CS458 - Problem Set 1

February 8, 2020

1 Problem 1 - News Story of Security Incident

In 2018, USPS website exposed data on 60 millions users. Apparently, the problem originated from an authentication weakness in the USPS API that tied to a Postal Servive initiative called "Informed Visibility". It was meant for buinesses, advertisers, and other bulk mail senders to "make better business decisions by providing them with access to near real-time tracking data". As a result, anyone logged into the usps.com was able to query the system for account details belonging to any the users. Information such as email address, usernames, user IDs, street address, phone numbers, and etc were released or available to anyone. They were also able to modified said users information.

This type of breach hit two of the big three security goals. There was definitely a loss of confidentiality since the website did not prevent unauthorized reading of information and there was a loss of integrity since the website did not prevent modification of the users' information.

The article mentions that many of those that were aware of the problem were able to obtain anyone's information for any purpose. There was an example of a user indicating that they had moved away to a new location due to an issue with neighbors and if such a breach occurred, there location was now available to their own neighbors.

2 Problem 2 - Definitions

- A. Define each of these terms: confidentiality, integrity, and availability.
  - a. Confidentiality - preventing unauthorized access of secured information
  - b. Integrity - preventing unauthorized modification of secured information
  - c. Availability - ensures data is available at all times
- B. Provide concrete example where confidentiality is more important than integrity.

  Anonymous submissions. For example, Piazza is platform that allows the students to confidently post any questions or comments anonymously. If that goal was removed, the students would lose trust within the site and no longer feel comfortable with asking questions or seeking for help.
- C. Provide a concrete exmaple where integrity is more important than confidentiality.

  Perhaps power/energy systems where a delicate balance of information/calculations is necessary to run whatever system or operation is being completed. A nuclear powerplant is another good example.

- D. Provide a concrete example where availability is the overriding concern.

  Accessing a bank account. It is important to reassure the user that their money is safe and available at all times.

3 Problem 3 - Bank Account Scenario

Q: From a bank's perspective, which is more important, the integrity of its customer's data or the confidentiality of the data? From the bank's customers, which is more important?

```
I believe confidentiality would be important for both sides. A customer would be upset if the a
```

4 Problem 4 - Scheming

Q: Sender and receiver have same key. To determine they have same key, sender generates R, XOR with K and sends to receiver. Receiver XOR R with K again, and sends back the original plaintext R to sender to confirm they have same K. Is there a flaw?

```
I think the obvious problem is that the receiver is sending back the plaintext to the original
```

5 Problem 5 - XOR Arithmetic Expressions

Given: a XOR b = c 1. a XOR a = 0 2. a XOR a' = 1 3. a XOR b' = c' 4. a' XOR b' = c 5. a XOR b XOR a = b 6. b XOR c = a

6 Problem 6 - Simple Shift Substitution

Given ciphertext: CSYEVIXIVQMREXIH

```
After doing frequency analysis, I = 3 and E = 2...Taking a wild guess, I assigned I = E, which
```

Plaintext: **YOUARETERMINATED**

7 Problem 7 - Encrypt using Double Transposition

Plaintext: We are all together; Use double transposition cipher with 4 rows and 4 columns. * Row permutation: (1, 2, 3, 4) -> (2, 4, 1, 3) * Column permutation: (1, 2, 3, 4) -> (3, 1, 2, 4)

Original:

$$\begin{pmatrix} w & e & a & r \\ e & a & l & l \\ t & o & g & e \\ t & h & e & r \end{pmatrix}$$

Row Permutation:

$$\begin{pmatrix} e & a & l & l \\ t & h & e & r \\ w & e & a & r \\ t & o & g & e \end{pmatrix}$$

Column Permutation:

$$\begin{pmatrix} l & e & a & l \\ e & t & h & r \\ a & w & e & r \\ g & t & o & e \end{pmatrix}$$

Final Ciphertext: **LEALETHRAWERGTOE**

8 Problem 8 - Computation

Q: Computer can test 2ˆ40 keys each second and the key space is size of 2ˆ128. Compute the average time taken to find the correct key.

$2^{128/2}40 = 2$ˆ88.