FINAL EXAM

Harshit Rai
2017152

PART I

Question 1

Alan Westin defined the four states of privacy as solitude, intimacy, anonymity and reserve.

The “Reserve” property basically means the creation of a psychological barrier against unwanted intrusion. It controls how and what all information the user allows to be publicly available. The reserve property is maintained on Twitter in following manner:

- The user can choose the audience (everybody, people they follow, no one) who can send them messages.
- They can limit their tweets visibility to either everybody, only to people they follow, or only to selected users.
- Twitter also restricts the use of certain “custom” words, which can not be commented on their tweets.
- Twitter gives the user the freedom to choose their account to be public or private.

According to me, the individuals who exhibit pragmatic idealism would be concerned about “Reserve” property because they are the ones who are most worried about the consequences of their actions. They are the ones with what information to share and what not to share kind of ideology.

Question 2

Leaking of sensitive information on social media is very common if proper privacy safety measures are not followed by the user. With opt-in and opt-out techniques, users can control or mitigate the damage of data breach. Facebook follows the opt-out technique while signing up on it. To change the privacy settings, users have to change the settings on their own after creating the account. Most of the users are not even aware of the various privacy settings, therefore they are more prone to attacks. Instead of agreeing

to the default privacy settings (opt-out), users must have the flexibility to change the settings according to their needs at the time of sign up. Therefore Facebook must include the following prompts (opt-in) while creating a new account:

- Allow/deny Facebook to access your **photo gallery.**
- Allow/deny Facebook to access your **contacts.**
- Allow/deny Facebook to access your **location.**
- Allow/deny Facebook to display your **pictures, contact information and other information** to the public (on Facebook).

Question 3

Keeping in mind the concept of “usable security”, the idea of eXpandable grids can be used to make a new modified version of it with 3 permissions (read, write, delete) and 2 levels (yes, no) and more inclined towards its usability among the users. The eXpandable grids might be difficult to understand for a person with colour blindness. Therefore a new modified method is designed. It basically deals with the counting or binary numbers.

	HW	**Quiz**	**Submissions**	**Marks**
Student	100	101	111	000
Teaching Assistant	110	100	100	110
Professor	111	111	100	111

Each cell has a binary number written in it. The binary number has three parts or all three digits represent a unique configuration. The numbers (1/0) are written in the same given order. **Read,Write,Delete** and **1- Access granted, 0- Access denied.**

For example, 110 means that the user has **Read access, Write access but no delete access.** In the same way 001 means that the user do not have **Read access, no Write access but has delete access.**

So in total we have 8 different access control configurations namely: **000, 001, 010, 011, 100, 101, 110, 111.**

Question 4

Federated Identity Management is an arrangement between two or more trusted web domains which allows them to share a user's digital identity among themselves. Which authorises the users to get access to their services.

The user's identities are stored on Cloud Identity or Google Workspace. Google uses **Security Assertion Markup Language (SAML)** at the time of sign-up, which links user's digital identity with identities managed by our external **Identity Provider (IdP).** At the time of log in, Google Workspace relays authentication on the SAML Identity provider to verify a user's credentiability. Yes, "sign in with google" on a third party website qualifies as a federated identity.

https://cloud.google.com/architecture/identity/overview-google-authentication

---

Question 5

Memory Forensics: It is a method of investigating a computer's memory dump in order to look for anything suspicious such as a virus or a malware. Malwares like Agent Tesla can not be detected using static analysis. They bypass the antivirus by tampering with the macros, we need to do a memory forensics or memory investigation in order to expose them.

Server Logs: These files are automatically generated and maintained by the system. It consists of all the activities performed by the system's server. They will tell us the traffic at our website. So if some program on your system accesses the internet and what all web domains it contacts etc, everything gets recorded in the server log file. It can be very useful in case of network analysis of a particular file.

https://www.portent.com/blog/design-dev/log-file.htm

Question 6

Parties in the security business which are liable to my company would be:

- **Product suppliers:** They would be liable to us if some product received is damaged, expired or not in good condition.
- **Security Guards:** Security guards at various "amazeon" base stations would be liable to us if in case of any theft.

- **Internet server provider:** The server providing firm would be liable to us in case of any virus gets spread online or something like this, because they have provided us with the online server to host our website and store the database of sensitive information.

Some of our primary responsibilities with the data are:

- The sensitive information of millions of users must be kept secure and confidential with maximum protection to avoid any kind of data breach.
- Users must be informed thoroughly about how the company is going to use their data, in order to maintain transparency.
- The company must follow the Reasonable security practices and procedures and sensitive personal data or information Rules, 2011.

Our company would be liable for the costumes in enormous ways. For example, if the product received is not correct or damaged, their sensitive data gets leaked, the delivery person does not treat them well or their mobile app or website contains some kind of malicious software.

Question 7

A. **Facebook Username:** Rank- 8. Although Facebook usernames are unique, there is a very high probability that multiple users have the same name as there are a total of 2.45 billion users signed up on Facebook. We can get a few multiple users with the same name but can not be 100% certain about any of them.

B. **Gmail ID:** Rank- 6. All Gmail IDs are unique. There are a total of 1.5 billion users on Gmail, and there is no specific search engine to search for a particular user unless we know their password beforehand. However, adversaries can take advantage of the forget password option to exploit the details.

C. **College ID card number:** Rank- 3. If we have only a college ID card number, then it becomes a very tedious job to identify a person uniquely because there are over a million colleges in the world. But if we are able to track down the college, then searching for a particular student is not a big deal. Also, college ID card numbers are not unique.

D. **Information about the bus number you take:** Rank- 3. A large number of people travel through buses every day, so it is very highly unlikely that we are able to track down a person using only the bus number they have traveled on. Also, bus numbers are not unique.

E. **Your percentile in the last semester:** Rank- 1. There are over 600 million students in college all over the world. Each student has their own last semester grade, which is not unique. So it is almost impossible to locate a particular student.

Question 8

A) Indeed privacy is not easy to visualize because it is a multifaceted concept. Every individual has their own different interpretation of privacy. It is very complex to explain in plain terms. A user can feel safe about their system's privacy but might not be secure. As we have studied in the FCS lectures that various malwares work very cleverly in the **background of your system**. They very intelligently deploy malicious softwares on your computer without even your knowledge. Malwares like **Agent Tesla** is even capable of deceiving anti-viruses. We studied various memory forensics techniques which can be used during such attacks. Also, one might feel that their passwords are secure as long as they are long enough or include some gibberish terms in it. I learned that **Security through obscurity** is not always a good choice for a password.

How a user feels safe while surfing through the internet, but softwares like **wireshark** captures internet traffic across the internet connection which can be used by adversaries to exploit users. We also learned that sharing our **publicly available information** quite often can give rise to a cyberattack. After studying so many concepts in FCS, I have realised that indeed "privacy is not easy to visualize", it has many aspects.

B)

<u>Reasons why privacy icon initiative will work:</u>

- **Taglines** alone can be very confusing and **icons** alone can draw people's attention but might not be very effective in conveying the actual message. The best combination is to write the tagline along with the icons in order to make a great impact on the users. As this was shown clearly in the study done by **"CyLab Usable Privacy and Security Laboratory."**
- Icons and symbols are very easy to understand by everyone with very little technical knowledge. Symbols are a great way of communication.
- The **colour and design of icons** play a very vital role in depicting the actual message. "Some small changes can make a big difference."

Reasons why privacy icon initiative will not work:

- Different individuals have **different meanings** of icons, colours, textures or appearance. So it can be **very confusing** at times when users are actually dealing with such icons.
- Icons can also mislead users, we saw in that video (shared in the question) that users felt perplexed with the toggle icon, as if they were supposed to click on them as an actual toggle button (as there is on IPhone).
- Designing such icons with great precision and accuracy about the message they want to convey, can be a very tedious task. As we saw in the video, the icons first need to be approved by the **California Office of the Attorney General (OAG)** to get approved.

PART II

A) encrypt(concat(m, hash(m)), public_alice)

No, Bob will not be able to decrypt the message, because the message is encrypted with Alice's public key and will only be deciphered with Alice's private key. Which is not available to Bob.

B) encrypt(concat(m, hash(m)), public_bob)

Yes, Bob will be able to decrypt the message, because the message is encrypted with his own public key and he can decrypt it using his private key.

Confidentiality: Confidentiality is maintained during the process because the message was encrypted with Bob's public key, which can only be decrypted using Bob's private key. As Bob's private key is available to only Bob, so no one else can read or alter the message. Hence, confidentiality is being maintained.

Non-reputability: Non-repudiability is not maintained. Because Alice did not attach her signature or message hash along with the message sent. So there is no way in which Alice can prove that the message was sent by her and no one else.

Steps to decrypt the message:
We have, C = encrypt(concat(m, hash(m)), public_bob)
we can do, M = decrypt(C, private_bob) to get the concatenation of message and hash of message.
As it is clearly mentioned in the question that we can unambiguously separate the two concatenated strings.
Now we are left with our message (m) and the hash of the message hash(m).

Also, to verify that the message sent by Alice hasn't altered, we can match the hash(m) with the hash(message_decyphered). If these two hashes match then the message is not altered and if not same then it has been altered.

C) encrypt(m, public_bob) ; sign(hash(m), private_alice)

Yes, Bob will be able to decrypt the message, because the message is encrypted with his own public key and he can decrypt it using his private key.

Confidentiality: Confidentiality is maintained during the process because the message was encrypted with Bob's public key, which can only be decrypted using Bob's private key. As Bob's private key is available to only Bob, so no one else can read or alter the message. Hence, confidentiality is being maintained.

Non-reputability: Non-repudiability is maintained. As Alice has attached her signature along with her private key.
Let, S = sign(hash(m), private_alice)
Bob can perform decrypt(S, public_alice) to get the hash of signatured message received.
Now, if this hash matches with the hash(message_decrypted, alice_private), then yes non-repudiability is maintained otherwise not.

Steps to decrypt the message:
We have, C = encrypt(m, public_bob)
we can do, M = decrypt(C, private_bob) to get the message.
Now we are left with our message (m).

Verification can be done in the same way as mentioned in part B.

D) encrypt(m, public_bob) ; sign(hash(m), private_bob)

Yes, Bob will be able to decrypt the message, because the message is encrypted with his own public key and he can decrypt it using his private key.

Confidentiality: Confidentiality is maintained during the process because the message was encrypted with Bob's public key, which can only be decrypted using Bob's private key. As Bob's private key is available to only Bob, so no one else can read or alter the message. Hence, confidentiality is being maintained.

Non-reputability: Non-repudiability is not maintained. As Alice has attached only her signature and Bob's private key.
Let, S = sign(hash(m), private_bob)

Now, to make sure that the message was indeed sent by Alice, we need to have Alice's private key to check it. But here we have used bob's private key for signature instead.
Therefore there is no certain way which would prove that yes the message was sent by Alice only.

Steps to decrypt the message:
We have, C = encrypt(m, public_bob)
we can do, M = decrypt(C, private_bob) to get the message.
Now we are left with our message (m).

Verification can be done in the same way as mentioned in part B.

E) encrypt(sym, public_alice) ; encrypt(sym, public_bob) ; encrypt(m,sym)

Yes, Bob will be able to decrypt the message, the steps to decrypt the message are given down below.

Confidentiality: Confidentiality is maintained during the process because to decrypt the message, the adversary must have "sym". "sym" can only be decrypted with the help of either private_alice or private_bob. Attackers do not have the access to any of them therefore confidentiality is being maintained.

Non-reputability: Non-repudiability is not maintained. Because Alice did not attach her signature or message hash along with the message sent. So there is no way in which Alice can prove that the message was sent by her and no one else.

Steps to decrypt the message:
Let, C1 = encrypt(sym, public_bob).
We can do, decrypt(sym, private_bob) to get sym.
Now, we have to perform decrypt(m, sym) to get the message (m).

F) encrypt(sym_1, public_alice) ; encrypt(sym_1, public_bob) ; encrypt(sym_2, public_alice) ; encrypt(sym_2, public_bob) ; encrypt(encrypt(m, sym_2), sym_1) ; sign(sym_1, private_alice) ; sign(sym_2, private_alice)

Yes, Bob will be able to decrypt the message, the steps to decrypt the message are given down below.

Confidentiality: Confidentiality is not maintained. Because the adversary can find sym_1 and sym_2 in the following manner.

S1 = sign(sym_1, private_alice).
By performing, decrypt(sym_1 ,public_alice) because they already know public_alice.

Using the above method, sym_1 and sym_2 can be easily known by hackers.
Finally they can perform, decrypt(encrypt(m, sym_2), sym_1) and decrypt(m, sym_2) to get the message (m).
As the message is now known to everyone, they can alter, delete or tamper it. Therefore confidentiality is not maintained in this case.

Non-reputability: Non-repudiability is maintained. As Alice has attached her signature along with her private key.

S1 = sign(sym_1, private_alice)
We can perform, decrypt(sym_1, public_alice) to get the signatured sym_1.
S2 = sign(sym_2, private_bob)
We can perform, decrypt(sym_2, public_bob) to get the signatured sym_2.

Finally perform, decrypt(encrypt(m, sym_2), sym_1) and decrypt(m, sym_2) to get the signatured message (m). This would verify that the message was indeed sent by Alice herself and no one else.

Steps to decrypt the message:
Let, C1 = encrypt(sym_1, public_bob)
We can do, decrypt(C, private_bob) to get sym_1.
In the same manner let, C2 = encrypt(sym_2, public_bob)
We can do, decrypt(C, private_bob) to get sym_2.

Also, C3 = encrypt(encrypt(m, sym_2), sym_1).
We can perform decrypt(encrypt(m, sym_2), sym_1)) as we now know sym_1 to get C4 = encrypt(m, sym_2)

Finally, perform decrypt(m, sym_2) because we know sym_2 as well, to get the message (m).

PART III

Question 1

Anomaly based malware detection can handle novel attacks. Because signature based malware detections are limited to only those attacks whose signature is being available or created before. Therefore they can not detect a novel malware, which is not the case in anomaly based malware detection.

Question 2

Tor is a network made up of multiple nodes and relays, which help the user in masking their identity at various stages. Every node in a relay network is encrypted to maintain the anonymity of the user. But the anonymity can be broken if an adversary is successful in monitoring the both traffic that enters and exits the network. In other words, if the DNS traffic is not routed, then the adversary might be able to track down all the traffic generated by our DNS queries. But by routing traffic, only the previous node's information is available with the adversary.

https://www.zdnet.com/article/how-dns-can-be-used-to-unmask-tor-users/

Question 3

The company should notify the user in case of a data breach incident irrespective of the fact that the data is protected/encrypted or not. There are enormous ways in which adversaries could decrypt the stolen data (not always). If data is stolen, the authority must inform about the same. Whether the data is protected or not is a secondary issue. Because adversaries might not be able to decrypt the data in a short time span, but might be able to decrypt the data in a longer run and the user whose data is being sacrificed will face the consequences. This does not sound ethically appropriate.

Question 4

There is one constant decryption key with the adversary, they deploy the encrypted viruses with different encryption keys to block some file or location on your system. As different keys are used for encryption, signature based detection fails to detect such

viruses. Moreover, to make the situation worse, viruses like cascade virus use multiple decryption keys instead of just 1.
Ransomwares like Cryptolocker is a kind of malicious softwares which locks/blocks access to certain files or locations on the system by encrypting it with strong hash functions. And demands for a huge sum of money to get your system running again (decryption).

Question 5

In case of a mobile phone theft which is password protected, adversaries can still exploit your sensitive information. They could steal and sell the internal hardware like memory card, processor or some other vital component in your device. They could also very cleverly hack into your device's memory (in rare cases) and get access to all your sensitive information on the mobile phone.

Question 6

Yes, a malware can cause hardware damage. Malwares can increase the system's fan speed, increase clock cycle which would harm the RAM of the system by overheating it. Malwares can command the system to corrupt the driver or run a command which extensively uses the GPU and overheats the system.

Question 7

Fail-safe default states that unless specified, all the setting/options should be denied or not given access to. Their default setting is not giving access to any of the options or choices unless a user changes it on its own.

Among opt-in and opt-out, the **opt-in** mechanism qualifies as fail-safe default.
