybody to delete my private key, if they hold a copy
2. Quickly delete `id_rsa` and `id_rsa.pub` from my home folder, hoping no one had noticed
3. Change my private key and update the file `authorized_keys` in all my servers
4. Change my private and public keys, and update the file `authorized_keys` in all my servers

Question 5-3

Consider this partial output of `ls -l /usr/bin`.

```
-rwxr-xr-x 1 root   root     2434552 Jan 11  2016 alex
-rwsr-sr-x 1 daemon daemon     51464 Jan 14  2016 at
lrwxrwxrwx 1 root   root          23 Jul 25  2017 emacs -> /etc/alternatives/emacs
-rwsr-xr-x 1 root   root       54256 May 17  2017 passwd
```

Which of these files will execute at the highest privilege levels, no matter which user executes the program?

1. alex
2. at
3. emacs
4. passwd

Question 5-4

I am considering whether I should run my server on a virtual machine instead of a chroot jail, in which it is currently confined. If I switch I will:

1. benefit in terms of compartmentalization, thanks to the separated network stack
2. benefit in terms of compartmentalization, thanks to the separated file-system
3. benefit in terms of speed, thanks to the load balancing offered by the VM
4. none of the above

Question 5-5

I wrote the following C program:

```
#include
#include
int main(int argc, char **argv) {
   char filename[256];
   char filedata[1024];
```

```
   if (argc > 1) {
      strcpy(filename, argv[1]);
      FILE *pFile = fopen(filename, "r");
      fread(filedata, 1024, 1, pFile);
      fprint("%s", filedata);
      fclose(pFile);
   }
   return 0;
}
```

Which of the following statements is true:

1. It does contain a buffer overflow, because I am reading arbitrary data into `filedata`, which is of fixed size
2. It does not contain a buffer overflow, because all Unix filenames are at most 256 bytes long
3. It does not contain a buffer overflow, because `fread` does bounded reads
4. It does contain a buffer overflow, because I am copying an arbitrary string into `filename`

Web Application Security

Question 6-1

Examination Corp hires you as a penetration tester, requesting a black-box audit. What is (typically) not part of a black-box audit?

1. Reading Examination Corp internal documentation
2. Port scanning
3. Accessing the Examination Corp webpage
4. Accessing the Examination Corp public ftp servers

Question 6-2

You try to figure out the version of the Examination Corp webserver. HTTP responses from it looks like this:

```
HTTP/1.1 200 OK
Date: Thu, 24 May 2018 13:56:27 GMT
Server: Microsoft-IIS/7.5
Cache-Control: no-cache, no-store
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Content-Length: 110367
Set-Cookie: ASP.NET_SessionId=2kbno3dmiplildxumb1q3sf2; path=/; HttpOnly
Set-Cookie: cookieConsent=maybe; domain=.exam.com; expires=Sat, 24-Nov-2018 14:56:26 GMT; path=
```

Which of the following HTTP headers are most important for session hijacking?

1. Server
2. Pragma
3. Set-Cookie
4. None of them

Question 6-3

You look at the pages served by the webserver. One lists comments and suggestions from the public; an input field invites you to add an additional comment to the list. You want to try an XSS attack. Pick the input most likely to succeed as an XSS attack:

1. `AAAAAAAAAAAAAAAA\x90\x90\x90\x90\x4a\x8a\x65\x56\x00\x00\x76\xa5\xb5`
2. `'; SELECT * from USERS; --`
3. `<input onClick="console.log('pwned!')">`
4. `)>) [ "user": "admin", "login": "now" ]`

Question 6-4

Another page has an "upload file" facility, enabled by the following html fragment:

```
...
<form >
  <input type="file" name="file_name" >
  <input name="path" value="../../uploads" >
  <input name="SESSION" hidden value="d3b07384d113edec49eaa6238ad5ff00" >
  <input type="abort">
</form >
...
```

You try for a remote file upload vulnerability. Which form field should you modify?

1. `SESSION`
2. `file`
3. `abort`
4. `path`

Question 6-5

To impress the CIO who hired you, you decide to attempt to exfiltrate data from the database behind the webserver. You want to try a SQL injection attack in the comment input field of question 6.3. Which of the following inputs is more likely to succeed?

1. `AAAAAAAAAAAAAAAAA\x90\x90\x90\x90\x4a\x8a\x65\x56\x00\x00\x76\xa5\xb5`
2. `'; SELECT * from USERS; --`
3. `<input onClick="console.log('pwned!')">`
4. `)>) [ "user": "admin", "login": "now" ]`

Question 6-6

You note that the webserver is using HTTPS but has a self-signed certificate. This gives you an opportunity for:

1. A replay attack
2. A man-in-the-middle attack
3. An idle scan
4. A brute-force attack

Question 6-7

Which is the better protocol as transport for web-site contents for a commercial web-banking system?

1. HTTP
2. HTTPS
3. FTP
4. SSH

Discussion Questions

Your answer to this question counts 20% towards the final grade.

A big European car manufacturer wishes to add wireless firmware update capabilities to its top-line models. Each car comprises two distinct but communicating computers:

- The Driving Controller, which controls engine and brakes during actual driving, taking inputs from pedals, steering wheel, etc.
- The Infotainment System, which among other functions contains a GPS. Only the Infotainment System has wireless capabilities.

The manufacturer plans on having the Infotainment System of each car wirelessly querying a central server for firmware updates. Such an update comprises new programming for both the Driving Controller and the Infotainment System. If there is an update, the Infotainment System downloads the update, forwards it to the Driving Controller, and both systems replace their firmware with the updated one. The query and update is scheduled to happen

automatically every night at 23:55 provided the car is at a stop and the engine is turned off. The manufacturer plans on neither confidentiality nor integrity checks for the update process.

Question D1

Your answer to this question counts 20% towards the final grade.

1. Assume the firmware is transmitted in the clear and not integrity protected. Outline a denial-of-service attack on this system.
2. Assume that the firmware itself is *not* confidential. Describe how to add integrity protection to the firmware update system using cryptographic primitives.
3. Assume that the firmware itself is confidential. Describe how to additionally add confidentiality protection to the firmware update system.

Report your answers to these three questions. Submit at most 500 words in total.

Question D2 (Risk analysis)

Your answer to this question counts 20% towards the final grade.

Write an abbreviated risk analysis for the firmware update system *including* both the integrity and confidentiality protections.

You may hypothesise details of the system and must stipulate yourself its security requirements. Be sure to cover System, Stakeholders, Assets, Vulnerabilities, Threats, and Risk. You may find Chapter 8 of the course book helpful.

Report your analysis as the answer to this question. Your answer is expected to consume at most 500 words.

(End of questions.)

Tue Aug 28 12:04:37 CEST 2018