UNIVERSITY OF WATERLOO
Cheriton School of Computer Science

CS 458/658 **Computer Security and Privacy** **Spring 2018**
Hassan Khan

ASSIGNMENT 2

Assignment due date: **July 4, 2018 3:00 PM**

Total Marks: 56
Written Response Questions TA: Jiayi Chen (jiayi[dot]chen[at]uwaterloo[dot]ca)
(Office hours: Fridays 14:00–15:00 in DC 3333)
Programming Questions TA: ()
(Office hours: Mondays 11:30–12:30 in DC 3333)

Please use Piazza for all communication. Ask a private question if necessary. The TAs' office hours are also posted to Piazza for reference. You are expected to follow the expected Academic Integrity requirements for Assignments; you can find them here: https://uwaterloo.ca/library/get-assignment-and-research-help/academic-integrity/academic-integrity-tutorial. Strict penalties will be enforced on students for any Academic Integrity violations.

Written Response Questions [24 marks]

Note: Please ensure that written questions are answered using complete and grammatically correct sentences. You will be marked on the presentation and clarity of your answers as well as on the correctness of your answers.

1. Hashing Password

Alice is designing a secure account database for an Online Social Networking website. Her idea is to only store password fingerprints by using a hash function so that the attacker cannot know the plaintext of passwords even if the database is compromised. Here is the outline of her scheme.

1. Generate an 8-bit random salt $\mathcal{S}$ for each password entry $\mathcal{P}$,
2. Compute the SHA-1 hash function $\mathcal{H} = \text{SHA1}(\mathcal{P} + \mathcal{S})$, and store $\mathcal{S}$, $\mathcal{H}$ in the database,
3. When a user logs into the website, verify the input password $\mathcal{P}^*$ by checking if $\mathcal{H} - \mathcal{S}$ is equal to $\text{SHA1}(\mathcal{P}^*)$.

(2 marks) a. What attacks can a salted hash defend against? Why should we use a random or user-specific salt?

Dictionary attacks and rainbow table attacks.

A user-specific salt prevents the situation that two identical passwords have the same hash.

(6 marks) b. Please find three problems in the scheme and provide necessary explanations or corrections.

1. the salt length is too small. It is possible to generate a rainbow table with all possibilities.

2. SHA-1 is now vulnerable to collision attacks (e.g., PDF collision). SHA-1 is too fast. A time or memory consuming hash function can slow down the attacks. It is better to use the hash functions like bcrypt, scrypt.

3. Due the property of hash, it is invalid to operate on the hash directly. To verify the input password $\mathcal{P}*$, one should compare the hash of input and password by checking if $\mathcal{H}$ is equal to $SHA1(\mathcal{P}^*)$.

2. Security Policies & Models

In Organization X, all documents have one of the following four sensitivity/clearance levels:

$$\text{Top Secret (TS)} >_c \text{Secret (S)} >_c \text{Confidential (C)} >_c \text{Unclassified (U)}, \quad (1)$$

where "$>_c$" means "more sensitive". Besides, most of them are assigned to one or more compartments for access control. Assume that there are 5 kinds of compartments, namely A, B, C, D, and E. If the document does not belong to any compartment, its compartment field will denoted as $\emptyset$. Please answer the following questions.

(5 marks) a. Suppose that the organization adopts the Bell-La Padula confidentiality model. Agent Bob is granted the clearance level (Secret, {A, C, E}). Please indicate whether he has read access, write access, both of them, or neither to each of the following documents.

- D101: (Unclassified, {A, E})
- D102: (Secret, {B})
- D103: (Top Secret, {A, C})
- D104: (Confidential, {A, C, E})
- D105: (Top Secret, {A, B, C, D, E})

D101: read D102: neither D103: neither D104: read D105: write

(5 marks) b. Suppose that the organization adopts the dynamic Biba integrity model (i.e., using the low watermark property for both subject and object). Carol has the integrity level (Secret, {B, D, E}) and Eve has the integrity level (Confidential, {B, C, D}). Please describe the change in the integrity level (with compartments) of either subject or object after each operation in the following sequence. Note that the integrity change resulted from the former operation will be kept in the latter ones.

(i) Carol writes to D201: (Secret, {A, D, E})

(ii) Carol reads from D202: (Top Secret, {A, B, D, E})

(iii) Eve reads from D203: (Unclassified, {B, C, E})

(iv) Eve writes to D204: (Secret, {C, D})

(v) Carol reads from D204

i. D201: (Secret, {D, E}) ii. No change in Carol's Integrity iii. Eve: (Unclassified, {B, C}) iv. D204: (Unclassified, {C}) v. Carol: (Unclassified, $\emptyset$)

3. Firewall

Suppose that you work at the IT security department of a certain company and the firewalls within the company network happen to be reset. The IP addresses of all devices in the company network are in the form of 11.22.x.x.

(2 marks) a. A series of IP packets with malicious code from outside the company network are intercepted. You simply check their IPv4 headers and find that their source IP addresses are all 11.22.3.4. What kind of attack is it? What kind of firewalls can be used to defend against it?

IP spoofing attack (non-internal network IP is spoofing an internal one). Packet filtering gateway is sufficient to defend against this attack.

(2 marks) b. Later, you notice that a lot of TCP/SYN packets from invalid source IP addresses are sent to the web server of your company. What harmful consequence may it result in? How does it work?

As the response of TCP/SYN packets, the server will send back SYN-ACK packets and wait for another response packet. However, since the IP addresses are invalid, there won't be any response. As a result, the server can hardly respond to legal requested and web services of the company will become inaccessible.

(2 marks) c. To protect the web server from this attack, you set up a stateful inspection firewall. However, you notice that there is still some connection problem of accessing the web services. Please analyze the potential reason for this failure.

Since the stateful inspection firewall needs to analyze and identify the incoming packets, it consumes a lot of CPU resources to do that. When there is a huge amount of SYN flooding from different IP addresses, it will become a problem. The CPU resource of the firewall is exhausted and the inspection of packets will affect the services. Also, the cache table overflow is another potential reason. If the firewall does not have enough memory to cache all established flows, it may drop the connections.

What to hand in

Using the "submit" facility on the student.cs machines (**not** the ugster machines or the UML virtual environment), hand in the following files:

a2.pdf: A PDF file containing your answers for all written questions and programming questions when requested. It must contain, at the top of the first page, your name, UW userid, and student number. **-3 marks if it doesn't!** Be sure to "embed all fonts" into your PDF file. Some students' files were unreadable in the past; if we can't read it, we can't mark it.

exploit{1_{a,b,c},2,3}.tar: Tarballs containing your exploits for the programming portion of the assignment. To create the tarball, for example for the first question, which is developed in the directory `exploit1_a/`, run the command

```
tar cvf exploit1_a.tar -C exploit1_a/ .
```

(including the `.`).