SECURITY FALL 2018

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, D2, and D3. 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. 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.

Authentication and Access Control

Question 1-1

You have to login to your email account from a computer on an Internet Cafe. You cannot trust the computer but you do not worry too much because you set your email account with

1. Strong password authentication (more than 8 characters)
2. Single Sign On
3. PIN authentication with maximum 3 failures
4. One Time Password

Question 1-2

A bank wants that customers who login by single-factor authentication can only download bank statements, while customers who logins by two-factor authentication can make any banking operation. Which security goal has been de-emphasised?

1. Confidentiality
2. Availability
3. Authentication
4. Integrity

Question 1-3

You are in charge of developing a secure operating system where you want to enforce fine granularity of access control in support of the principle of least privilege. Which of the following approaches fits better with your goal?

1. Access Control List
2. Capability List
3. Attribute-based Access Control
4. Discretionary Access Control

Cryptography

Question 2-1

Let S be a binary string of length N (i.e. S \= s0 s1 s2 ... sN). Let K be a truly random binary string of length N (i.e. S \= s0 s1 s2 ... sN). The encryption C of S is done by the function `ci\=si + ki mod 2`, bit by bit. Is this cipher secure?

1. Yes
2. Yes, but only if S <> K
3. Yes, but only if N is big
4. No

Question 2-2

You are developing your own block cipher and want to ensure that, given two plaintexts P1 and P2 differing on a single bit, the two corresponding ciphertexts C1 and C2 differ with high probability for at least half of their bits. To get some inspiration you should look to which function(s) of AES?

1. Add Round Key
2. Substitute Bytes
3. Shift Rows and Mix Columns
4. Key Expansion

Question 2-3

The word “security” has the SHA-1 hash value of “8eec7bc461808e0b8a28783d0bec1a3a22eb0821”. Given the SHA-1 hash value “8eec7bc461808e0b8a28783d0bec1a3a22eb0822”, to calculate the corresponding word we need to

1. There is no easy way to find the corresponding word
2. To know the key used by SHA-1
3. Hash twice the word “security”
4. Try all combinations of words that start with “securit”

Question 2-4

You are given a transcription of a pair of RSA keys that are generated with the parameters outlined below.

- p

```
1208094633628121882036524566217509042101983282913575302801026
4768682001051530457738188435136484264867139654649231057390628
058463657296412521949387008096847
```

- q

```
1024618986308523081192987658279122237435546089735652471755243
2500150646746478820178508652542022282425161457760873208466755
125173780872021573759325872701418
```

- N

```
1237836698872812822596337141614766445990918671766343261781893
0259622623463352215416741935355688552228351295973933433150783
6581303720202583078143533976561574216976586643194117012672498
9430989794516456108018586343153374777841940447076687780805858
0197337425413640569093008067285043406885146897711359578385013
2199
```

- d

```
5186346325640259287985843351328237764997579353347272475894380
3652742361975706621164886522564635542615362045279496794312734
5573648298372328416427865093367663051883240647592475374095918
9387020810462099869168228060879728241452169595939873144528243
5452883127775688820028320628315535187698213522296232068629124
625
```

- e

```
65537
```

You spot that there is an error with one of the parameters. Which one? Recall that N\=pq is the modulus, d is the private exponent, and e is the public exponent.

1. p
2. q
3. d
4. e

Question 2-5

A digital signature primitive is constructed similarly to plain RSA public key encryption, in which

- the plain RSA encryption algorithm serves as signing algorithm
- the plain RSA decryption algorithm servers as verification algorithm

This is a weak construction because { ~ plain RSA does not provide confidentiality, hence the message is not secret ~ plain RSA is one-way, hence a signature cannot be verified. ~ plain RSA does not provide availability, hence it does not guarantee Anti-DoS = plain RSA is malleable, hence it does not guarantee origin of a message }

Security protocols

Question 3-1

Alice can use asymmetric encryption to send a secret message to Bob provided that { ~ They use the same (secure) hash function ~ The message space is smaller than the size of the public key = Alice knows the public key and Bob knows the private key ~ Bob knows the public key and Alice knows the public key }

Question 3-2

Below is the full version of the asymmetric-crypto Needham-Schroeder protocol. Which goal does it fail to achieve?

```
A->S: A,B
S->A: {Kb, B} signS
A->B: {Na, A}Kb
++++++++++++
B->S: B,A
S->B: {Ka, A} signS
B->A: {Na,Nb}Ka
A->B: {Nb}Kb
```

1. Confidentiality of Kb
2. Authentication of S to B
3. Authentication of A to B
4. Authentication of B to A

Question 3-3

In Kerberos, which party or parties derive(s) keys from the password of the client?

1. Only the client

2. The client and the Authentication Server
3. The client, the Authentication Server, and the Ticket-granting server
4. The client, the Authentication Server, the Ticket-granting server, and the Application Server.

Question 3-4

Digital certificate are useless in

1. Symmetric cryptography
2. Asymmetric cryptography
3. HTTPS
4. None of the above

Question 3-5

You are the CTO of a start-up company and want to get a digital certificate for the company website. Which options below provides the website visitors more certainty that the website really is controlled by the company?

1. A certificate from a third party with support to Extended Validation
2. A certificate from a third party with support to Domain Validation
3. A wildcard certificate from a third party
4. A self-signed certificate

Question 3-6

Which of these entity or entities in a PKI know(s) the private key corresponding to the server's public key in that server's digital certificate?

1. Only the Root CA
2. The Root and the Intermediate CAs
3. The corresponding client
4. None of the above

Security protocols (2)

Question 4-1

Which of these proposal aims at mitigating the security issue due to a compromised Certification Authority

1. OCSP
2. CRLset
3. OneCRL
4. Certificate Transparency

Question 4-2

Which of the following phrases better describes Certificate Transparency?

1. Proactive approach
2. Reactive approach
3. Privacy-preserving approach
4. Anti-DoS approach

Question 4-3

Which of these is a building block for many security protocols?

1. Needham-Schroeder
2. Hash functions
3. Kerberos
4. TLS

Question 4-4

The TLS Alert Protocol sends a fatal alert if

1. The CA has been compromised
2. The server does not support Certificate Transparency
3. The client does not support Certificate Transparency
4. An integrity check fails

Question 4-5

If you want to establish a session key through asymmetric encryption, you would use

1. AES
2. Hash functions

3. Kerberos
4. TLS

Question 4-6

Which of the following statements about TLS is correct:

1. If the server does not require the client certificate, the server should completely ignore the client_hello message
2. If the client does not require the server certificate, the client should completely ignore the server_hello message
3. If both client and server do not require certificates, the handshake protocol can be skipped
4. In any case, both client_hello and server_hello should never be ignored

Network security

Question 5-1

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

1. Password
2. Connect
3. Ping
4. Idle

Question 5-2

You are asked to do a security audit of Naive Corp. You use nmap to scan a webserver, and you find the following:

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

On which port should I try common user/password combinations?

1. 22
2. 80
3. 443
4. 8023

Question 5-3

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 and 8023. What should I do?

1. Close port 8023
2. Filter all ports
3. Filter port 8022
4. None of the above

Question 5-4

A reflection attack is a form of

1. DNS Spoofing
2. Denial of service
3. Port scanning
4. Injection

Question 5-5

An amplification attack is a form of

1. DNS Spoofing
2. Denial of service
3. Port scanning
4. Injection

Binary exploitation

Question 6-1

I wrote the following C program:

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

Question 6-2

I'm trying to construct a buffer overflow for a C program, and I've used a debugger to determine that just prior to reading unlimited input into a bounded buffer, my stack looks like this:

```
0xbffad5d0:     0x00000000      0x0804865b      0x0000000a      0x00000000
0xbffad5e0:     0x42424242      0x00000000      0x00000000      0x00000000
0xbffad5f0:     0x00000000      0x00000000      0x00000000      0x00000000
0xbffad600:     0x00000000      0x00000000      0x00000000      0x00000000
0xbffad610:     0x00000000      0x00000000      0x00000000      0x00000000
0xbffad620:     0x00293ff4      0x00000000      0xbffff748      0x0810556b
0xbffad630:     0xbffff640      0x00118fa6      0x0012bff4      0x00000000
0xbffad640:     0x00000000      0x000000ca      0x00000006      0xbffff68c
```

The debugger tells me that the return address is saved at address 0xbffad62c, with value 0x0810556b. It also tells me that the buffer I'm trying to overflow starts at address 0xbffad5e0. I've determined myself that I'd rather have the program return to 0x080485c5. What input should I provide to the program in order to overflow the buffer?

1. 17*4=68 non-zero bytes followed by "\xc5\x85\x04\x08"
2. 18*4=72 non-zero bytes followed by "\xc5\x85\x04\x08"
3. 19*4=76 non-zero bytes followed by "\xc5\x85\x04\x08"

4. 20*4=80 non-zero bytes followed by "\xc5\x85\x04\x08"

Discussion Questions

Question D1

Your answer to this question counts 15% towards the final grade.

The IT department is considering to introduce multi-step authentication to protect their users. In the proposed multi-step authentication, each user picks *any two* authentication methods from the list below at each login.

1. Password
2. Fingerprint recognition
3. Student card
4. SMS via phone
5. Call via phone
6. Email confirmation
7. Iris Scanning

Give a recommendation: Should this policy be adopted or not? Discuss and motivate your recommendation.

Question D2

Your answer to this question counts 15% towards the final grade.

The IT department at ITU is considering new password rules to protect their users. Any password must satisfy all of the following rules:

1. Passwords must be longer than 8 characters
2. Passwords should not be dictionary words
3. Passwords must contain at least two non-consecutive digits, two non-consecutive capital letters, and exactly one special character
4. Passwords must be changed at least every semester
5. “Paste” functionality is disabled in every login page related to ITU when entering a password.

Give a recommendation: Should this policy be adopted or not? Discuss and motivate your recommendation.

Question D3

Your answer to this question counts 10% towards the final grade.

A vendor of software solutions for practicing doctors ("GPs", "praktiserende læger") offers an on-line appointment module. Patients authenticate themselves to the system with their CPR-number and an automatically-generated password that the doctor provides to the patient over the phone or during a consultation. Once authenticated, the patient is shown a list of open slots in the immediate future, and a link to PDF-version of his patient records.

Write an abbreviated risk analysis for the on-line appointment module.

(End of questions.)
