THE UNIVERSITY OF
MELBOURNE

SWEN90010 – High Integrity System Engineering

Assignment 1

Student Name:	Lihua Wang	Yuhan Jiang
Student ID:	1164051	967659
Student Email:	lihuwang@student.unimelb.edu.au	yuhjiang@student.unimelb.edu.au
Semester:	20201/S1	
Coordinator	Toby Murray	

School of Computing and Information Systems

Contents

Task1: Components: 2

Architecture of the system 2

Components Introduction: 2

Task 2-4: Threat Modeling Report 4

Spoofing: 4

Tampering: 7

Repudiation: 10

Information Disclosure 12

Denial of Service 17

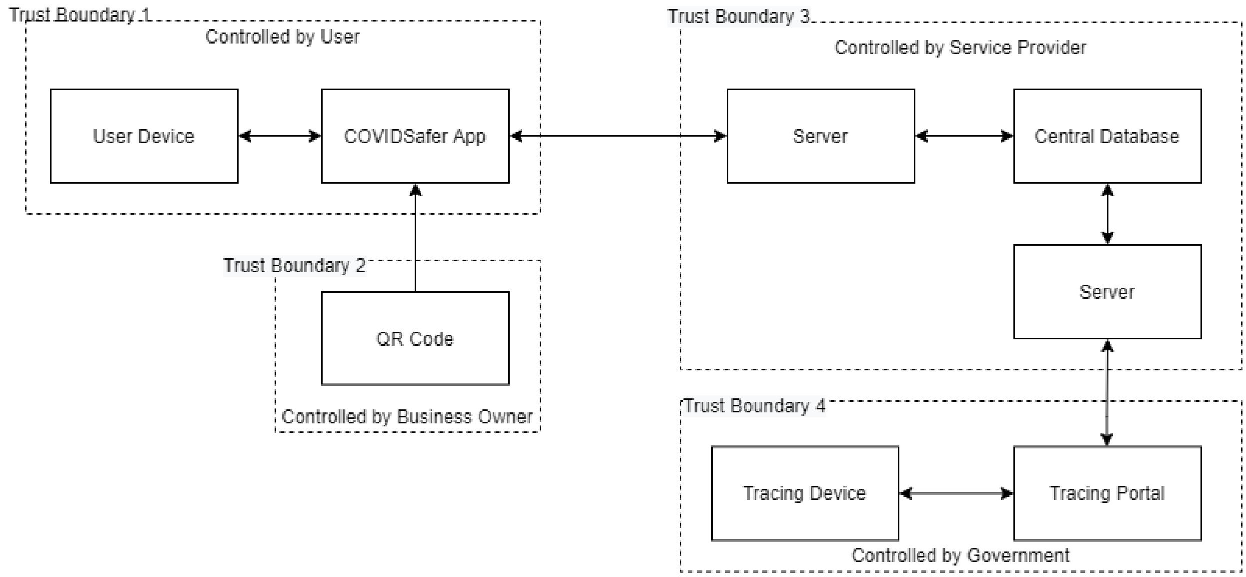
Elevation of Privilege 21

Summary: 24

Reference 24

Task1: Components:

Architecture of the system



In this system, we decided the four trust boundaries of the components.

Trust Boundaries	Components	Controlled party
Trust Boundary 1	User Devices, COVIDSafer App	Users
Trust Boundary 2	QR Code	Business owners
Trust Boundary 3	COVIDSafer App server, Central Database, Portal Server	The third party
Trust Boundary 4	Tracing Portal, Tracing Devices	Government

Figure 1. Trust Boundaries introduction

Components Introduction:

Controlled by users:

User Device:

Role: local mobile phone of users to run the COVIDSafer app

Data interaction: The information of users, like location or encoded tokens which are stored in the user's device, will be required when running the COVIDSaffer app.

COVIDSafer App:

Role: Obtain, encode and upload the users' check-in records after scanning the QR code.

Data interaction: When scanning the QR code and requiring the location check-in, the encoded location information of business owners will be obtained, and then such check-in records will be sent to the central database via COVIDSafer app server which is controlled by the third-party.

Controlled by government:

Tracing Device:

Role: Local devices of tracing staff to access the tracing portal.

Data interaction: Tracing staff can only require access to the portal website via tracing devices. Like query login authentication.

Tracing Portal:

Role: A web-site used by contact tracing staff to access the central database.

Data interaction: The portal allows contact tracing staff to run certain queries on the central database via a portal server controlled by the third-party.

Controlled by Business Owners:

QR Code:

Role: The business owner displays the QR code to the user, which includes the encoded location information.

Data interaction: When users use a mobile device to scan the QR code, the COVIDSafer app will receive the data after QR code analysis locally and loaded automatically.

Controlled by Service Providers:

COVIDSafer App Server:

Role: COVIDSafer App server manages server-side components, and it provides a fully functional and reliable operating environment for server-side components. It is also responsible for collecting the information from COVIDSafer App and sending it to the Central Database.

Data interaction: COVIDSafer App server receives the information from COVIDSafer App and uploads users' tracing information to the Central Database.

Central Database:

Role: Central Database is responsible for receiving the information from App Server.

Data interaction: The Central database receives these information， informs the app server that the information is successfully transmitted and stores these information as tracing records.

Portal Server

Role: Portal server provides the access control for the central database.

Data interaction: Portal Server is responsible for verifying whether the log-in token of tracing staff is legal. When the correct and legal tracing staff token is verified, the tracing staff enters the database to query information based on appropriate permissions.

Task 2-4: Threat Modeling Report

The core of threat modeling is to think like an attacker and to identify threats from the perspective of the attacker. The first step is to establish the data flow diagram is composed of four types of elements: External Entities, Processing Process, Data Storage, and Data Flow.

Based on the data flow diagram and stride methodology, we can find that not every element will face six threats. For example, external entities only have two types of threats: spoofing and repudiation. We don't need to care about whether external entities will be tampered with or information leakage will occur. And denial of service, etc., because external entities are originally outside of our control.

Among them, the process (processing process) will face all six types of threats. The Repudiation in the data storage is red, which means that only the stored data is an audit log and will be at risk of repudiation. There is no repudiation when storing other data.

Spoofing:

Threat 1:

Threat description:

An attacker who may be a malicious business owner, might impersonate users to access any confidential portals by forging a fake check-in QR code. When users scan the code, it will lead them to access malicious websites or automatically download malicious plugins in their mobile devices. That could allow attackers to learn information including user's credentials, for example, bank account, or encrypted tokens which are the keys to decrypting user's sensitive information.

Possible Attacker:

Business owner/ Cyber-criminals

Security goals:

Authentication: Authentication of users.
Confidentiality: Avoid disclosing information to an authorized user. File and I/O access control.

Possible Mitigation(s):

- The QR code will only be opened through the COVIDSafer app.
- Ensure that unknown code cannot execute on devices
- The sensitive information should be encrypted before writing to the mobile's local file system.

Consequences:

Negligible: The attack might allow the attacker to learn the confidential information of users' which might cause the user's information disclosure and harm to their property or reputation, etc. However, since this attack doesn't harm the system, and the cost to repair it is not expensive, we set the consequences class as negligible.

Threat 2:

Threat description:

An attacker might pretend to be a user to create and transport fake check-in records by running an app that impersonates the COVIDSafer app to interact with the server which will cause integrity problems in the central database.

Possible Attacker:

Cyber-criminals

Security goals:

Authentication, integrity: Only authorized users are able to modify a system or the data on it. Prevent attackers spoof or impersonate a process or machine.

Possible Mitigation(s):

- Ensure that using a standard authentication mechanism to authenticate users' identities
- Ensure that password and account policy are implemented
- Enable authentication when connecting to MSMQ queues in WCF
- Ensure appropriate controls are in place when accepting files from users

Consequences:

Marginal: The attack might cause integrity problems in the central database which makes the tracing data unreliable and harm the accuracy of the system. Besides, it is hard to track a fake app and the repair cost is expensive, so we set the consequences class as marginal.

Threat 3:

Threat description:

An attacker might forge a malicious website to impersonate a tracing portal to access the central database. The fake portal looks the same as a valid one and induces staff to input their account credentials. That could allow attackers to obtain the database credentials by cheating and pretend to be a tracing staff to log in the database.

Possible Attacker:

Cyber-criminals

Security goals:

Authentication: Authentication of users. Ensure the access control schema optimal. Prevent attackers spoof or impersonate a user.

Possible Mitigation(s):

- Ensure that contact tracing portal can only be accessed via contact tracing devices.
- Access third-party JavaScript from trusted sources only, implement Content Security Policy (CSP), and disable inline JavaScript
- Ensure that unknown code cannot execute on tracing devices
- Ensure that only the minimum services/features are enabled on tracing devices
- Ensure that tracing devices have end-point security controls configured as per organizational policies

Consequences:

Critical: The attack might cause system breakdown or damage the integrity of the data in the central database which will cause the information disclosure and system unavailable. The loss of property of the third-party and government will be large and it might spend too much money and time to fix the threat. Therefore, we set the consequences class as critical.

Threat 4:

Threat description:

An attacker might obtain the staff accounts credentials by cheating and then pretend to be a staff member to access the central database. For example, due to improper logout from the server, attackers can get access to the tracing portal's session.

Security goals:

Authentication: Authentication of users. I/O access control. Prevent attackers spoof or impersonate a process.

Possible Attacker:

Cyber-criminals/government staff who doesn't have privilege to administrate tracing portal

Possible Mitigation(s):

- Ensure that contact tracing portal can only be accessed via contact tracing devices.
- Ensure that devices have end-point security controls configured as per organizational policies
- Ensure that the default login credentials of the field gateway are changed during installation.
- Encrypt OS and additional partitions of Device with bit-locker
- Ensure that only the minimum services/features are enabled on devices

Consequences:

Marginal: The attack might damage the integrity of the data in the central database which will cause the information disclosure. However, it's not difficult to mitigate the threat and we set the consequences class as marginal.

Threat 5:

Threat description:

Assume the server was provided an identity authentication scheme, and all the central database administrators credentials were stored in the server. (Justification: Since the administrators need to access the central database by interacting with the server first to verify their identity.) However, the attacker might abuse poorly managed signing keys of the server. In case of key compromise, an adversary will be able to create valid auth tokens using the stolen keys and gain access to the resources.

Possible Attacker:

Cyber-criminals / The adversary of the third-party provider

Security goals:

Authentication: Authentication of users. Data encryption schema is optimal. Prevent attackers spoof or impersonate a user.

Confidentiality: keep data and communication secret, be sure the source and content of tokens.

Possible Mitigation(s):

- Ensure that signing keys are rolled over when using Identity Server.
- Ensure that do not use access tokens that provide direct access to the server
- Use per-device authentication credentials
- Ensure that TokenReplayCache is used to prevent the replay of authentication tokens
- Ensure that least-privileged accounts are used to connect to the server.

Consequences:

Marginal: The attack might cause the information disclosure once the attacker obtains the sensitive information. However, it’s not difficult to mitigate the threat by optimizing the encryption schema, so we set the consequences class as marginal.

Threat 6:

Threat description:

Since the third-party service provider is one of the managers of the central database. An attacker might spoof the service provider administrator and gain access to the central database if the administrator's credentials are compromised.

Possible Attacker:

Cyber-criminals / The adversary of the third-party provider / the staff of the third party who doesn’t have authority of accessing the central database

Security goals:

Authentication: Authentication of users. Access control schema optimal.

Possible Mitigation(s):

- Enable central database Multi-Factor Authentication for administrators
- Ensure that least-privileged accounts are used to connect to Database servers.
- Implement Row Level Security RLS to prevent tenants from accessing each other's data.
- Ensure that auditing and logging is enforced on the database

The above mitigations are not sufficient for preventing a super administrator from the third-party to access. Actually, it is hard to monitor a database owner’s operations if they want to hide.

Consequences:

Marginal: The attack might cause the central database not available and cause the information disclosure. It will harm the reputation of the third-party and government, as well as the large property. However, it may not be difficult to track the compromised credential and fix this issue, so we set the consequences class as marginal.

Tampering:

Threat 1:

Threat description:

An attacker who has credentials to access the central database, might damage the sensitive information deliberately or unintentionally, which will cause the integrity of a data compromise.

Possible Attacker:

Tracing staff / administrators of the third-party

Security goals:

Integrity: Only authorized users should be able to modify the data.

Possible Mitigation(s):

- Ensure that least-privileged accounts are used to connect to Database servers.
- Implement Row Level Security RLS to prevent tenants from accessing each other's data.
- Ensure that using strong encryption algorithms to encrypt data in the database.
- Ensure that database backups are encrypted.
- Ensure that auditing and logging is enforced on the database

However, this threat still cannot be reasonably mitigated. One case is that if an attacker were given the highest priority of the central database, he/she can easily bypass the administration of the database and then reformulate the rules of management which stands for their benefits.

Consequences:

Catastrophic: The attack will damage the integrity of data seriously and cause the information disclosure. The case will get worse when an attacker has the highest priority to operate the database illegally without being noticed. Since this attack is hard to defend and mitigate thoroughly, we set the consequences class as catastrophic.

Threat 2:

Threat description:

An attacker might tamper the data in transit via the internet. For example, an attacker might perform attacks on check-in records in transit from COVIDSafer app via server to central database by using various tools and reverse engineer binaries, which allows attackers damage the integrity of data.

Possible Attacker:

Cyber-criminals

Security goals:

Integrity: keep data and communication secret, be sure the source and content of data.

Possible Mitigation(s):

- Ensure that binaries are obfuscated. This is to stop reverse engineering of assemblies. Tools like *CryptoObfuscator* may be used for this purpose.
- Consider using Encrypted File System (EFS) to protect confidential check-in records.
- Secure communication to Event Hub using SSL/TLS
- Ensure that all traffic to Identity Server is over HTTPS connection

Consequences:

Marginal: The attack might cause the information disclosure once the attacker obtains the sensitive information. However, it’s not difficult to mitigate the threat by optimizing the encryption schema of the data transmission, so we set the consequences class as marginal.

Threat 3:

Threat description:

Since the tracing portal is a website to access central databases over the internet. Data tampering in websites (tracing portal) is a way that an attacker who might be a member of tracing staff, gets into tracing portal and changes, deletes or to access unauthorized important files. That will allow attackers to be able to read, change or alter other government staff's credentials, which might lead authorization to the central database to fail and eavesdrop on important information.

Possible Attacker:

Cyber-criminals / tracing staff

Security goals:

Integrity: Ensure that unauthorized people do not alter the data.
Authentication: authentication of users, access control.
confidentiality: Protection of the system protection data.

Possible Mitigation(s):

- Ensure that proper authorization is in place and principle of least privileges is followed. Implement dynamic data masking and encryption to limit sensitive data exposure non privileged users
- Ensure that staff's credentials are encrypted and stored in salted hash format in the portal.
- Ensure that sensitive content is not cached on the portal.
- Business logic and resource access authorization decisions should not be based on incoming request parameters.
- Ensure staff properly logout from the portal and server.

Consequences:

Critical: The attack might cause the confidential information like credentials disclosure, and once they were modified, it may cause the portal system breakdown. The cost of repairing it will be expensive, so we set the consequences class as critical.

Threat 4:

Threat description:

An attacker might tamper portal website indirectly by using a script exploit that is the attacker would get the script to execute by masking it as a staff input from the portal website page or as a web link, the execution might leave the server vulnerable to attack and allow attackers access and modify unauthorized information.

Possible Attacker:

Cyber-criminals / an adversary of the third-party

Security goals:

Integrity: Ensures the authenticity and accuracy of the data, restricting permissions for editing or the ability to modify information.
Confidentiality: Keep data secret, central database must be accessible only to authorized users.

Possible Mitigation(s):

- Proper validation of users' inputs and proper encoding of outputs.
- A firewall and windows security are required to lock down important files, directories and other resources.
- The web application (portal) needs to integrate with composition analysis tools (e.g., snyk, npm audit, BlackDuck ...etc) to identify 3rd party libraries/dependencies with known security vulnerabilities.
- The web application (portal) should run with minimum privileges.
- When getting information from untrusted sources, to make sure it does not contain any malicious executable code.
- Ensure that sensitive content is not cached on the server. (portal)
- Encrypt sections of Web Application’s configuration files that contain sensitive data.
- Implement Content Security Policy (CSP), and disable inline JavaScript

Consequences:

Marginal: The attack might cause the confidential information disclosure, and once the attacker obtains the sensitive data, like login credentials, it may cause the portal system breakdown. However, it’s not expensive to maintain a website, so we set the consequences class as marginal.

Repudiation:

Threat 1:

Threat description:

Assume the check-in records in the central database will be kept for 21 days since it is uploaded. (Justification: This is a reasonable strategy to manage data. Firstly, 21-day is almost the longest period to detect a positive infection. Besides, there will be a huge dataset and consume too much memory if we don’t delete useless records in time.) However, since the users’ check-in records are only kept for a limited period, once the time expires or database damage that results in records deleted, users may deny that they have been somewhere.

Possible Attacker:

users

Security goals:

Non-repudiation: users cannot deny what they have done.

Possible Mitigation(s):

- Ensure the check-in records can be kept for a longer period, e.g., 3 months.
- Ensure that log rotation and separation are in place, which will make sure keeping more records and make it updated.
- Ensure the database was backed up.

However, the threat still not be able to mitigate thoroughly due to the cost of preserving all the data in the database are too expensive, and sometimes due to the limit of the storage, the third party provider cannot extend the database as large as the records required.

Consequences:

Negligible: Though the users' denied claim will cause the integrity of data, it does not cause a large damage to the system, and it's also easy to mitigate such situations, like storing the records for a longer period.

Threat 2:

Threat description:

An attacker who has the priority to operate the database might deny performing a destructive action on a central database (e.g., deleting all records) by erasing or truncating log files for hiding their tracks.

Possible Attacker:

Administrator of central database from the third-party / tracing staff

Security goals:

Non-repudiation: The log records of operations in the system are accurate and reliable.

Possible Mitigation(s):

- Ensure that login auditing is enabled when accessing the database
- Collecting and storing audit data regularly and uploading the logs to a storage for long term retention. Enable the following monitoring categories: Device identity operations, data modifying operations.

However, the above mitigation does not work for preventing repudiation from the third-party server provider. Since the databases were built by them, they have the highest priority to manage and administrate the database. It's quite difficult to monitor their operations in the database.

Consequences:

Catastrophic: The attack will damage the integrity and reliability of data seriously if the log records do not work for a super administrator. Since this attack is hard to defend and mitigate thoroughly, we set the consequences class as catastrophic.

Threat 3:

Threat description:

Since the central database will keep an access log which saves to a storage space. An attacker might cause that log storage space to become full, which allows attackers to behave suspiciously/erratically without any record.

Possible Attacker:

Administrator of central database from the third-party / tracing staff / an adversary of the third-party / cyber-criminals

Security goals:

Non-repudiation: The log records of operations in the system are accurate and reliable.
Availability: Data should be accessible when needed. Protection against denial of services attacks.

Possible Mitigation(s):

- Implement sufficient Audit Failure Handling. Ensure that the configuration can generate an exception when it fails to write to an audit log.

- Ensure that the logs are kept in the cloud storage so that it can extend storage space automatically.

Consequences:

Critical: The attack will cause the database's log function unavailable which is harm to the integrity and reliability of data. Even more, cause a serious data disclosure. However, there are several methods to solve such problems like extending the cloud storage or triggering the DDOS alarm, and the cost of them may not be expensive, therefore, we set the consequences class as critical.

Information Disclosure

Threat 1:

Threat description:

Attackers can get sensitive data of user devices if COVIDSafer App saves sensitive data on phone SD card or local storage which may get stolen. This allows them to learn the users' sensitive data so that they may sell the information for grey income or use this to blackmail users.

Possible Attacker:

Cyber Criminal/ User

Security Goals:

Confidentiality: Keep sensitive information not available or disclosed to unauthorized individuals, entities or processes

Possible Mitigation:

- Strengthen mobile phone anti-theft function ；
- Avoid COVIDSafer app storing the sensitive info in the phone SD card or local storage (i.e. password)

This refers to the security requirements of the physical protection requirement. That is the system shall protect itself from physical assault.

Consequence:

Negligible: This may result in the users' data being publicly released. More seriously, this may bring the economic loss of users. However, these entities (i.e. SD card) are out of the system, which is not under our control and the mitigation for this is easy, so we set the consequence as negligible.

Threat 2:

Threat description:

Criminals or business owners use the replacement of the QR code to induce users to download malicious plugins so that they can invade the user's mobile phone in order to obtain sensitive information of the user, such as address, ID information etc.

Possible Attacker:

Cyber Criminals / User / Business Owner

Security Goals:

Confidentiality: preserve the access control and disclosure restrictions on information. Guarantee that no one will break the rules of personal privacy and proprietary information.

Possible Mitigation:

- Strengthen the QR code parsing technology from the app side, so that inaccurate QR codes will not cause COVIDSafer app load.
- There should be a notification to users if malware is detected during a scan

This refers to extent to which a system shall verify the identity of its externals before interacting with them

Consequence:

Negligible: Attackers can invade the user's mobile phone in order to obtain sensitive information of the user, such as address, ID information etc. This may result in the loss of some uses' sensitive information but not threaten all users' data. Moreover, the current QR code parsing technology is mature, and such threats can be easily mitigated. So we judge the consequence is negligible.

Threat 3:

Threat description:

Attackers eavesdrop or destroy channel transmissions, obtain transmission information, and capture data streams between two components. This may result in the possibility of leakage or capture of encrypted transmission information between two components (i.e. COVIDSafer App and App Server, App Server and Central Database, Central Database and Portal Server and Portal Server and Portal).

Possible Attacker:

Cyber Criminals

Security Goals:

Confidentiality: Keep the data transmission secure and reliable so that the data integrity can be guaranteed.

Possible Mitigation:

- Strengthen the strength of encrypted transmission.
- Install firewall

This refers to the integrity of data being encrypted and the security of channel transmissions.

And this requires a system to ensure that its data and communications are not intentionally corrupted via unauthorized creation, modification or deletion etc.

Consequence:

Critical: The attacker will obtain the users' information from channel transmission and use this information to undermine the security of the system. The potential consequence may result in the loss of users' device sensitive information even modify the information sent to another component.

As the harm caused by eavesdropping will threaten the accuracy and integrity of data transmission, such damage will harm the purpose of the system. That is why we think the damage is large. However, there are many ways to prevent eavesdropping, such as optimizing the encryption algorithm of information so that even if the attacker gets the information, it cannot decrypt it and loses its meaning. So repair and preventive measures are easy compared to other threats. So we think such a consequence is critical.

Threat 4:

Threat description:

Government tracing staff or third party provider staff abuses legitimate database privileges for unauthorized purposes. In detail, they use reasonable access to access database data and leak it to others or institutions maliciously. Or, this may result from government tracing staff or third party provider staff due to mis operation.

Possible Attacker:

Government tracing staff / Third-Party provider staff

Security Goals:

Confidentiality: This refers to the specification of the access and usage privileges

of authenticated users and verification of authenticated user's login (i.e. Government tracing staff and third party staff). The system needs to strictly review the user's login and operation to ensure the integrity of the information.

Possible Mitigation:

- Enhance access control (E.g. double verification and face recognition etc.).
- Establish an audit log of user login and operation.

This refers to the authentication requirement of the system. It should verify the identity of require login-in user before allowing them to use its functions.

Consequence:

Catastrophic: Government tracing staff or third party provider staff (i.e. AWS) causes tracing records to be publicly released or the database and server being destroyed.

Since the authority of insiders is very high, and it is difficult to detect the threats caused by using the accounts of insiders to operate, the loss it brings is difficult to measure. More seriously, it may damage the entire database and server. And the difficulty of repairing is also very high, so we think such a threat is catastrophic.

Threat 5:

Threat description:

Attackers attack the database in order to obtain sensitive information. This attack may be achieved by exploiting unused and unneeded database services or functional vulnerabilities. Or an attacker can extract user data and machine secrets by exploiting bugs like SQL injection to read DB tables or read error messages.

Possible Attacker:

Cyber Criminals

Security Goals:

Confidentiality： System needs to strengthen its own protection and early warning mechanism to protect the information from being leaked, so as to ensure the integrity of the data.

Possible Mitigation:

- Build audits and logs;
- Increase the capacity of the database.
- Regular review of the database mechanism and prevention

This refers to the immunity and Intrusion detection requirement. That is a system shall have well organized protection mechanisms to protect itself from infection by unauthorized undesirable programs or vulnerabilities.

Consequence:

Critical: This allows attackers to learn the user sensitive information or tracing record information in the center database. The potential consequences may threaten the security of the user tracing record, but it will not threaten the administrator's authority and further threaten the operation of the database (such as closing the database, etc.). Since the repair cost of databases is large and the difficulty of repairing databases is large, we judge this consequence is critical based on our judgement rules.

Threat 6:

Threat description:

The tracing staff may release their login in token intentionally to seek improper benefits. Or they release their login token unintentionally, which are captured by malicious people.

Possible Attacker:

Government Tracing Staff / Cyber Criminals

Security Goals:

Confidentiality: keep the data including tracing staff login in information secret so that to protect the integrity of data in database

Possible Mitigation:

- System should review and verify the login host and IP information strictly when they try to access the system
- Change the token regularly
- Double verification during login

This refers to the requirement of Authentication requirements and intrusion detection requirements. The system should have a well-organized alarm mechanism to detect and record attempted accesses that fail authorization requirements by the staff and the abused user login token. Also the system should have a strict authentication mechanism for access control.

Consequence:

Catastrophic: Since the staff have a high authority to access the database, like querying the data in the central database, the loss of potential consequence is large, which refers to the integrity of the data and the stability of the system, even affects user trust in the system. At the same time, this threat is difficult to find and is likely to involve various aspects of damage since it occurs internally. The repair cost and difficulty of the potential is very likely to be very high. Hence, we judge this consequence potential is catastrophic.

Threat 7:

Threat description:

Attackers attack the portal and tampered the portal interface, causing the user's login to be monitored. This may allow attackers to learn about tracing staff login information.

Possible Attacker:

Cyber Criminals

Security Goals:

Confidentiality: Keep resources not available or disclosed to unauthorized individuals, entities or processes

Possible Mitigation:

Establish an effective webpage anti-tampering and monitoring mechanism:

- Realize real-time monitoring of web files. Monitor file integrity, read, write, delete, create, execute, link, rename
- Realize real-time protection of web files. Prevent website directory files from being maliciously tampered with, deleted and created.

Consequence:

Critical： Attackers may enter the database at will to view or leak user information stored in the database and may use this information to conduct illegal transactions.

The damage of this consequence affects the security and integrity of general users' sensitive information seriously, and affects users' trust in the system. However, there are many ways to quickly mitigate the consequences of this threat. Since we are more serious about the damage caused by the consequences, we mark such consequences as critical.

Threat 8:

Threat description:

An adversary may sniff the data sent from Server (app server or portal sever) to lead to a compromise of the tokens issued by the Identity Server so that they can collect the information from the server.

Security Goals:

Confidentiality: Ensure that the information transmitted by the server will not be leaked to illegal users to ensure the integrity and accuracy of the information

Possible Mitigation:

- Establish a mechanism to ensure that all traffic to server is over secure HTTPS connections.
- The server implements TLS (http+tls, websocket+tls, tcp+tls, mqtt+tls, etc.), closes non-TLS port communication, and ensures that the data transmission process must be encrypted.

This requires privacy and integrity requirements. The system shall keep its sensitive data and communication private from unauthorized individuals and programs to ensure its system shall ensure that its data and communications are not intentionally corrupted via unauthorized creation, modification, or deletion. Based on these, systems can ensure data integrity.

This requires

Consequence:

Critical: The possible consequence is that the sensitive data of many users is leaked， even the information of server administrators. When it may involve the leakage of sensitive data of many users, we would think that this kind of harm is relatively large. Although there are many repair methods and the cost is lower than the cost of repairing the server, we still pay more attention to the impact of the harm, so we mark this consequence as critical.

Denial of Service

Threat 1:

Threat description:

The attacker uses IP spoofing, and the compression server resets the connection of illegal users, which affects the connection of legitimate users. A large number of connection requests hit the app server or portal server, causing all available operating system resources to be exhausted, and ultimately the app server or portal server can no longer process legitimate user requests

Possible Attacker:

Cyber Criminals

Security Goals:

Availability: protect the system from DoS attacks and DDoS attacks to keep the stable operation of the system.

Possible Mitigation:

- Establish a trust level for all visiting IP. When a DDoS attack occurs, the IP with a high level of trust has priority access, thus solving the identification problem.
- Set up rules by installing a firewall, such as allowing or denying specific communication protocols, ports or IP addresses. When the attack is sent from a few abnormal IP addresses, you can simply use the denial rule to block all communications sent from the attack source IP.

The refers to survivability requirements of a system, that is the system should have capacity to survive itself when it meets attacks and decrease the loss of the attacks as much as possible.

Consequence:

Critical: May bring service interruption of app server or portal server.

This is more likely to affect the normal operation of the server. Moreover, this will seriously affect the transmission and storage of user data, so this is very harmful. But we usually think that a server will have disaster backups and daily backups, so it is relatively easy to restore the server's services. So we mark such consequences as critical.

Threat 2:

Threat description:

The attacker commands a bot army to flood the portal server or app server or portal server with traffic. This may result in the app server or portal server denial of service. The huge amount of traffic hits the network, causing all available network resources to be exhausted, and finally causing legitimate user requests to fail. The attacker is able to prevent the server from providing service to a legitimate user.

Possible Attacker:

Cyber Criminals

Security Goals:

Availability: protect system from DOS attacks and DDOS attacks to ensure the server stable operation and consistent operation so that the resources and data can be provided for legal users when needed

Possible Mitigation:

- Increase network capacity
- Monitor the usage of internal network traffic and server resources, and detect sudden changes in network traffic and abnormal usage of system resources as early as possible.
- Cooperate with Internet service providers (ISP) or information security service providers, and use their operation centers to monitor Internet communications.
- Record security matters and check the warnings issued by various security systems, such as network intrusion detection system (IDS) or network intrusion prevention system (IPS), anti-malware solutions, Internet gateways and firewalls, and detect suspicious things early Network activity.

This refers to the physical protection requirement and Survivability requirements of system to keep the system alarm in time when it meets attacks.

Consequence:

May bring service interruption of app server or portal server

This is more likely to affect the normal operation of the server. Moreover, this will seriously affect the transmission and storage of user data, so this is very harmful. But there a lot of mature technology to survive the system from such attacks so it is relatively easy to restore the server's services. So we mark such consequences as critical.

Threat 3:

Threat description:

The attacker hits the tracing device with a large number of connection requests, so that all available operating system resources are exhausted, and finally the tracing device can no longer provide the device.

Possible Attacker:

Cyber Criminals

Security Goals:

Availability: resources should be accessible when it is requested reasonably

Possible Mitigation:

- Prepare spare device in advance

This refers to the survivability requirement of the system to ensure the system has multiple ways to defend against attacks. This can reduce the possibility of system interruption or denial of service.

Consequence:

Negligible: The tracing device cannot provide service for tracing staff. Since this will only temporarily affect tracing staff's access to the database to query data without affecting the transmission and storage of user data, and can be mitigated in a simple way, we mark such consequences as negligible.

Threat 4:

Threat description:

The attacker uses the controlled machine to continuously send access requests to the portal or server, forcing the number of IIS connections to exceed the limit. When the CPU resources or bandwidth resources are exhausted, the portal website is also crashed

Possible Attacker:

Cyber Criminals

Security Goals:

Availability: protect system from DOS attacks and DDOS attacks

Possible Mitigation:

- Provide margin bandwidth in advance
- Use private network: through the internal logical isolation of the network, to prevent attacks from the internal network broilers
- Maintain the server regularly.

This refers to the survivability requirements and system maintenance security requirements of the system to keep the server in good working conditions and survive itself during attacks.

Consequence:

Critical: May bring service interruption of app server or portal server or portal website, even destroy the server. This is more likely to affect the normal operation of the server. Moreover, this will seriously affect the transmission and storage of user data, so this is very harmful. But we usually think that a server or database will have disaster backups and daily backups, so it is relatively easy to restore the server's services. So we mark such consequences as critical.

Threat 5:

Threat Description:

Attackers use possible vulnerabilities in the database to attack the central database, causing the database to crash (such as closing the database/deleting files, etc.) Or they crack the weak password of the privileged database user to enter the database to destroy the configuration of the database so that makes the database service terminal.

Possible Attacker:

Cyber Criminals

Security Goals:

Availability: ensure the system safety and stability

Possible Mitigation:

- Maintain the database regularly
- Install firewall
- Keep the antivirus software up to date

This refers to the survivability requirements and system maintenance security requirements of the system to keep the server in good working conditions and survive itself during attacks.

Consequence:

Critical： The database will interrupt the service, or the database may be destroyed in severe cases. This will affect the storage of data. The database denial of service will seriously affect the operation of the system and even affect the integrity of the data. The harm this brings cannot be ignored. As a software serving the public, we assume that the database will be backed up, so it is not difficult to restore the database, so we mark such consequences as critical.

Threat 6:

Threat Description:

App server crash due to technical failure or server capacity limitation

Possible Attacker:

Third Party Provider Staff or None attacker

Security Goals:

Availability: Keep the stability of the system. Preventing data delays or denials (removal) so that the data or resources should be accessible when needed

Possible Mitigation:

- Maintain the server regularly
- Optimize the server configuration and design

This refers to the survivability requirements and system maintenance security requirements of the system to ensure the server in good working conditions and design and survive itself during attacks to decrease the loss as much as possible.

Consequence:

Negligible ：May bring service interruption of app server or portal server. Assuming that the server undergoes rigorous and thorough testing before going online, the probability of such a threat occurring is low. Moreover, service interruption caused by non-malicious attacks is usually quick to recover. So we mark such consequences as negligible.

Elevation of Privilege

Threat 1:

Threat description:

By exploiting vulnerabilities (such as arbitrary code execution), an attacker expands initial unauthorized access rights of the portal server or app server to access other account content or privacy of the server.

Possible Attacker:

Cyber Criminals

Security Goals:

Authentication:

Possible Mitigation:

- Data execution protection
- The running application adopts the principle of least privilege (such as not using the administrator SID to run Internet Explorer) to reduce the possibility of buffer overflow exploits abusing the privileges of advanced users.
- Encryption of software and firmware.
- Use an operating system with mandatory access control
- Use the latest antivirus software

This refers to the immunity requirement Intrusion detection requirements of the system. That is the system should have a great protection mechanism to ensure it will not be infected by malicious users or programs and can detect any attempt by malicious users.

Consequence:

Catastrophic: The attacker may gradually probe the server and gain more permissions than initially, such as: access more sensitive information from other accounts, or even gain complete management control over the server. The damage of obtaining high authority for malicious purposes is large since it can affect the whole system availability， data integrity and confidentiality. And the repair cost is also large based on this. Hence, we judge such consequences is catastrophic.

Threat 2:

Threat description:

A user was misconfigured by an administrator intentionally or unintentionally and was mistakenly granted access permissions that exceeded his actual needs. For example, an ordinary user with certain access rights can easily access the database, even if the user does not have the relevant access rights to the database originally. Attackers only need to obtain these privileged user passwords to enter the database system, and then access and read any table in the database.

Possible Attacker:

Cyber Criminals / Government Tracing Staff / Third party Provider staff

Security Goals:

Authentication: this refers to system verify the identity of system externals before interacting with them to ensure the authentication is correct and authorized users have no abuse of their authority.

Possible Mitigation:

- Regularly ask authoritative audit institutions to audit the distribution and use of internal permissions
- Set up a reasonable permission distribution mechanism, such as modifying permissions and obtaining permissions requires multiple audits
- Set a strong password for the privileged account and record the operation record of the privileged account. If there is any abnormality, it will warn other users in real time.

This requires the security auditing requirements and authorization of system to ensure the system shall enable security personnel to audit the status and use of its security mechanisms and Specifies the access and usage privileges of authenticated users.

Consequence:

Catastrophic: The consequence may modification the permissions of other user accounts or modification the files of the server and database. When reasonable permissions are abused and permissions are mis-allocated and maliciously used by intentional people, the losses caused are difficult to measure. Because advanced permissions mean that the system (involving servers and databases) can be further damaged. Its repair difficulty and scope are likely to be higher. Therefore, we regard such consequences as catastrophic.

Threat 3:

Threat description:

An attacker can gain unauthorized access to resources in the app server or portal server by stealing the credentials of an app server or portal server. This allows them to get the control authority of the server and can modify key information of the server for blackmailing the server's administrator.

Possible Attacker:

Cyber Criminals

Security Goals:
Authentication: this refers to verification that the originator of an action is the originator.

Possible Mitigation:
- Use the latest antivirus software
- Architecture optimization
- Server hardening

This refers to the integrity requirements and identity requirements and privacy requirements. The system should have a mechanism to ensure keep its sensitive information private to unauthorized individuals and programs and ensure data not intentionally corrupted via unauthorized creation, modification, or deletion.

Consequence:
Catastrophic: May cause sensitive information on the server been publicly released or modified and the loss of control right of the server. When part or all of the administrative rights are used by unknown malicious attackers, it may cause a devastating blow to the system and is difficult to repair, so we believe that such consequences are disastrous.

Threat 4:

Threat description:
An attacker may gain unauthorized access to COVIDSafer App due to weak network configuration of the user so that the attacker can have access to modify the COVIDSafer App settings or get unauthorized access to get in touch with the sensitive information.

Possible Attacker:
Cyber Criminals

Security Goals:
Authentication ： this refers to unauthorized acquisition and elevation of authority

Possible Mitigation:
- Have a strict mechanism to authenticate the network
- Set network blacklist and whitelist for the COVIDSafer app
- Set firewall for network settings

This refers to the intrusion detection requirement of the system to detect potential danger that may influence the access authority of the system.

Consequence:
Negligible: The potential of the attacker may change the setting of COVIDSafer App or access to the uses sensitive information. Since this potential damage just covers a small group of user's information and is less likely to affect the server and database, it is easy to mitigate by having a correct configuration. So we judge this consequence is negligible.

Summary:

We mainly rate the severity of each threat consequence from two aspects: the potential damage and the cost (difficulty) of repairing the problems caused by the damage.

In terms of potential damage, we generally believe that the threat of being able to fully obtain administrator or tracing staff rights is more serious than the threat of leaking sensitive information. Because full access to the administrator authority may affect the security of the entire database data, the damage caused may not only be the leakage of user data, but also the damage of the database and the crash of the server. The harm of leaking sensitive data is generally greater than that of leaking general information. In terms of repair costs, the cost of repairing databases and servers will be higher, which involves the maintenance of the entire system, and it is significantly easier to repair the threat of tampering with pages or QR codes that cause users to enter malicious websites.

At the same time, since this system is for the public and is non-profit in nature, we will pay more attention to the impact caused by the great potential damage than the impact of high repair costs. Therefore, when the damage is high and the repair cost is low, we will consider it as critical, and when the damage is low and the repair cost is high, and we will consider it as marginal.

Reference

Docs.microsoft.com. 2021. *Microsoft Threat Modeling Tool overview - Azure*. [online] Available at: <https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool> [Accessed 28 March 2021].