DSCI-519, Assignment 1
Rishit Saiya

Q1-A: [Assumption: The entire staff force can access the given database using their credentials with no explicit access control policy for the database. Data is not encrypted.]

1. What are the threats?

To give a context, data has been equivalent gold for most of the conglomerates around the world. This makes the data very critical and with increasing regulations and policies. It is very important for the organizations to manage customer data, its protection and its integrity. In the motive of above question, some of the security concerns which might turn out be potential threats are as follows:

• Social Engineering: Sometimes due to improper knowledge about the veracity of the communicator, often employees of the company are susceptible to social engineering attacks. They basically fall into the trap of some adversaries which might result in the above-mentioned database maintenance being a major risk in terms of its confidentiality, integrity and availability. The customer database is hence vulnerable in that way.

• Privilege Escalation: Privilege escalation is a type of attack which gains unauthorized access to systems within a secure boundary. Privilege can be escalated and critical data like can be accessed.

• Weak Authentication/Password Leakage: The infrastructure basically needs only one leak in order to get totally exposed and exploited. This can pop up from the usage of weak or guessable passwords which often happens in the case of organizations. Due to the absence of a weak access control policy, unauthorized company employees (HR team, Account team) would be able to access and modify the customer information database.

• System Vulnerabilities: Services which are integrated in the system infrastructure of the companies such as log4j, Microsoft Utilities, etc. tend to have vulnerabilities which have been exploited in the past and impacted the financial, intellectual assets of the companies.

• Denial of Service attack: Bombarding a system with a particular targeted attack like huge amounts of network traffic in terms of large packet numbers can disintegrate the availability of the system and make it temporarily dysfunctional. This might cause disruption to the flow of the information within the company.

• Compliance Violation: Compliances like NIST, PCI-DSS, HIPAA, ISO, IEEE are in place which essentially talk about the minimum bar of security required for the system infrastructure of the company mentioned above.

2. Why are the threats important?

The following is a small exhaustive list of why the above-mentioned threats are important?

• Social Engineering: The importance of social engineering is that it develops a security sense in the current cyber space and the only downside is that it can’t be eliminated as there are unforeseen developments in technology and also there is always a human error factor which comes into play.

• Privilege Escalation: This technique typically shows how to protect user critical information in systems and maintain the cybersecurity landscape.

• Weak Authentication/Password Leakage: A very guessable and common password enables intruders to exploit and easily penetrate into the systems. On the other hand, it is relatively difficult to crack passwords with complexities. This makes it difficult to crack and hence this threat is important to keep systems secure.

• System Vulnerabilities: This vulnerability helps to keep our infrastructure safe including networks, servers, cloud, etc. This is important as it helps analyze any incompatibilities between softwares and such.

• Denial of Service Attack: Often hackers use this easy technique to disrupt the availability of a service and threat becomes important as it even solves the problem of huge traffic interception on the network and helps to maintain applications online after such attacks.

• Compliance Violation: It is vital to ensure that cybersecurity compliance is a mandatory requirement coming from regulatory agencies and it might be consequential for the business overall.

There are many other threats as well which are very prominent in current state-of-the-art techniques. But the very reason why threats are important can be cited back to the Cyber Risk Infrastructure Management wherein we assess the likelihood and impact of the systems integrated in the company. The threats mentioned above are recognized in the Risk Assessment of audits of large organizations and this helps the authorities to gauge and recognize the weaknesses of their systems in advance. This also enables the companies/organizations to reallocate their resources and try to safeguard themselves against potential attacks.

3. A brief description of the threat mitigation techniques.

Some of the threat mitigation techniques for the above-mentioned threats are as follows:

- Social Engineering: Train your staff, Implement Technical Measures
- Privilege Escalation: Least Privilege Principle, Analyze and assess risk to each privileged user
- Weak Authentication/Password Leakage: Harder Passwords, Resistant to Brute-Force Attacks
- System Vulnerabilities: Regular audits, Black box penetration testing
- Denial of Service attack: Firewalls, IDS, Packet Detection
- Compliance Violation: Regular Compliance Audit, Knowledge on latest compliance releases

4. How would you apply the proposed techniques?

The answer to this would be to elaborate on the above-mentioned mitigation techniques.

- For the social engineering attacks, we basically need to train staff about the current techniques and how to deal with them. Along with that, we must also implement few of the technical measures such as not allowing the proprietary IP (Intellectual Property) to attach on personal emails, etc.
- The Least Privilege Escalation Principle can be implemented to make sure that the privilege is assigned to least mode or only need-to-know basis. As to be reported to CISO, a recommendation would be to analyze and assess risk associated with each privileged user in the organization.
- For weak Authentication we need a combination of harder passwords such as combination of alphanumeric with special characters. Regularly change passwords at regular intervals
- A lot of system-based Vulnerabilities can be eliminated through regularly timed audits. A technique of Black box penetration testing can be applied to assess all the weaknesses in the system.
- An additional array of additional security services like Firewall services such as Cloudflare can be used to filter a lot of packets and allow legitimate packets in case of Denial-of-Service attack.
- A regulatory audit in the realm of Compliance is needed to keep up-to-date with the upcoming policies and compliance requirements to meet the maintenance of the company.

5. How would the techniques protect against the threats?

In a social engineering attack, a trained staff would be likely to avoid falling for such attacks. This would help the organization to avoid attacks in the future from this end.

Inculcating the Least Privilege Escalation Principle helps organizations to reduce their surface area of attack and enables the authorities to have a verifiable scope within their reach.

A very common technique of harder password with properties recommended such as special characters, case characters makes it very hard for the adversary to guess or brute force such passwords. This keeps the company's critical assets safe.

A system vulnerability is best to be patched as early as possible in order to avoid most of the attacks. Since a lot of software based attacks in the form of Buffer Overflow (statistically given) are prevalent, engineers working on safeguarding system vulnerabilities help it to protect against the threats.

DDos attacks are relatively lower in place in current machines as bots which are installed filtering the non-legitimate traffic and allowing only the required packet and this is helping the system to not let enter any malicious traffic into the network.

Upcoming releases of compliances and policies are becoming stricter in terms of regulating the security standards of the organization and this is making the companies more resilient to attacks.

Q2-A: [Assumption: All working employees/customers have files on cloud. The files are shared at the discretion of users. The admin can view/edit/execute all the files of the employees/customers within the company. Some of the conventions used below are as follows: Read referred as ‘r’, Write referred as ‘w’, Execute referred as ‘x’, Own referred as ‘o’. The advertisements are based on the public files only.]

1. What are some security policies that this system should enforce? Consider the access needs of the users (Alice and Bob) as well as the Administrator

- Owner of a file has “rwxo” permissions. Owners can alter their own file’s availability on cloud. Users log in to their cloud accounts using their password based authentication.

- Owners of files can share/revoke access and give permissions of “rwxo” to any co-workers at their own discretion [DAC Policy]. The admin can view/edit/execute all the files of the employees/customers within the company. The admin can maintain users’ database by adding/editing/removing users’ information.

- Unauthorized users can’t access files. Public files can be viewed by everyone.

2. Draw an access matrix that implements the policies. Use any of the access modes (read, write, execute, own) from the readings.

Premise for drawing the access matrix is as follows:

- Files owned by Alice: FA1, FA2 and FA3 (A: rwxo). FA1 is a file shared with Bob (B: rwx). FA2 is a private file. FA3 is an open public record file (Public: r).
- Files owned by Bob: FB1, FB2 and FB3 (B: rwxo). FB1 is an open public record file. FB2 is shared only with Alice (A: rx). FB3 is a private file.
- Files owned by Administrator: FAd1, FAd2 (Admin: rwxo). FAd1 is a private file, FAd2 is a public record file.

Subject/ Objects	**Alice’s Files**			**Bob’s Files**			**Admin**	
	FA1	**FA2**	**FA3**	**FB1**	**FB2**	**FB3**	**FAd1**	**FAd2**
Alice	rwxo	rwxo	rwxo	r	rx	-	-	r
Bob	rwx	-	r	rwxo	rwxo	rwxo	-	r
Administrator	rwxo	rwxo	rwxo	rwxo	rwxo	rwxo	rwxo	rwxo
Public	-	-	r	r	-	-	-	r

3. Sketch the system and “interpret” the reference monitor (including the subjects, objects, access database, audit records). You can list the elements or draw a diagram. Just be sure to demonstrate the mapping between the entities and the RM components.

4 components of Reference Monitor:

1. **Subjects:** Alice, Bob, Administrator, Public, Employees, Customers, etc.
2. **Objects:** User/Customer Files (like FA1, FA2, …, FB1, FB2, …) , Administrator Files (like FAd1, FAd2, …)
3. **Authorization Database:** User/Customer Database containing all credential information, personal information, files information (date created, size, permissions, Access Control Lists)
4. **Audit Log:** Server Logs of the cloud are saved that relate to accessing files with respect to users and permissions.

4. What are some of the possible security mechanisms the system could use to implement the reference monitor?

A potential security mechanism the system could use to implement the reference monitor is in fact the RVM (Reference Validation Mechanism) wherein we check the security capabilities of the system. It can be atomically checked through the principles of Reference Monitor.

Checking Isolation Property: A security mechanism which will be responsible for user authentication and authorization of user access for given files. Authentication can be implemented using 2FA, MFA. Implementing cloud security service and utilities to authorize user granted access. (DAC) will be stored as an access control list; for instance, in the access control list, FA3 object will be displayed as follows:

Subject/Objects	**Alice’s Files**
	FA3
Alice	rwxo
Bob	r
Administrator	rwxo
Public	r

Checking Completeness Property: A security mechanism wherein the above method cannot be circumvented. Each file access request is verified through this security mechanism to verify if the user accessing it has the access to the file or not.

Checking Verifiability Property: A security mechanism which might not include the whole proprietary software of the cloud but includes some TCB (Trusted Computing Base) which allows it to be checked for vulnerabilities. So, it can be deduced that the TCB code can be used to verify the vulnerabilities in code using techniques like Formal Analysis, Static Analysis, etc. and is not that complex to analyze as well.

Q3-A:

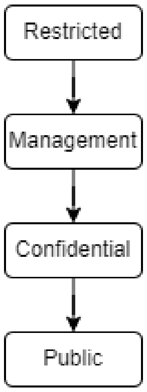
Define MAC labels (access classes) that contain levels and categories. Define classifications and clearances for the objects and subjects i.e., assign the labels to specific types of users and types of information to express the policy you want to enforce

The nomenclature used here is defined as follows:

BRD: Board Restricted Data, MRD: Managerial Restricted Data, HRD: HR Data, ARD: Account Receivable Data, SCD: Sensitive Client Data, IRD: Insider Restricted Data, Corp: Corporate, Conf: Confidential, U: Public Datas	A: Anyone, E: Employees, M: Managers, NDA: Non-Employee NDA signed People, E’: Certain Employees who can access IDR, M’: Certain Managers who can access IDR, HM: High Level Manager, B: Board Members, CM: C-Level Managers, D: Director, E”: Need to know basis Employees, M”: Need to know basis Managers.

Assumptions:

- (HM = B ∪ CM ∪ D), (E” ⊆ E’ ⊆ E), (M”⊆ M’⊆ M), (HM ⊂ M), (M, M’ ⊆ E), (CM, B ⊆ HM)
- All the employees have signed NDA
- E’ and M’ can access IRD. E” and M” can access HRD.
- Hierarchy of Employees: B > CM > D > M > E > U



The following is the actual interpretation of the information classification policy as mentioned in the problem.

- (U, {A})
- (Conf, {NDA, E})
- (Corp, {E})
- (IRD, {E’, M’, NDA})
- (MRD, {HM})
- (BRD, {CM, B})
- (HRD, {E”, B”})
- (ARD, {E”, M”})
- (SCD, {E”, M”})

Classifications and clearances for the objects and subjects

With the above considerations of assumptions, we can interpret, define classifications and clearances for given policies. The users/subject categories are clubbed together in the following manner and their access hierarchical structure is as:

Restricted (R*): {CM, HM, B, D} || Management (M*): {E’, M’} || Confidential (C*): {E, E’, M, M’} || Public (P*): {A} ***(Reference to Above Image)***

The object categories are clubbed together in the following manner and their access hierarchical structure is as:

Restricted (R*): {BRD, MRD} || Management (M*): {HRD, ARD, SCD} || Confidential (C*): {IRD, Conf, Corp} || Public (P*): {U} ***(Reference to Above Image)***

Show the dom relationship for your MAC labels

In order to establish lattice domination, the assumption mentioned above is implemented. The lattice formed is as follows: **MAC labels (access classes)**

1 - (R*, {BRD, MRD, HRD, ARD, SCD, IRD, Corp, Conf, U})
2 - (R*, {MRD, HRD, ARD, SCD, IRD, Corp, Conf, U})
3 - (M*, {HRD, IRD, Corp, Conf, U})
4 - (M*, {ARD, SCD, IRD, Corp, Conf, U})
5 - (M*, {SCD, IRD, Corp, Conf, U})
6 - (C*, {Corp, U})
7 - (C*, {IRD, U})
8 - (C*, {Conf, U})
9 - (P*, {U})