+1/1/60+

COM 301 Final Exam, 24.01.2020

Name: **Chris P. Chicken**

Sciper: **123123**

Please wait for instructions before opening this document

- This is a **closed book** exam. Books, notes and electronic devices are not allowed.

Multiple choice questions:

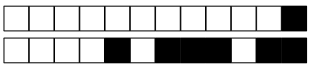
- There are 20 multiple choice questions, each worth 1 point.
- Only one answer is correct; *there is a 0.25pt penalty for wrong answers*
- Make a mark *inside* the box corresponding to your answer
- Use a black or blue pen to mark your answers. Pencils are not allowed.
- Use white-out fluid or tape if you ticked the wrong answer.
- If you white-out a wrong answer, do not try to re-draw the boxes.

Open text questions:

- There are 15 open text questions, each worth 2 points.
- Please write your answers in the corresponding text boxes.
- Do not write more than the lines specified in the box. Any text outside of the boxes **will be ignored**.
- Do not tick the grading boxes of the top of the text boxes.
- Please mind your calligraphy; undecipherable responses will not be graded.

Questions

- The supervisors will not answer any questions regarding the content of the exam questions



Part 1: Multiple-choice questions
Mark the correct answer by *completely* filling in the corresponding square (■).
There is **only one** correct answer per question.
Each correct answer earns +1 point. Incorrect answers have a penalty of -0.25 points each. No answer neither adds nor subtracts points. Multiple marked answers are considered incorrect and will result in -0.25 points.
Use white-out fluid to change (delete) an answer (other deletion methods yield -0.25).
Read the answers carefully; the template may split the answers across columns.

Question 1 **[Authentication]** Gru decides to build a homemade authentication system for his minions. Gru wants to try alternative approaches to passwords and listed four substitutes. Minions are very friendly, and tend to hang out in big groups to party and eat bananas. Which authentication method provides Gru with the *least* assurance of the identity of a Minion?

- ☐ User's behaviour
- ☐ Biometric
- ☐ User's social ties
- ☐ Smart cards

Question 2 **[Attacks]** A system implements Data Execution Prevention, Stack Canaries, and Address Space Layout Randomization. This guarantees that software running in this system will not contain exploitable vulnerabilities. This statement is:

- ☐ True, as these defenses eliminate control flow attacks.
- ☐ False, no existing defense guarantees absence of bugs.
- ☐ False, that only happens if the system is also checked using fuzzing.
- ☐ False, that only happens if the system also implements Safe exception handlers.

Question 3 **[Access Control]** The office Boss keeps a log of when employees enter work. To indicate they have arrived, employees must execute the script `update`. Assume that the Boss sets the permissions as follows:

```
-rwx--x---  Boss Employees update
-r-x------  Boss Employees entrylog
```

The Boss asks you whether the configuration will ensure that all arrivals get logged and employees cannot delete them. Which of the following would be a correct answer:

- ☐ No, the employees cannot delete logs, but they cannot add new entries
- ☐ No, the employees cannot delete the logs, but they can add fake entries
- ☐ Yes, this configuration achieves the goal
- ☐ No, the employees can delete logs

Question 4 **[Security Principles]** Which of the following approaches is NOT defense in depth:

- ☐ Checking a password and a code sent via SMS to access a web
- ☐ Having a bastion host behind a firewall
- ☐ Using two antivirus from different companies to analyze suspicious files
- ☐ Checking the PIN and 9999 – PIN to unlock the phone, where PIN is a 4-digit number input by the user

Question 5 **[Access Control]** Which of the following security violations is NOT caused by a confused deputy?

- ☐ A hacker performs Cross-site Request Forgery to gain access to a user's social network account
- ☐ A virus infects an email client to send spam
- ☐ A journalist tricks a banker into revealing the bank statements of a famous singer
- ☐ A detective leaks information to a criminal using a covert channel

Question 6 **[Network Security]** Alice wants to post a photo on instagram.com while at work, but she does not want her company's IT team to learn about her activities. She uses DNSSEC to obtain the IP address for instagram.com, and HTTPS to connect to the website. With this configuration, which of the following statements is true?
Note: Assume that Alice's Instagram account is protected/private.

- ☐ The IT team will know that Alice is trying to visit instagram.com and may prevent this by spoofing the DNS record returned to Alice.
- ☐ The IT team will not know that Alice is visiting instagram.com, since DNSSEC and HTTPS provide confidentiality.
- ☐ The IT team will know that Alice visited instagram.com, and also which photo she posted.
- ☐ The IT team will know that Alice visited instagram.com, but will not know which photo she posted.

Question 7 **[Privacy]** In which scenario does encryption of communication help?

- ☐ Hiding which record you are retrieving from the database provider
- ☐ Hiding the identity of the receiver from the Internet Service Provider when sending an email via your Gmail account
- ☐ Hiding who you are calling from the Telco provider when making a phone call
- ☐ Hiding the message receiver from Telegram when using Telegram's secret chat

Question 8 **[Security Policies]** Assume that a university uses the Bell-LaPadula model. The classification labels are public $<$ limited $<$ confidential, and the categories are {teaching, research, admin}. Which of the following statements is true:

- ☐ A principal with the security level (confidential, {teaching}) can read a file with the level (public, {admin}).
- ☐ The security level that gives the most privileges for writing is {public, {}}.
- ☐ A principal with the security level (confidential, {teaching}) write to a file with the level (public, {admin}).
- ☐ The security level that gives the most privileges for writing is {public, {teaching, research, admin}}.

Question 9 **[Malware]** Which of the following malware types is self spreading and does not require a host program?

- ☐ Trojan
- ☐ Keylogger
- ☐ Virus
- ☐ Worm

Question 10 **[Access Control]** Simon is the owner of Color OS, a simple OS that has 4 files: `red`, `yellow`, `green`, and `blue`. Simon says that a user Harry can read the file `red`, can write `yellow`, and can read and execute `blue`.
What is the capability that Simon should give to Harry?

- ☐ red: {(Harry, read, no write/execute)}, yellow: {(Harry,write, no read/execute)}, blue: {(Harry, read/execute, no write)}.
- ☐ red: {(Harry, read)}, yellow: {(Harry,write)}, blue: {(Harry, read/execute)}.
- ☐ Harry: {(red, read), (yellow,write), (green,"), (blue, read/execute)}.
- ☐ Harry: {(red, read), (yellow,write), (blue, read/execute)}.

Question 11 **[Privacy]** A VPN can hide the destination of your communication against an adversary looking at your local traffic. What would be the advantage of using Tor if a VPN can already do that?

- ☐ To prevent trust centralization
- ☐ To eliminate traffic analysis attacks
- ☐ To protect against weak cryptographic keys
- ☐ To reduce latency

Question 12 **[Authentication]** Consider the following authentication exchange in which Spock uses his password 'LongAndProsper' to prove his identity to Kirk:

```
Spock ----    (Spock, 'I want to login')     ----> Kirk
Spock <---         Hash(Spock)               ----- Kirk
Spock ---- Enc('LongAndProsper', Hash(Spock)) ----> Kirk
```

Which of the following statements is correct?

- ☐ Hash(Spock) is not a good challenge because it will be used every time
- ☐ Hash(Spock) is not a good challenge because anyone can compute it
- ☐ The protocol is bad because the login is sent on the first message
- ☐ Hash(Spock) is a good challenge because hashes output random numbers

Question 13 **[Security Policies]** Alice and Bob work for a company with a Chinese Wall security policy with clients in the following companies (each group indicates competing companies):

- Apple, Facebook, Microsoft
- HBO, Netflix, Disney
- Prada, Armani
- Lindt, Frey

Alice has previously worked on cases for Frey and Microsoft, while Bob works with Facebook and Prada. Alice is ready for a new assignment. According to the policy, which options are available to her:

- ☐ Armani, Frey
- ☐ Prada, Armani
- ☐ Armani, Facebook
- ☐ Prada, Frey

Question 14 **[Network Security]** Alice subscribed to a digital diary site. She is worried that her roommate might try to read her diary. She went through the COM-301 material to learn what attacks her roommate could launch. She made a shortlist of worrisome attacks and asked you to confirm. Which attack would you remove from the list?

- ☐ BGP hijacking
- ☐ ARP poisoning
- ☐ Looking over the shoulder
- ☐ DNS hijacking

Question 15 **[Network Security]** Alice has designed a private file-sharing protocol over HTTPS (on the same port as typical applications). Which of the following firewall types can block the file-sharing connections without impacting other protocols over HTTPS?

- ☐ Stateless
- ☐ Stateful
- ☐ Both stateful and stateless
- ☐ Neither stateful nor stateless

Question 16 **[Attacks]** Which of the following approaches does NOT help to ensure that you do not run adversarial code in the Trusted Computing Base?

- ☐ Make sure code updates are signed.
- ☐ Sanitize the compiler code before compiling updates.
- ☐ Only accept updates encrypted with your public key.
- ☐ Check for new updates using an antivirus.

Question 17 **[Software Security]** Alice has used two test cases {a = -1, b = -1},{a = 1, b = 1} to test the following program. What is the maximum level of coverage that this test achieves?

```
1. int test(int a, int b) {
2.      if(a < 0)
3.          b += 1;
4.      if(b == 1)
5.          return 0
6.      else
7.          return 1;
8. }
```

- ☐ Path coverage
- ☐ Statement coverage
- ☐ Branch coverage
- ☐ Method coverage

Question 18 **[Applied cryptography]** CBC encryption mode can not achieve:

- ☐ Parallel encryption
- ☐ Limiting error propagation in transmission
- ☐ Parallel decryption
- ☐ Confidentiality

Question 19 **[Security Principles]** Dany and Jorah decide to hide a dragon egg inside a crypt. The crypt has two locks and can be opened only if both locks get unlocked. Dany has the key to one lock and Jorah has the key to the other. What security principle did Dany and Jorah follow to decide on this mechanism?

- ☐ Least common mechanism.
- ☐ Least privilege.
- ☐ Complete mediation.
- ☐ Separation of privilege.

Question 20 **[Security Policies]** David and Robert are co-workers. They have started dating and they don't want the people in their office to know about their relationship, including the system administrators that inspect the network traffic and the corporate email server to avoid information leaks. What is a good *covert channel* to agree on the time for their next date:

- ☐ Sending the meeting time in an email through Tor
- ☐ Writing the meeting time on the door of the restroom
- ☐ Encoding the meeting time in whitespaces added to the corporate emails they send to each other for work
- ☐ Sending the meeting time in an encrypted corporate email

Part2: Short answer questions: Write your answer using *only* the lines provided. Anything beyond the specified number of lines will not be considered for grading.
Answers are graded on a scale from 0 to 2.
Please mind your calligraphy; undecipherable responses will not be graded.

[Applied cryptography] Alice decides to design her own secure messaging app. The application sends each message m as follows:

$$key, Sign(Sk\_A, key), Enc(key, m), MAC(key, m)$$

Sk_A : Alice's secret key.

Sign : Signs a message with a secret key.

key : A symmetric key.

Enc : Encrypts a message with a symmetric key.

MAC : Computes the MAC of a message with the specified symmetric key.

Question 21 Does this protocol protect the integrity of the message m from an active adversary that can intercept messages? Justify your answer. ☐**0** ☐**0.5** ☐**1** ☐**1.5** ☐**2**

.....

.....

.....

Question 22 Can a sender in Alice's application repudiate having sent a message m to another sender? Justify your answer. ☐**0** ☐**0.5** ☐**1** ☐**1.5** ☐**2**

.....

.....

.....

Question 23 For the properties that are not provided, provide a fix. You can use any cryptographic primitive seen during the course.
Hint: we expect a protocol line in the same style as the one in the question.

☐0 ☐0.5 ☐1 ☐1.5 ☐2

.....

.....

Question 24 **[Malware]** After taking an entrepreneurship class, Alice registers a new start-up that designs and sells antivirus. In her first attempt to building an antivirus, Alice gathers a large data set of viruses and hashes their binary. Whenever the antivirus scans a program, it hashes the binary and checks whether this hash is a known virus. Describe one method to bypass this antivirus, and one countermeasure to avoid the bypass.

☐0 ☐0.5 ☐1 ☐1.5 ☐2

.....

.....

.....

.....

[Network Security] John Oliver has aired a new show to expose the evil nature of Evil corp, the owners of Evil Service Provider, a famous ISP with millions of users. Since seeing this video may lead to loss of customers, the corporation decides to block access to this content through its provider.

Question 25 Describe one method that the Evil Service Provider can use to prevent its customers from accessing the show.

☐0 ☐0.5 ☐1 ☐1.5 ☐2

.....

.....

.....

Question 26 Can Evil Service Provider's users bypass the censoring which you designed in the previous part? Justify. *Assume that Evil Service Provider is the only ISP available to the users.*

☐0 ☐0.5 ☐1 ☐1.5 ☐2

.....

.....

.....

Question 27 Seeing that users are being censored, Good corp deploys a new ISP that does not do blocking. Since the users love John Oliver, they decide to switch to Good corp's ISP. Evil corp wants to ensure that any John Oliver lover suffers, so they decide to lower the quality of the user's access to the show without harming other users of Good corp. Is this possible? Justify.

☐0 ☐0.5 ☐1 ☐1.5 ☐2

.....

.....

.....

Question 28 **[Authentication]** You are hired at WhoAreYou.com to audit their authentication system. They use login and password, and their main engineers store every password in a file `securepass.txt` where each line reads:
`H(password || k), salt`
where k is a symmetric key stored in another file on the same machine.
Does this scheme protect the confidentiality of the passwords if an adversary compromises the machine hosting the file `securepass.txt`? Justify your answer ☐0 ☐0.5 ☐1 ☐1.5 ☐2

.....

.....

.....

Question 29 **[Privacy]** The city of Lausanne selects 100 citizens to help with a study on urban mobility. These users carry a device that records their location continuously during a week. Agree or disagree with the following statement (Justify your answer):
The city of Lausanne can build an anonymized version of the citizens' trajectories and publish it without endangering the citizens' privacy. ☐0 ☐0.5 ☐1 ☐1.5 ☐2

.....

.....

.....

.....

Question 30 **[Access Control]** Alice can read the file `xxx.sys`, read and execute the file `yyy.sys`, and has no access to the file `zzz.sys`. Bob can write and execute `xxx.sys`, cannot access `yyy.sys`, and can read `zzz.sys`. Charlie cannot access `xxx.sys` or `yyy.sys`, but can read `zzz.sys`.

Provide the set of access control lists. ☐0 ☐0.5 ☐1 ☐1.5 ☐2

.....

.....

.....

.....

[Applied cryptography] Bob publishes a new game on his website that users can download. He loves open source, so he also publishes the source of the game. He also publishes the hash of the game executable, so that users can verify that they have the correct version.

Question 31 Assume that Bob is an amazing programmer and never has a bug in his code. He is also trustworthy and publishes the correct hash. Charlie wants to get compensation from Bob by claiming that Bob published a game with bugs. As there are no bugs, Charlie inserts a bug into the game code. What are the minimal property/properties of the hash function which enable Bob to show that Charlie is cheating?

☐0 ☐0.5 ☐1 ☐1.5 ☐2

.....

.....

.....

.....

Question 32 After learning about Charlie's intentions, Bob is furious and wants to take revenge. Bob wants to send a rigged version of his new game to Charlie which ensures that Charlie will always lose in a humiliating way. Bob still wants to release the healthy version of the game and its hash to the public. Bob knows that Charlie always checks the hash of programs before installing them. Which hash property/ies may prevent Bob from getting his revenge?

☐0 ☐0.5 ☐1 ☐1.5 ☐2

.....

.....

.....

.....

[Attacks] AwesomeWebsite.com/hello.php has the following PHP code:

```
$userid = $_GET['userID'];
echo '<div class="header">Hello, '.$userid.'</div>';
```

Question 33 Write a URL to inform a third party, http://iamcharlie.com, of the cookie of the user visiting the page. ☐0 ☐0.5 ☐1 ☐1.5 ☐2

.....

.....

Question 34 What instructions would you give to the programmer to fix this? ☐0 ☐0.5 ☐1 ☐1.5 ☐2

.....

.....

.....

.....

Question 35 **[Software Security]** Rick is learning to program and has written the code below. The function gives users a login based on a `username` input on the keyboard by the user and prints a transformed version according to an input parameter `trasnformPos`. Because he is afraid of his code having vulnerabilities, he has enabled *stack canary* protection.

```
1. int transformName(int transformPos) {
2.       char username[10];
3.       char newname[10];
4.
5.       printf("Enter your username : ");
6.       gets(username);
7.
8.       for (int i = 0; i < 10; i++) {
9.          if (i < transformPos) { newname[i] = username[i]; }
10.          else { newname[i] = username[transformPos-i]; }
11.      }
12.
13.      printf("Your new username is: \%s\n", newname);
14.
15.      return 0;
16. }
```

Identify one *exploitable* vulnerability in the code. Please provide the line number and explain i) how you can exploit the vulnerability and ii) what can be achieved exploiting it.

☐ **0** ☐ **0.5** ☐ **1** ☐ **1.5** ☐ **2**

.....

.....

.....

.....