Final Security Requirements Report

Architeture	Hybrid Application
Application domain type	m-Health
Authentication	Username and Password
Has DB	Yes
Type of data storage	SQL
Which DB	MySQL
Type of data stored	Personal Information ; Confidential Data ; Critical Data
User Registration	Yes
Type of Registration	The users will register themselves
Programming Languages	HTML5 ; PHP
Input Forms	Yes
Upload Files	Yes
The system has logs	Yes
The system has regular updates	Yes
The system has third-party	Yes
System Cloud Environments	Public Cloud
Hardware Specification	Yes
HW Authentication	Basic Authentication (user/pass)
HW Wireless Tech	4G / LTE ; 3G ; Bluetooth ; Wi-Fi ; GPS ; NFC
Data Center Phisical Access	Yes

Confidentiality

The property that ensures that information is not disclosed or made available to any unauthorized entity. In other words, information cannot be accessed by an unauthorized third party.

This requirement is applied were the information is stored.

Integrity

Is the property of safeguarding the correctness and completeness of assets in a Cloud & Mobile system. In other words it involves maintaining the data consistent, trustworthy and accurate during it life-cycle.

This requirements is applied in the Cloud and Mobile Ecosystem.

Not addressing this requirement may lead to vulnerabilities explored by attacks such as:

SQL Injection Attacks:

In this type of attack, the attacker inserts malicious code with the intention of accessing the unauthorized database for the purpose of obtaining confidential or critical data from the legitimate user.

Wrapping Attacks:

In a wrapping attack scenario, the attacker duplicates the SOAP message in the course of the translation and sends it to the server as a legitimate user. Therefore, the attacker may interfere with the malicious code.

MITM Attacks:

In this type of attack, an attacker attempts to intrude on a mail exchange or continuous message between two users or clients of a cloud-based mobile application (client-server).

Cookie Poisoning:

This type of attack consists of replacing or modifying cookie content in ways to gain unauthorized access to applications or Web pages. # Availability

Refers to the property which ensures that a mobile device or system is accessible and usable upon demand by authorized entities. In other words the mobile cloud-based application need to be always available to access by authorized people.

This requirement is applied were the information is stored.

Not addressing this requirement may lead to vulnerabilities explored by attacks such as:

DoS Attacks:

In this type of attacks, the attacker attempts to prevent the provision of a service or resource that are signed by authorized users by launching various types of flood

DDoS Attacks:

It is an improved case of DoS attacks in terms of flooding the target server with server with a huge amount of packets.

Authentication

Is the assurance that information transaction is from the source it claims to be from. The device authenticates itself prior to receiving or transmitting any information. It assures that the information received is authentic. It is assumed that communications may be intercepted by an unauthorized entity and data at rest may be subject to unauthorized access during transport and rest, taking into account the nature of the cloud and mobile ecosystem.

This security requirement is applied across all layers of the ecosystem under consideration, i.e., communication, transport and storage of information shared or exchanged between authorized entities.

Security Verification Requirements

- If the app provides users access to a remote service, some form of authentication, such as username/password authentication, is perfumed at the remote endpoint;
- if stateful session management is used, the remote andpoint uses rendomly generated session identifiers to authenticate client requests without sending the user's crendentials;
- If stateless token-base authentication is used, the server provides a token that has been signed using a secure algorithm;
- The remote endpoint terminates the existing session when the user logs out;
- A password policy exists and is enforcer at the remote endpoint;
- The remote endpoint implements a mechanism to protect against the submission of credentials an excessive number of times;
- Sessions are invalidated at the remote endpoint after a predefined period of inactivity and access number of times;
- Biometric authentication, if any, is not event-bound (i.e. using an API that simply returns "true" or "false"). Instead, it is based on unlocking the keychain/keystore;
- A second factor of authentication exists at the remote endpoint and the 2FA requirements is consistently enforced;
- Sensitive transactions require set-up authentication;
- The app informas the user of all login activities with their account. Users are able view a list of devices used to access the account, and to block specific devices.

Not addressing this requirement may lead to vulnerabilities explored by attacks such as:

Botnet Attack

A botnet is a collection of compromised devices that can be remotely controlled by an attacker, i.e. the bot master. Its main purpose is to steal business information, remote access, online fraud, phishing, malware distribution, spam emails, etc.

Phishing Attack

In a scenario of this type of attack, when using cloud services, an attacker can conduct phishing attacks by manipulating the web link to redirect it to a false link and hijack the user account for the purpose of stealing the your sensitive data.

DNS Attack

DNS attacks always occur in the case where the attacker makes use of the translation of the domain name in an Internet Protocol (IP) address, in order to access the confidential data of the user in an unauthorized way

MITM Attack

In this type of attack, an attacker attempts to intrude on a mail exchange or continuous message between two users or clients of a cloud-based mobile application (client-server).

Reused IP Address Attack:

This type of attack occurs whenever a IP address is reused on a network. This occurs because in a network the number of IP addresses is usually limited, which causes an address assigned to one user to be assigned to another, so that it leaves the network.

Wrapping Attacks

In a wrapping attack scenario, the attacker duplicates the SOAP message in the course of the translation and sends it to the server as a legitimate user. Therefore, the attacker may interfere with the malicious code.

Cookie Poisoning Attack

This type of attack consists of replacing or modifying cookie content in ways to gain unauthorized access to applications or Web pages.

Google Hacking Attacks

This type of attack involves the use of the Google search engine for the purpose of discovering confidential information that a hacker or wrongdoer can use for their benefit by hacking the account of a used.

Hypervisor Attacks:

In this type of attack the attacker aims to compromise the authenticity of sensitive user data and the availability of services from the cloud at the VM level.

References

- In general - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x04e-Testing-Authentication-and-Session-Management.md;
- For Android - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05f-Testing-Local-Authentication.md;
- For iOS - https://github.com/OWASP/owasp-mstg/blob/master/Document/0x06f-Testing-Local-Authentication.md.# Authorization

The property that determines whether the user or device has rights/privileges to access a resource, or issue commands.

These requirements or assumptions apply to the secure coding of PHP, C/C++, Java, C#, PHP, HTML, JavaScript, Swift programming languages in building mobile Android application and were the information might be accessed from and between the communications in the cloud and mobile ecosystem.

Not addressing this requirement may lead to vulnerabilities explored by attacks such as:

SQL Injection Attack

In this attack the perpetrator injects malicious code in the system to gain access to information or even to gain control of the entire system

XSS Attack

In this attack the perpetrator injects malicious code in the system to gain access to information or even to gain control of the entire system Reused IP Address This type of attack occurs whenever a IP address is reused on a network. This occurs because in a network the number of IP addresses is usually limited, which causes an address assigned to one user to be assigned to another, so that it leaves the network.

Botnet Attacks

A botnet is a collection of compromised devices that can be remotely controlled by an attacker, i.e. the bot master. Its main purpose is to steal business information, remote access, online fraud, phishing, malware distribution, spam emails, etc. ## Sniffer Attacks This type of attack is carried out by attackers using applications that can capture data packets in transit on a network, and if they are not heavily encrypted, can be read or interpreted.

Wrapping Attacks

In this attack scenario, the attacker duplicates the SOAP message in the course of the translation and sends it to the server as a legitimate user. Therefore, the attacker may interfere with the malicious code.

Google Hacking Attacks

This type of attack involves the use of the Google search engine for the purpose of discovering confidential information that a hacker or wrongdoer can use for their benefit by hacking the account of a used.

Hypervisor Attacks

Neste tipo de ataque o atacante tem como alvo comprometer a autenticidade dos dados sensíveis dos utilizadores e a disponibilidade de serviços a partir da cloud ao nível das VMs.

OS Command Injection

Applications are considered vulnerable to the OS command injection attack if they utilize non validated user input in a system level command what can lead to the invocation of scripts injected by the attacker.

Buffer Overflows

Buffer overflows is an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory. It can be triggered by non-validated inputs that are designed to execute code.

Session Hijacking

An attacker impersonates a legitimate user through stealing or predicting a valid session ID.

Session Fixation

An attacker has a valid session ID and forces the victim to use this ID.

Note:

The last three attack types only apply in the case where the C/C ++ and PHP programming language are used, respectively.

References

https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Transaction_Authorization_Cheat_Sheet.md

Non-Repudiation

The security property that ensures that the transfer of messages or credentials between 2 mobile users entities is undeniable .

This requirement is applied between information transactions, between information transactions over the Internet in the Cloud and in the database.

Accountability

The property that ensures that every action can be traced back to a single user or device .

This requirement is applied over Internet transactions.

Not addressing this requirement may lead to vulnerabilities explored by attacks such as:

DNS Attacks

DNS attacks always occur in the case where the attacker makes use of the translation of the domain name in an Internet Protocol (IP) address, in order to access the confidential data of the user in an unauthorized way.

MITM Attacks

In this type of attack, an attacker attempts to intrude on a mail exchange or continuous message between two users or clients of a cloud-based mobile application (client-server).

Reliability

Refers to the property that guarantees consistent intended behavior of an a general system, in this case applied to cloud and mobile ecosystem.

This requirement is applied over Internet transactions in the cloud and mobile ecosystem.

Privacy

In the context of cloud and mobile, privacy refers to the control of the user over the disclosure of his data. In other words only the user has control of the sharing of is personal information, is data is only made public if the user allowed it.

This requirement is applied where the information is stored .

Physical Security

Refers to the security measures designed to deny unauthorized physical access to mobile devices and equipment, and to protect them from damage or in other words gaining physical access to the device won't give access to it's information.

This requirement is applied were the information is stored in the device.

Not addressing this requirement may lead to vulnerabilities explored by attacks such as:

Physical Attack

This type of attack occurred when the perpetrator gains physical access to the location where the system is operating and tries to gain information stored in the system using his physical access.

Forgery Resistance

Is the propriety that ensures that the contents shared between entities cannot be forged by a third party trying to damage or harm the system or its users. In other words no one can try to forge content and send it in the name of another entities.

This requirement is applied in the device, in the cloud, and in the database.

Not addressing this requirement may lead to vulnerabilities explored by attacks such as:

Tampering

This type of attacks occurs when an attacker preforms physical modifications on the hardware where the software is implemented.

Reused IP Address Attack

In this attack some nods are made more attractive than others by tampering with the routing information, when arriving to the sinkhole node the messages may be dropped or altered.

Tamper Detection

Ensures all devices are physically secured, such that any tampering attempt is detected.

This requirement is applied were the information in the device.

Not addressing this requirement may lead to vulnerabilities explored by attacks such as:

Tampering

Is when an attacker preforms physical modifications on the hardware where the software is implemented.

Data Freshness

Status that ensures that data is the most recent, and that old messages are not mistakenly used as fresh or purposely replayed by perpetrators. In other words this requirement provides the guarantee that the data displayed is the most recent .

This requirement is applied to the cloud, since it says that messages sent between components of the cloud and mobile ecosystem can be captured and forwarded, by hypothesis and between the communications.

Not addressing this requirement may lead to vulnerabilities explored by attacks such as:

Tampering:
This type of attacks ocurrs when a attacker preforms physical modifications on the hardware where the software is implemented
Reused IP Address Attack: In this attack some nods are made more attractive than others by tampering with the routing information, when arriving to the sinkhole node the messages may be dropped or altered.

Confinement

Ensures that even if a party is corrupted, the spreading of the effects of the attack is as confined as possible.

This requirement is applied in the entire system.

ot addressing this requirement may lead to vulnerabilities explored by attacks such as: **Impersonation Attack:**
In this attack the attacker pretends to be one of the users of the system to fulfill is bad intentions.

Interoperability

Is the propriety that ensures that different software communicates and works well with each-other. I.e a software in health-care that works with data that comes from a third-party needs to be able to use and process the information given to it by this software.

This requirement is applied in the entire system.

ot addressing this requirement may lead to vulnerabilities explored by attacks such as:

Impersonation Attack:

In this attack the attacker pretends to be one of the users of the system to fulfill is bad intentions.

Data Origin Authentication

Ensures that the data being received by the software comes from the source it claims to be. In other words it ensures that the data being received is authentic and from a trusted party.

This requirement is applied between the communications.

Not addressing this requirement may lead to vulnerabilities explored by attacks such as: * MITM attack: This type of attacks occurs when an attacker gains access to a packet and re-sends it when it's beneficial to him, resulting in him gaining the trust of the system.