Final Security Requirements Report

Mobile Plataform	Hybrid Application
Application domain type	m-Health
Authentication	Yes
Authentication schemes	Factors-based authentication ; ID-based authentication
Has DB	Yes
Type of data storage	SQL (Relational Database)
Which DB	SQLite
Type of data stored	Critical Data
User Registration	Yes
Type of Registration	Will be an administrator that will register the users
Programming Languages	HTML5
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	3G ; 4G/LTE ; 5G ; 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.

Note *This requirement is applied were the information is stored*.

Failure to guarantee this security requirement can lead to the leakage or loss of confidential data shared among authorized users of the application e a aplicação poderá estar sujeita aos seguintes ataques:

1. Brute Force

The attacker attempts to gain access to systems' asset (information, functionality, identity, etc.) protected by a finite secret value by using trial-and-error to exhaustively explore all the possible secret values in the hope of finding the secret (or a value that is functionally equivalent) that will unlock the asset.

2. Eavesdropping

Eavesdropping is a type of attack where the attacker tries to gain access to sensitive information of legitimate users from the messages (text, voice and video) exchanged between two or more users of Instant Messaging (IM) applications. The same applies to recorded calls, call logs and multimedia stored in clear text on memory cards.

3. Session Hijacking

This type of attack involves an adversary exploiting weaknesses in the use of an application's authentication sessions. Put another way, this type of attack results from the successful exploitation of improper authentication. Its main purpose is account hijacking. The attacker may be able to steal or manipulate an active session and use it to gain unauthorised access to the application.

4. Session Fixation

The aim of this attack is account hijacking, with the aim of fraudulently accessing the area restricted to legitimate users of a web app or a hybrid mobile app. The success of this attack depends on prior login, as it requires the session ID of a legitimate user of the target application, impersonating the victim, which grants privileges and results in the violation of confidentiality, access control and authorisation of sensitive user data, and theft of money from mobile banking app or mobile interbank application.

5. Cross Site Request Forgery

Cross-site Request Forgery (CSRF) is an attack that forces the user to execute unintended actions in an application for which it is already authenticated in a given moment. These attacks target unrequested status changes, and not directly data theft, as the attacker cannot see the answer to the forged request.

6. 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).

7. Server Side Request Forgery

We are in the presence of a Server Side Request Forgery Attack (SSRF) as long as the web application is vulnerable and redirects the attacker's requests to the internal network and exposes local services to the remote attacker, which introduces different forms of risks.

8. Sniffing Attacks

Sniffing is the act of obtaining data in real time from data transmitted between smartphones (or tablets) and with the Cloud, through a network (Bluetooth, Wireless Sensor Network (WSN), Wi-Fi, 3G/4G/5G, etc.)

9. Buffer Overflow

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.

10. Spoofing

Spoofing attacks are a fraudulent act in which an entity fakes its identity to attempt to access resources and critical data. There are four variants of the spoofing attack, namely, content spoofing, identity spoofing, resource location spoofing and action spoofing.

11. Code Inclusion

Unlike code injection, in this type of attack, an attacker exploits a weakness in the target in order to force arbitrary code to be retrieved locally or from a remote location and executed.

12. Malware-as-a-Service

Malicious code, or simply malware, are scripts or programs that can be injected in the Cloud and Mobile ecosystem. Malware are traditionally mainly classified based on two main factors: propagation strategy (e.g., virus or worm) and malicious activity (trojan horse, spyware, adware, rootkits, botnets, ransomware, backdoors and key-loggers).

13. Code Injection

This type of attack targets injecting malicious code into user inputs from the interface (web application forms or hybrid mobile applications) of applications written in HTML5.

14. Command Injection Attacks

This is a class of attacks to which web applications are susceptible, resulting from the semantic gap existing between database interpretation and web application interpretation, as well as from the inappropriate handling of user input.

15. SQL Injection Attack

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

16. Reverse Enginnering

Reverse engineering attacks target the assets embedded in software. In such an attack scenario, the attacker by reverse engineering attempts to steal confidential information, such as embedded cryptographic keys or intellectual property in the form of algorithms.

17. Cryptanalysis

Cryptanalysis focuses on finding vulnerabilities in cryptographic algorithms and using these weaknesses to decrypt the ciphertext without knowing the secret key.

18. Cellular Rogue Base Station Attacks

Cellular Rogue Base Station is a security threat targeting a mobile phone network that can exploit the radio interface between smartphones and base stations, potentially launching passive or active attacks against user equipment. Such attacks range from acquiring the International Mobile Subscriber Identifier (IMSI) of subscribers, DoS, leaking private information on 4G networks and eavesdropping.

19. Rogue Access Points

The Access Points (AP) in a Wi-Fi networks are subject to the attack of access point spoofing, usually called Rogue Access Point (RAP). This attack consists of cloning the Media Access Control (MAC) address and Service Set IDentifier (SSID) of an AP, giving rise to the emergence of a fake access point posing as a genuine one, leading users to connect to this new network as if they were connecting to the genuine network. After connection, an attack is able to eavesdrops on its communication to hijack client's communication, re-direct clients to malicious websites, steal credentials (session hijacking) of the clients connecting to it.

20. GPS Spoofing Attacks

GPS has grown to such an extent that today it is considered a ubiquitous technology that provides positioning, navigation and timing services (PNT). As an essential element of the global information infrastructure, GPS cybersecurity faces serious challenge issues. Although some mission-critical systems even rely on GPS as a security measure, GPS in civilian version has no protection against malicious acts such as spoofing. According, "GPS spoofing breaches authentication by forging satellite signals to mislead users with wrong location/timing data that threatens homeland security".

21. Access Point hijacking

This type of attack is a variant of the session hijacking attack and targets the AP access credentials of legitimate administrators. These credentials can be extracted through a sniffing, brute force or MiTM attack. After this, the attacker is able to carry out other types of attacks, such as DoS and Rogue Access Points.

22. NFC Payment replay attacks

This type of attack targets the exploitation of vulnerabilities in the European Visa and Mastercad (EMV) wireless communication protocol between the smartcard and the payment terminal, namely, the authenticity of the payment terminal is not guaranteed to the customer's payment device and the banking data exchanged between the customer's payment device (smartcard) and the point of sale terminal are not encrypted and are transferred in clear text.

23. Wi-Fi SSID Tracking Attacks

This type of attack aims to obtain sensitive data (location, routine, trajectory, etc.) of users of mobile devices using Wi-Fi networks to access the Internet. Furthermore, it consists of using sophisticated sniffing devices to bypass authentication (for closed networks), extract and identify the MAC address of the mobile device and establish a match with its potential owner.

24. Phishing Attacks

In this type of attack scenario, an attacker can perform a phishing attack by manipulating a web link to attempt to redirect users to a false one and capture user information and account access, with the final objective of stealing sensitive data. Main attacks vectors are e-mail keyloggers through trojan horses and Man-in-the-Middle Attack of data proxies.

25. Pharming Attacks

Pharming is a special type of phishing attack or DNS poisoning attack in which the user is redirected to a fake website by changing the IP address on the DNS server. The target of the attack is the same as the phishing attack, i.e. theft of sensitive data and money from legitimate users of the applications.

26. Malicious QR Code

Although this type of attack also affects the category or application layer, it also falls under the category of Social Engineering attacks as it mainly relies on human behaviour and its vulnerabilities. For example, the victim may be tricked into reading a malicious QR code advertising a fake promotional campaign for a product from a supermarket car park.

27. On-Off Attacks

This type of attack targets a wireless sensor network, aiming to disrupt a trust redemption scheme, behaving alternately good and bad, in order to ensure immediate trust redemption before another attack occurs. On the other hand, this occurs because there is a security vulnerability that has to do with the fact that not all trust redemption schemes are able to effectively discriminate an On-Off attack and temporary errors, especially when it is good most of the attacker's behaviour, making him able to remain active in the system, as he has the ability to disguise attacks as temporary errors.

28. Mobile SIM Swapping

This attack targets the SIM card of a smartphone user, i.e. swapping the victim user's SIM card. SIM swapping can happen remotely. A cybercriminal, with a few important details about your life in hand, can answer security questions correctly, impersonate you, and convince your mobile carrier to reassign your phone number to a new SIM card. At that point, the criminal can get access to your phone’s data and start changing your account passwords to lock you out of your online banking profile, email, and more.

References

1. [https://capec.mitre.org/data/definitions/651.html];
2. [https://capec.mitre.org/data/definitions/112.html].

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.

Note: *This requirements is applied in the Cloud and Mobile Ecosystem.*

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

1. 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.

2. 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.

3. 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).

4. Cookie Poisoning:

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

5. Session Hijacking

This type of attack involves an adversary exploiting weaknesses in the use of an application's authentication sessions. Put another way, this type of attack results from the successful exploitation of improper authentication. Its main purpose is account hijacking. The attacker may be able to steal or manipulate an active session and use it to gain unauthorised access to the application.

6. Cross Site Request Forgery

Cross-site Request Forgery (CSRF) is an attack that forces the user to execute unintended actions in an application for which it is already authenticated in a given moment. These attacks target unrequested status changes, and not directly data theft, as the attacker cannot see the answer to the forged request.

7. Server Side Request Forgery

We are in the presence of a Server Side Request Forgery Attack (SSRF) as long as the web application is vulnerable and redirects the attacker's requests to the internal network and exposes local services to the remote attacker, which introduces different forms of risks.

8. Buffer Overflow

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.

9. Spoofing

Spoofing attacks are a fraudulent act in which an entity fakes its identity to attempt to access resources and critical data. There are four variants of the spoofing attack, namely, content spoofing, identity spoofing, resource location spoofing and action spoofing.

10. Audit Log Manipulation Attacks (ALM)

This type of attack targets log files for the purpose of manipulating (deleting, reading, and altering) them.

11. Code Inclusion

In this type of attack, an attacker exploits a weakness in the target in order to force arbitrary code to be retrieved locally or from a remote location and executed.

12. Malware-as-a-Service

Malicious code, or simply malware, are scripts or programs that can be injected in the Cloud and Mobile ecosystem. Malware are traditionally mainly classified based on two main factors: propagation strategy (e.g., virus or worm) and malicious activity (trojan horse, spyware, adware, rootkits, botnets, ransomware, backdoors and key-loggers).

13. Code Injection

This type of attack targets injecting malicious code into user inputs from the interface (web application forms or hybrid mobile applications) of applications written in HTML5.

14. Command Injection Attacks

This is a class of attacks to which web applications are susceptible, resulting from the semantic gap existing between database interpretation and web application interpretation, as well as from the inappropriate handling of user input

15. Reverse Enginnering

Reverse engineering attacks target the assets embedded in software. In such an attack scenario, the attacker by reverse engineering attempts to steal confidential information, such as embedded cryptographic keys or intellectual property in the form of algorithms.

16. Access Point hijacking

This type of attack is a variant of the session hijacking attack and targets the AP access credentials of legitimate administrators. These credentials can be extracted through a sniffing, brute force or MiTM attack. After this, the attacker is able to carry out other types of attacks, such as DoS and Rogue Access Points.

17. Phishing

In this type of attack scenario, an attacker can perform a phishing attack by manipulating a web link to attempt to redirect users to a false one and capture user information and account access, with the final objective of stealing sensitive data. Main attacks vectors are e-mail keyloggers through trojan horses and Man-in-the-Middle Attack of data proxies.

18. Malicious QR Code

Although this type of attack also affects the category or application layer, it also falls under the category of Social Engineering attacks as it mainly relies on human behaviour and its vulnerabilities. For example, the victim may be tricked into reading a malicious QR code advertising a fake promotional campaign for a product from a supermarket car park.

19. Malicious Insider

This type of attack occurs when there a malicious entity (client, employee, hypervisor, Cloud provider/corrector, etc.) takes advantage of its privileges to secretly realize a malicious activity, such as information theft and data or physical infrastructure destruction. This type of attack also occurs from client to server, when the person, employee or team with insider knowledge on how the system is built can implant malicious code to fully destroy the Cloud solution.

20. On-Off Attacks

This type of attack targets a wireless sensor network, aiming to disrupt a trust redemption scheme, behaving alternately good and bad, in order to ensure immediate trust redemption before another attack occurs. On the other hand, this occurs because there is a security vulnerability that has to do with the fact that not all trust redemption schemes are able to effectively discriminate an On-Off attack and temporary errors, especially when it is good most of the attacker's behaviour, making him able to remain active in the system, as he has the ability to disguise attacks as temporary errors.

21. Mobile SIM Swapping

This attack targets the SIM card of a smartphone user, i.e. swapping the victim user's SIM card. SIM swapping can happen remotely. A cybercriminal, with a few important details about your life in hand, can answer security questions correctly, impersonate you, and convince your mobile carrier to reassign your phone number to a new SIM card. At that point, the criminal can get access to your phone’s data and start changing your account passwords to lock you out of your online banking profile, email, and more.

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.

Note: *This requirement is applied were the information is stored.*

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

1. Flooding

In this type of attacks, commonly referred to as denial of service (DoS) or distribuited denial of service (DDoS), the attacker attempts to negatively impact of the service or resource availability from authorized users, by using different types vulnerability exploitation or flooding - SYN flooding attacks, User Datagram Protocol (UDP) flooding, Internet Control Message Protocol (ICMP) flooding, etc. - on the server.

2. Session Hijacking

This type of attack involves an adversary exploiting weaknesses in the use of an application's authentication sessions. Put another way, this type of attack results from the successful exploitation of improper authentication. Its main purpose is account hijacking. The attacker may be able to steal or manipulate an active session and use it to gain unauthorised access to the application.

3. Server Side Request Forgery

We are in the presence of a Server Side Request Forgery Attack (SSRF) as long as the web application is vulnerable and redirects the attacker's requests to the internal network and exposes local services to the remote attacker, which introduces different forms of risks.

4. Buffer Overflow

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.

5. Spoofing

Spoofing attacks are a fraudulent act in which an entity fakes its identity to attempt to access resources and critical data. There are four variants of the spoofing attack, namely, content spoofing, identity spoofing, resource location spoofing and action spoofing.

6. Malware-as-a-Service

Malicious code, or simply malware, are scripts or programs that can be injected in the Cloud and Mobile ecosystem. Malware are traditionally mainly classified based on two main factors: propagation strategy (e.g., virus or worm) and malicious activity (trojan horse, spyware, adware, rootkits, botnets, ransomware, backdoors and key-loggers).

7. Code Injection

This type of attack targets injecting malicious code into user inputs from the interface (web application forms or hybrid mobile applications) of applications written in HTML5.

8. Command Injection Attacks

This is a class of attacks to which web applications are susceptible, resulting from the semantic gap existing between database interpretation and web application interpretation, as well as from the inappropriate handling of user input

9. SQL Injection Attack

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

10. GPS Jamming Attacks

This attack aims to interrupt or obstruct the communication between the emitting satellite and the device (smartphone/tablet) receiving the GPS signal. Normally, the attack consists of blocking the signal from the receiver, since the receiving signal is weaker compared to the broadcasting signal, and can be carried out in two different ways, namely, blanket jamming, and deception jamming.

11. Orbital Jamming Attacks

This type of attack targets low-orbit satellites because, although these low-orbit satellites are attractive due to the low power levels required for communications links from terrestrial terminals, they can also be vulnerable to jamming attacks when used in some applications. In fact, a jammer of reasonable power could easily saturate the RF front-end of a low-orbit satellite, resulting in disabling the link across the entire frequency band.

12. DoS (Cellular) Jamming Attack

Interference attacks target radio communication technology (communication between smart devices and base stations). This attack can be caused by noise, interference, disruption or by sending corrupted data packets, with the purpose of causing DoS in the physical transmission of signals on certain routes.

13. Bluejacking and Bluesnarfing Attacks

These are DDoS-type attacks that target a Bluetooth wireless network in order to shut down activity on it. It usually occurs through an attack coming from a connection of malicious entities in a target network.

14. Wi-Fi Jamming Attacks

This is a denial-of-service attack that blocks the radio frequency, making access to the Wi-Fi network and consequently to the Internet unavailable.

15. Access Point hijacking

This type of attack is a variant of the session hijacking attack and targets the AP access credentials of legitimate administrators. These credentials can be extracted through a sniffing, brute force or MiTM attack. After this, the attacker is able to carry out other types of attacks, such as DoS and Rogue Access Points.

16. Phishing

In this type of attack scenario, an attacker can perform a phishing attack by manipulating a web link to attempt to redirect users to a false one and capture user information and account access, with the final objective of stealing sensitive data. Main attacks vectors are e-mail keyloggers through trojan horses and Man-in-the-Middle Attack of data proxies.

17. Malicious QR Code

Although this type of attack also affects the category or application layer, it also falls under the category of Social Engineering attacks as it mainly relies on human behaviour and its vulnerabilities. For example, the victim may be tricked into reading a malicious QR code advertising a fake promotional campaign for a product from a supermarket car park.

18. Malicious Insider

This type of attack occurs when there a malicious entity (client, employee, hypervisor, Cloud provider/corrector, etc.) takes advantage of its privileges to secretly realize a malicious activity, such as information theft and data or physical infrastructure destruction. This type of attack also occurs from client to server, when the person, employee or team with insider knowledge on how the system is built can implant malicious code to fully destroy the Cloud solution.

19. Mobile SIM Swapping

This attack targets the SIM card of a smartphone user, i.e. swapping the victim user's SIM card. SIM swapping can happen remotely. A cybercriminal, with a few important details about your life in hand, can answer security questions correctly, impersonate you, and convince your mobile carrier to reassign your phone

number to a new SIM card. At that point, the criminal can get access to your phone’s data and start changing your account passwords to lock you out of your online banking profile, email, and more.

Authenticity

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.

Note: *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:

1. Botnets 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.

2. Phishing

In this type of attack scenario, an attacker can perform a phishing attack by manipulating a web link to attempt to redirect users to a false one and capture user information and account access, with the final objective of stealing sensitive data. Main attacks vectors are e-mail keyloggers through trojan horses and Man-in-the-Middle Attack of data proxies.

3. 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

4. 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).

5. 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.

6. 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.

7. 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.

8. 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.

9. VM Escape

This type of attack occurs whenever an application escapes the VM and obtains control over the VMM, as it escalates its VM privileges to root level. The malicious application accesses the host machine, bypassing the hypervisor.

10. Session Fixation

The aim of this attack is account hijacking, with the aim of fraudulently accessing the area restricted to legitimate users of a web app or a hybrid mobile app. The success of this attack depends on prior login, as it requires the session ID of a legitimate user of the target application, impersonating the victim, which grants privileges and results in the violation of confidentiality, access control and authorisation of sensitive user data, and theft of money from mobile banking app or mobile interbank application.

11. Brute Force

The attacker attempts to gain access to systems' asset (information, functionality, identity, etc.) protected by a finite secret value by using trial-and-error to exhaustively explore all the possible secret values in the hope of finding the secret (or a value that is functionally equivalent) that will unlock the asset.

12. Buffer Overflow

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.

13. Spoofing

Spoofing attacks are a fraudulent act in which an entity fakes its identity to attempt to access resources and critical data. There are four variants of the spoofing attack, namely, content spoofing, identity spoofing, resource location spoofing and action spoofing.

14. Cache Poisoning

This type of attack has to do with any attack whereby an attacker caches incorrect or harmful material. The cache targeted can be an application's cache (e.g., a web browser cache) or a public cache (fe.g., a DNS or ARP cache).

15. Reverse Enginnering

Reverse engineering attacks target the assets embedded in software. In such an attack scenario, the attacker by reverse engineering attempts to steal confidential information, such as embedded cryptographic keys or intellectual property in the form of algorithms.

15. NFC Payment replay attacks

This type of attack targets the exploitation of vulnerabilities in the European Visa and Mastercad (EMV) wireless communication protocol between the smartcard and the payment terminal, namely, the authenticity of the payment terminal is not guaranteed to the customer's payment device and the banking data exchanged between the customer's payment device (smartcard) and the point of sale terminal are not encrypted and are transferred in clear text.

16. Bypassing Physical Security

This type of attack aims to circumvent or avoid detection by physical security and building surveillance systems and use methods to bypass electronic or physical locks protecting entry points. It also results in other types of attacks aimed at accessing, altering or destroying sensitive user information or making a service or resource unavailable.

17. Physical Theft

This type of attack aims to access and steal the target user's device in order to perform a malicious action, such as altering, deleting, leaking, inserting and destroying data, as well as stealing money through banking transactions, posing as the rightful owner. The attacker can simply destroy the device, preventing the user from accessing their data and the services provided in the form of an application as a service.

18. On-Off Attacks

This type of attack targets a wireless sensor network, aiming to disrupt a trust redemption scheme, behaving alternately good and bad, in order to ensure immediate trust redemption before another attack occurs. On the other hand, this occurs because there is a security vulnerability that has to do with the fact that not all trust redemption schemes are able to effectively discriminate an On-Off attack and temporary errors, especially when it is good most of the attacker's behaviour, making him able to remain active in the system, as he has the ability to disguise attacks as temporary errors.

19. Mobile SIM Swapping

This attack targets the SIM card of a smartphone user, i.e. swapping the victim user's SIM card. SIM swapping can happen remotely. A cybercriminal, with a few important details about your life in hand, can answer security questions correctly, impersonate you, and convince your mobile carrier to reassign your phone number to a new SIM card. At that point, the criminal can get access to your phone’s data and start changing your account passwords to lock you out of your online banking profile, email, and more.

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;
- CAPEC - https://capec.mitre.org/data/definitions/141.html.

Authorization

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

Note: *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:

1. SQL Injection Attack

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

2. 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.

3. 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.

4. 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.

5. Sniffing 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. Buffer Overflow

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.

11. Session Fixation

The aim of this attack is account hijacking, with the aim of fraudulently accessing the area restricted to legitimate users of a web app or a hybrid mobile app. The success of this attack depends on prior login, as it requires the session ID of a legitimate user of the target application, impersonating the victim, which grants privileges and results in the violation of confidentiality, access control and authorisation of sensitive user data, and theft of money from mobile banking app or

mobile interbank application.

12. Brute Force

The attacker attempts to gain access to systems' asset (information, functionality, identity, etc.) protected by a finite secret value by using trial-and-error to exhaustively explore all the possible secret values in the hope of finding the secret (or a value that is functionally equivalent) that will unlock the asset.

13. Cross Site Request Forgery

Cross-site Request Forgery (CSRF) is an attack that forces the user to execute unintended actions in an application for which it is already authenticated in a given moment. These attacks target unrequested status changes, and not directly data theft, as the attacker cannot see the answer to the forged request.

14. 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).

15. VM Escape

This type of attack occurs whenever an application escapes the VM and obtains control over the VMM, as it escalates its VM privileges to root level. The malicious application accesses the host machine, bypassing the hypervisor.

16. Malware-as-a-Service

Malicious code, or simply malware, are scripts or programs that can be injected in the Cloud and Mobile ecosystem. Malware are traditionally mainly classified based on two main factors: propagation strategy (e.g., virus or worm) and malicious activity (trojan horse, spyware, adware, rootkits, botnets, ransomware, backdoors and key-loggers).

17. Reverse Enginnering

Reverse engineering attacks target the assets embedded in software. In such an attack scenario, the attacker by reverse engineering attempts to steal confidential information, such as embedded cryptographic keys or intellectual property in the form of algorithms.

18. Phishing

In this type of attack scenario, an attacker can perform a phishing attack by manipulating a web link to attempt to redirect users to a false one and capture user information and account access, with the final objective of stealing sensitive data. Main attacks vectors are e-mail keyloggers through trojan horses and Man-in-the-Middle Attack of data proxies.

19. Malicious Insider

This type of attack occurs when there a malicious entity (client, employee, hypervisor, Cloud provider/corrector, etc.) takes advantage of its privileges to secretly realize a malicious activity, such as information theft and data or physical infrastructure destruction. This type of attack also occurs from client to server, when the person, employee or team with insider knowledge on how the system is built can implant malicious code to fully destroy the Cloud solution.

20. Mobile SIM Swapping

This attack targets the SIM card of a smartphone user, i.e. swapping the victim user's SIM card. SIM swapping can happen remotely. A cybercriminal, with a few important details about your life in hand, can answer security questions correctly, impersonate you, and convince your mobile carrier to reassign your phone number to a new SIM card. At that point, the criminal can get access to your phone’s data and start changing your account passwords to lock you out of your online banking profile, email, and more.

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 .

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

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

1. VM Escape

This type of attack occurs whenever an application escapes the VM and obtains control over the VMM, as it escalates its VM privileges to root level. The malicious application accesses the host machine, bypassing the hypervisor.

2. Mobile SIM Swapping

This attack targets the SIM card of a smartphone user, i.e. swapping the victim user's SIM card. SIM swapping can happen remotely. A cybercriminal, with a few important details about your life in hand, can answer security questions correctly, impersonate you, and convince your mobile carrier to reassign your phone number to a new SIM card. At that point, the criminal can get access to your phone’s data and start changing your account passwords to lock you out of your online banking profile, email, and more.

Accountability

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

Note: *This requirement is applied over Internet transactions.*

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

1. 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.

2. 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).

3. VM Escape

This type of attack occurs whenever an application escapes the VM and obtains control over the VMM, as it escalates its VM privileges to root level. The malicious application accesses the host machine, bypassing the hypervisor.

Reliability

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

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

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.

Note: *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:

1. Bypassing Physical Security

This type of attack aims to circumvent or avoid detection by physical security and building surveillance systems and use methods to bypass electronic or physical locks protecting entry points. It also results in other types of attacks aimed at accessing, altering or destroying sensitive user information or making a service or resource unavailable.

2. Physical Theft

This type of attack aims to access and steal the target user's device in order to perform a malicious action, such as altering, deleting, leaking, inserting and destroying data, as well as stealing money through banking transactions, posing as the rightful owner. The attacker can simply destroy the device, preventing the user from accessing their data and the services provided in the form of an application as a service.

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.

Note: *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:

1. Tampering

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

2. 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.

Note: *This requirement is applied were the information in the device.*

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

1. Tampering

Is when an attacker performs 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.

Note: *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:

1. Tampering

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

2. 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.

Note: *This requirement is applied in the entire system.*

Interoperability

Is the propriety that ensures that different software communicates and works well with each-other, sharing resources such as network, processing and memory without constraints.

Note: *This requirement is applied in the entire system.*

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.

Note: *This requirement is applied between the communications.*

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

1. 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.

2. Brute Force

The attacker attempts to gain access to systems' asset (information, functionality, identity, etc.) protected by a finite secret value by using trial-and-error to exhaustively explore all the possible secret values in the hope of finding the secret (or a value that is functionally equivalent) that will unlock the asset.

3. VM Escape

This type of attack occurs whenever an application escapes the VM and obtains control over the VMM, as it escalates its VM privileges to root level. The malicious application accesses the host machine, bypassing the hypervisor.

4. Spoofing

Spoofing attacks are a fraudulent act in which an entity fakes its identity to attempt to access resources and critical data. There are four variants of the spoofing attack, namely, content spoofing, identity spoofing, resource location spoofing and action spoofing.

5. Cache Poisoning

This type of attack has to do with any attack whereby an attacker caches incorrect or harmful material. The cache targeted can be an application's cache (e.g., a web browser cache) or a public cache (fe.g., a DNS or ARP cache).