# Assignment 3

SENG 2250

–

System and Network Security

Cheuk Hang Ku

C3291914

## Assignment Cover sheet

# ASSIGNMENT/ASSESSMENT ITEM COVER SHEET

**Student Name:** Cheuk Hang | **Ku**

FIRST NAME | FAMILY / LAST NAME

**Student Number:** 3 2 9 1 9 1 4 Email: c3291914@uon.edu.au

| Course Code | Course Title |
|---|---|
| S E N G 2 2 5 0 | **System and Network Security** |
| *(Example)* A B C D 1 2 3 4 | *(Example)* Intro to University |

Campus of Study: Callaghan (eg Callaghan, Ourimbah, Port Macquarie)

Assessment Item Title: Assignment 3 Due Date/Time: 12th Oct

Tutorial Group (If applicable): Word Count (If applicable): 1513

Lecturer/Tutor Name:

Extension Granted: ○ Yes ⦿ No Granted Until:

Please attach a copy of your extension approval

**NB: STUDENTS MAY EXPECT THAT THIS ASSIGNMENT WILL BE RETURNED WITHIN 3 WEEKS OF THE DUE DATE OF SUBMISSION**

**Please tick box if applicable**

☒ *Students within the Faculty of Business and Law, Faculty of Science and Information Technology, Faculty of Engineering and Built Environment and the School of Nursing and Midwifery:*
I verify that I have completed the online Academic Integrity Module and adhered to its principles

☐ *Students within the School of Education:*
"I understand that a minimum standard of correct referencing and academic literacy is required to pass all written assignments in the School of Education; and I have read and understood the School of Education *Course Outline Policy Supplement*, which includes important information related to assessment policies and procedures.

I declare that this assessment item is my own work unless otherwise acknowledged and is in accordance with the University's academic integrity policy available from the Policy Library on the web at http://www.newcastle.edu.au/policylibrary/000608.html
I certify that this assessment item has not been submitted previously for academic credit in this or any other course. I certify that I have not given a copy or have shown a copy of this assessment item to another student enrolled in the course.

I acknowledge that the assessor of this assignment may, for the purpose of assessing this assignment:
- Reproduce this assessment item and provide a copy to another member of the Faculty; and/or
- Communicate a copy of this assessment item to a plagiarism checking service (which may then retain a copy of the item on its database for the purpose of future plagiarism checking).
- Submit the assessment item to other forms of plagiarism checking.

**DATE STAMP HERE**

Insert this way

I certify that any electronic version of this assessment item that I have submitted or will submit is identical to this paper version.

Turnitin ID: (if applicable)

Signature: Cherren Date: 23rd Sept

To copy and paste the completed form into another document use the "snapshot" tool. Print Form

THE UNIVERSITY OF NEWCASTLE AUSTRALIA

## Table of Contents

# Task 1

## Q1) Analyse potential security threats and issues of this system.

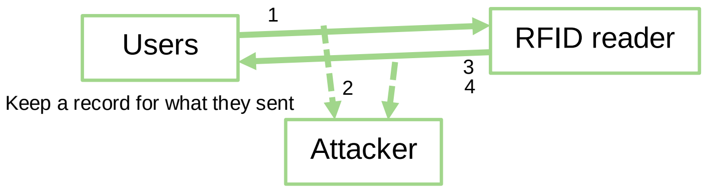
DoS (Denial of Service) attacks, replay attacks and physical attacks are the potential threats in the system. To justify the potential threats above.

DoS attack:

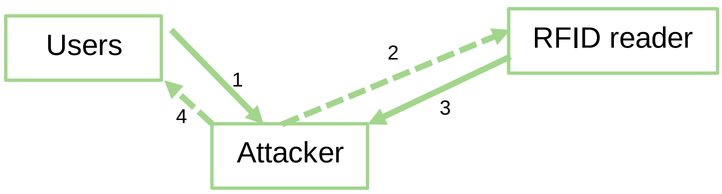
When the reader request information from a tag, it receives the identification id and send the data to the could server and compares the id with the one stored in the could server. Both RFID reader and the could server are vulnerable to DoS attacks. When attackers start the DoS attack, the tags fail to verify its identity with the reader and as a result the service gets interrupted. Or when the attacker tries to send too many request to the cloud server, it will cause a DoS attack as well.

Replay attacks:

Attacker intercepts communication message flowing between the reader and the tags and he records the tag’s response that can be used as a response to reader’s request.




Step 1




Step 2

Physical attacks:

When the attacker physically obtains tags and alter its information. Attacker can use a probe to read and alter the data on tags or use X-ray band to destroy data in tags, which an attacker can use to attack an RFID system-this type of attack is also known as radiation imprinting. Attackers can also remove tags from the tags physically, which makes the object unrecognizable by the RFID reader. Other than destroying the tag, attackers can also use electromagnetic which can disrupt communication between the tags and the reader.

## Q2) What technology can be used to provide client authorisation in this system?

We can use the tag and the reader to do the authorisation. The tags will contain hashed password inside, when we use the reader to read the tag, it will retrieve the hashed password, decrypted it in the reader and send it to the cloud server to verify the identity, then the cloud server send a signal back to the reader then the reader will send a signal to the access control panel, then allow user to access.

## Q3) Design a public-key based mutual authentication protocol for tag authentication.

1) The RFID reader chooses a random challenge, $r_1$, and encrypted it (hash function) then put it into the tag, once the reader scans the tag and decrypt it, it will get the random number r, then send to the cloud server.
2) The cloud server chooses a random challenge, $r_2$, It also computes $y_1 = sig_{server}(reader|| r_1|| r_2)$ and sends Cert(server), $r_2$ and $y_1$ to RFID reader.
3) RFID verifies cloud server's public key, $ver_{server}$, on the certificate Cert(server). Then he checks that $ver_{server}(reader|| r_1|| r_2, y_1)$ = true. If so, then RFID reader "accepts", then send an accept signal to access control panel; otherwise, RFID reader "rejects". RFID reader also computes $y_2 = sig_{reader}(server || r_2)$ and sends Cert(Server) and $y_2$ to Could server.
4) Cloud server verifies RFID reader's public key, $ver_{reader}$, on the certificate Cert (RFID reader). Then it checks that $ver_{reader}(Server ||r_2,y_2)$ = true. If so, then cloud server "accepts"; otherwise, cloud server decline.

| Tag | Access control panel | RFID reader | | The cloud server |
|---|---|---|---|---|
| | | Generate random number | | |
| store the random number | $H(r_1)$ | | | |
| | | Scan the number | | |
| | | decrypt the number | $r_1$ | |
| | | | | $y_1 = sig_{server}(reader\|\| r_1\|\| r_2)$ |
| | | | $r_2$, $y_1$ | |
| | | $ver_{server}(reader\|\| r_1\|\| r_2, y_1)$ = true? | | |
| | correct signal | | | |
| | allow users | | | |
| | | $y_2 = sig_{reader}(server \|\| r_2)$ | | |
| | | | $y_2$ | |
| | | | | $ver_{reader}(Server \|\|r_2,y_2)$ = true? |

## Q4) Design a symmetric-key based mutual authentication protocol to satisfy the following requirement.

The tag will store the identity and encrypted with the secrete key, then send it to the RFID reader.

Once the RFID reader received the message, it uses its own secrete key to encrypt the message and send it back to the tag.

When the tag received the message back with another secrete key in the message, it will unlock its secrete key, then send it to the RFID reader again.

Then the RFID reader will send received the message along with its own secret key, then it unlocks it, so it can read the message.

$$A \rightarrow B: E(SK_a, a_0)$$

$$B \rightarrow A: E(SK_a, a_0, SK_b)$$

$$A \rightarrow B: E(a_0, SK_b)$$

The authentication method will be similar when the RFID reader send the message to the cloud server.

First, RFID reader send the message and encrypted with its own secrete key to the cloud server.

When the cloud server received the message, it adds its own secrete key in the encrypted message and send it back.

Then the RFID reader take out its own secrete key and send it back.

The could server will know the message once it unlocks the secrete key it set earlier.

Then could server compare the message to the data base, and see it the data is valid or not, and send a signal back to the RFID reader, with the same method.

Then the signal will transfer to the access control panel.

$$B \rightarrow C: E(SK_b, a_0)$$

$$C \rightarrow B: E(SK_b, a_0, SK_b)$$

$$B \rightarrow C: E(a_0, SK_c)$$

$$C \rightarrow B: E(a_1, SK_c)$$

$$B \rightarrow C: E(SK_c, a_0, SK_b)$$

$$C \rightarrow B: E(a_1, SK_b)$$

In order to keep the key updated, the message in the tag should change every 3 months. There should be another machine (RFID reader), once the cloud server generates a new code, encrypted it and send it to the RFID reader then rewrite the code in the tag, in order to avoid man-in-middle attack, we should set up pin or password for users in order to verify the user.

The reader will first encrypt the pin by using its own private key.

Then send it to the cloud server, with the authentication I mentioned. The cloud server will first look for the pin, and see which user is going to use the tag.

Then the tag will send the encrypted message to the RFID reader and send it to the cloud server with the same authentication method.

The cloud server will verify if the pin and the massage in the tag are true. If yes, then the cloud server will encrypted the new password (for tag) and send it back to RFID reader and to the tag.

$$P \rightarrow B: E(SK_p, a_0)$$

$$B \rightarrow P: E(SK_p, a_0, SK_b)$$

$$P \rightarrow B: E(a_0, SK_b)$$

$$B \rightarrow C: E(a_1, SK_b)$$

$$C \rightarrow B: E(SK_b, a_0, SK_c)$$

$$B \rightarrow C: E(a_1, SK_c)$$

Besides, to keep the freshness of the key, we need to generate random number and the key will only last for one time only.

## Task 2

### RSA

```
Enter the plain text:
12345
Encrypting String: 12345
String in Bytes: 4950515253
Decrypting Bytes(RSA): 4950515253
Decrypted String(RSA): 12345
```

### 3DES

```
Enter the plain text:
12345
Encrypted code(DES): 2pQDM/g=
Original text(DES): 12345
```

### SHA

```
Enter Plain Text:
12345
Plain Text:12345
Hashed Value:
5994471abb01112afcc18159f6cc74b4f511b99806da59b3caf5a9c173cacfc5
```

### STS

```
client.pkey
client.skey
SENG2250.iml
SENG2250Assi
server.pkey
server.skey
```

The generated public key and secret key for both client and server side are store as a file.