Final Attack Models Report

Mobile Plataform iOS App
Application domain type m-Health
Authentication Yes

Authentication schemes ID-based authentication

Has DBYesType of data storageSQLWhich DBSQLite

Type of data stored Personal Information; Confidential Data; Critical Data

User Registration Ye

Type of Registration The users will register themselves

Programming Languages C/C++
Input Forms Yes
Upload Files No
The system has logs Yes
The system has regular updates Yes
The system has third-party Yes

System Cloud Environments Private Cloud

Hardware Specification Yes

HW AuthenticationBasic Authentication (user/pass)HW Wireless Tech3G; 4G/LTE; 5G; Wi-Fi

Data Center Phisical Access Yes

Denial of Services

In a DoS attack scenario, the attacker attempts to disrupt the network or disable services provisioned by a server by sending uninterrupted data packets to the target server and without changing nodes, data packets, or decrypting encrypted data. Typically, these data packets take up bandwidth and consume server resources.

Definition

In such attacks, the attacker attempts to prevent a service or feature that is signed by authorized users from being released by launching various types of floods - SYN flooding, User Datagram Protocol (UDP) flooding, Internet Control Message Protocol (ICMP) attacks) flooding, etc - on the server.

Technical Impact

- · Crash, Exit, or Restart;
- Bypass protection mechanism;
- Other.

Risk

High.

Likelihood of Exploit

• High.

Attacker's Powers

- Prevent the availability of a service or resource to authorized users;
- Perpetrating other types of attacks while services or features are unavailable, such as Spoofing.

Recommendations

In order to ensure that the mobile application is resilient or immune to the DoS attacks, it is recommended that the measures described in the good practice report and the security tests present in the full report are followed.

References

1. [https://cwe.mitre.org/data/definitions/400.html]

Denial of Services Attacks Diagram

availability system communication resources OR |- 1. Block mobile communication services |- 2. Compromise machine to support in flooding |- 1. Flood by a large number of requests |- 1. Launch Application DoS Attack OR | |- 1. Back |- 2. RUDY J-3. Slowloris J- 2. Launch Protocol DoS attack |- 1. ARP Poison |- 2. Land |- 3. Neptune (SYN Flood) |-4. Ping of Death J-5. Teardrop |-3. Launch Volume DoS attack |- 1. Smurf (ICMP Flood) |- 2. UDP Storm |- 3. Peer-to-peer |- 4. Physical destruction or alteration of components AND |- 1. Permanent DoS

Distributed Denial of Services Attacks

Distributed Denial of Services (DDoS) is an enhanced DoS attack type, originating from multiple network attack surfaces that were previously compromised to disrupt the services or resources provided by the target server. It differs from DoS in that it generates more traffic, so that the targeted server cannot handle requests.

Definition

The DDoS attack attempts to make a service unavailable to intended users by draining the system or network resource. Attackers can now launch various DDoS attacks, including resource-focused attacks (eg, network bandwidth, memory, and CPU) and app-focused attacks (eg, mobile applications, database service) from almost every attack. places.

Technical Impact

- · Crash, Exit, or Restart;
- · Bypass protection mechanism;
- · Other.

Risk

High.

Likelihood of Exploit

High.

Attacker's Powers

- Make features and services unavailable to authorized users;
- Perpetrate other types of attacks and even extract sensitive and critical data.

Recommendations

In order to ensure that the mobile application is resilient or immune to the DDoS attacks, it is recommended that the measures described in the good practice report and the security tests present in the full report are followed.

References

1. [[https://cwe.mitre.org/data/definitions/400.html]

Distributed Denial of Services Attacks Diagram

Goal: Stop the system availability an
communication resources
OR
- 1. Block mobile communication services
- 2. Compromise machines to support in flooding
AND
- 1. Flood by a large number of requests
OR
-1. Launch Application DDoS Attack
-3. Slowloris
- 2. Launch Protocol DDoS attack
-2. Lattu
-3. Neptune (SYN Flood) -4. Ping of Death
-3. Launch Volume DDOS attack
OR
-3. Peer-to-peer
-4. Physical destruction or alteration of
components
AND
-1. Permanent DDoS

Buffer Overflows Attack

As its name implies, buffer overflows occur when data exceeding its capacity is placed in a buffer. This occurs in programs implemented in C or C++, as these programming languages do not check if buffer limits are violated.

Definition

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. Buffer overflow may result in erratic program behavior, including memory access errors, incorrect results, a crash, or a breach of system security.

Technical Impact

- · Modify Memory;
- Execute Unauthorized Code or Commands.

Risk Analysis

• High Risk

Likelihood of Exploit

• High.

Attacker Powers

- Overwrite the return address of a procedure call;
- Obtain control of a system;
- Launch more virulent attacks, such DoS or DDoS.

Recommendations

In order to ensure that the mobile application is resilient or immune to the buffer overflows attack, it is recommended that the measures described in the good practice report and the security tests present in the full report are followed.

References

- 1. [https://cwe.mitre.org/data/definitions/120.html];
- 2. [https://www.first.org/cvss/calculator/3.1#CVSS:3.1/];
- 3. [https://www.first.org/cvss/v3.1/examples].

Buffer Overflows Attack Diagram

```
OR
|- 1. Heap Buffer Overflow
| AND
| - 1. Exploit the heap overflow vulnerability
| |- 2. Pass as a program argument a string ...
|- 2. Stack Buffer Overflow
| AND
| |- 1. To access to source code
| | OR
| | |- 1. Trial-error stategy
| | |- 2. Use reverse engineering techniques
| |- 3. Exploit buffer overflow exploit to overwrite the return address
```

Spoofing Attacks

In a nutshell, spoofing attacks consist of spoofing the caller ID in order to impersonate a trusted entity and thus obtain confidential information in a disguised manner.

Definition

In this type of attack, the attacker can spoof the "Caller ID" and impersonate him as a legitimate user, i.e., an attacker could spoof the "Caller ID" and impersonate a trusted party. Recent studies have also shown how to spoof MMS messages that appeared to be messages from a number that operators use to send alerts or update notifications. In addition, base stations can also be counterfeited. On the other hand, there is also the mobile application spoofing attack, which consists of an attack where a malicious mobile application mimics the visual appearance of another one. The goal of the adversary is to trick the user into believing that she is interacting with a genuine application while she interacts with one controlled by the adversary. If such an attack is successful, the integrity of what the user sees as well as the confidentiality of what she inputs into the system can be violated by the adversary.

Technical Impact

- · Bypass Protection Mechanism;
- Gain Privileges or Assume Identity.

Risk Analysis

· Critical Risk.

Likelihood of Exploit

High.

Attacker Powers

- Faker caller ID;
- · Monitoring of calls and access to the confidential information of legitimate users from voice or text messages.

Recommendations

To ensure that the mobile application is resilient or immune to Spoofing attacks, it is recommended that the measures described in the good practice report and the security tests present in the full report are followed to ensure authenticity, integrity, privacy and authenticity of the data.

References

1. [https://cwe.mitre.org/data/definitions/290.html].

Spoofing Attacks Diagram

```
Goal: Access resources or obtain banking and other
critical information
OR
|- 1. IP Spoofing
I AND
   |- 1. Obtains the IP address of a legitimate user
   |- 2. Alter TCP/IP packet headers to MTH
   |- 3. Hides the identity
|- 2. Metadata Spoofing
I AND
   |- 1. Obtains the IP address of a legitimate user
   |- 2. Alter TCP/IP packet headers to MTH
|- 3. DNS Spoofing
| AND
   |- 1. Supplie false DNS information to a VM
   |- 2. Alter TCP/IP packet headers to MTH
   J- 3. Hides Its identity
   |- 4. The user reach the attackers fake site
|- 4. ARP Spoofing
I AND
   |- 1- Binds its MAC address to IP address ...
   |- 2. Sends spoofed ARP messages
|-5. Mobile User ID Spoof
| OR
   I-1. Spoof caller ID
   |- 2. Spoof MMS sender ID
```

VM Migration Attacks

A malicious user can start or redirect the migration process to a different network in which he has access or untrusted host, or it can just be copied and used elsewhere, which compromise the VM with the passwords, credentials on it and in case of coping it makes it difficult to trace the attacker.

Definition

VMs roll back to their previous state if an error occurs. Unfortunately, this factor can re-expose them to security vulnerabilities, and attackers can gain benefit to attack on this compromised hypervisor. It is important to protect the data during migration. In fact, this is the defending of data privacy and integrity from various network attacks during migration. Live migration might be susceptible to many attacks like "man-in-the-middle", "denial-of-service" and "replay. The data during the migration can be sniffed or tampered easily as it is not encrypted.

Technical Impact

- Read Application Data (lack of confidentiality);
- · Modify Application Data (lack of integrity and confidentiality).

Risk Analisys

High Risk.

Likelihood of Exploit

High.

Attacker Powers

- Launch attacks such as man-in-the-middle, DoS and replay;
- Detect or tamper with data during migration as it is not encrypted.

Recommendations

To ensure that the mobile application is resilient or immune to VM Migration attacks, it is recommended that the measures described in the good practice report and the security tests present in the full report are followed to ensure authenticity, integrity, privacy, confinement, and authenticity of the data.

References

1. [https://cwe.mitre.org/data/definitions/311.html].

VM Migration Attacks Diagram

	al: Obtain user confidential data
AN	
_	Initiate migration of desired VM/data Obtain and process captured files
-	AND
li '	- 1. Remote captured files
li .	I OR
li .	-1. Exfiltrate via network
	- 2. Exfiltrate via removable media
	- 3. Exfiltrate via capture device
İ	- 4. Exfiltrate via Wireless
1	- 2. Process captured files
1	OR
1	-1. Local
1	AND
	-1. Obtain forensic apps
ļ	
!	-1. Downloads existing apps
ļ.	-2. Write customs application
H	-2. Introduce forensic apps into the system -3. Execute applications
H	
H	AND -1. Opportunity to run processor-intensive
li .	-2. Write to run executable/binary Files
li	-3. Exclusive access to one or more PCs
li .	-4. Suficiente storage
i	- 2. Remote
i	AND
Ī	- 1. Obtain forensic apps
1	
1	-1. Downloads existing apps
_	-2. Write custom apps
	- 2. Execute applications
ļ.	
l!	-1. File recovery
1 2	- 2. Registry analysis 3. Install network tap
	AND
li ʻ	- 1. Physical access to desired cable(s)
li	OR
i	- 1. Trial and error
1	AND
İ	-1. Access to significant proportion of cable infranstructure
1	- 2. Suficiente storage space
1	-3. Time!
1	- 2. Understand cable/network infrastructure
1	- 2. Tap and connect listening computer
	AND
	-1. Expose cable and connect tap device
	- 2. Install packet capture device
	-3. Connect tap to capture device without dropping connect
	- 3. Time! - 4. Possession of dedicated hardware
	AND
	I-1. Obtain
i	- 2. Introduce into the organization covertly

This type of attacks ocurre when there is a malicious entity (client, employee, Hypervisor, Cloud Provider/Broker, etc.) takes advantage of its privileges to covertly carry out any malicious activity such as information theft and data destruction or physical infrastructures.

Definition

Malicious Hypervisor, Malicious Clients, Malicious Cloud Provider/Broker, etc. are all the other terms which can also be used as an alternative to malicious insiders. This kind of attack occurs from client to server when the person, employee or staffs who know how the system runs, can implant malicious codes to destroy everything in the cloud system.

Technical Impact

- · Read Application Data;
- · Read Files or Directories;
- Modify Application Data;
- · Modify Files or Directories;
- · Gain Privileges or Assume Identity.

Analysis of Risk

• High.

Likelihood Of Exploit

• High.

Attacker Powers

• Implants malicious codes to destroy everything in the cloud system; * Steals confidential data.

Recommendations

In order to ensure that the mobile application is resilient or immune to Malicious Insiders attacks, it is recommended that the measures described in the good practice report and the security tests present in the full report are followed.

References

1. [https://cwe.mitre.org/data/definitions/285.html].

Malicious Insiders Attacks Diagram

```
Goal: Stop the system availability
communication resources
OR
|- 1. Alteration
| OR

    |-1. Unauthorized alteration of registry

  |- 2. Launch virus or malware injection
|- 2. Snooping
OR
  |- 1. Misuse
  |- 2. Violation of organization policy
|-3. Elevation
| AND
  |- 1. Acquire admin privilege
      |- 1. Send email exploit
      |- 2. Poor configuration
      AND
        |- 1. Steal password
         | OR
      | | |- 1. Sniff network
     | | |- 2. Rout Telnet
|-4. Distribution
| AND
  |- 1. File sharing
  | OR
      |- 1. E-mail
      | OR
         |-1. Local account
         |- 2. Web-based account
      J-2. Electronic Drop Box
      OR
         |-1. FTP to file
         |- 2. Internet
         | OR
         | |- 1. Post to new group
           |- 2. Post to website
      J-3. Online chat
      |-4. Copy to media
      | OR
         |- 1. Card memory MicroSDXC
         |- 2. CD-Room
         |- 3. USB Drive
```

VM Escape Attacks

This type of attack occurs when an application escapes from the VM and gains control of VMM, as it escapes the VM privilege and obtains the root privilege.

Definition

VM escape is where an application running on a VM can directly have access to the host machine by bypassing the hypervisor, being the root of the system it makes this application escape the VM privilege and gain the root privilege. In this type of attack the attackers attempt to break down the guest OS in order to access the hypervisor or to penetrate the functionalities of other guest OS and underlying host OS. This breaking of the guest OS is called as escape. If the attackers escapes the guest OS it may compromise the hypervisor and as a result it may control over the entire guest OS. In this way the security breach in single point in hypervisor may break down all the hypervisor. If the attacker controls the hypervisor, it can do anything to the VM on the host system.

Risk Analysis

Critical Risk.

Attacker Powers

- Shutdown and eliminate target or victim VMs, resulting in the loss and destruction of data or information;
- Compromise the hypervisor and other resources.

Recommendations

To ensure that the mobile application is resilient or immune to VM Escape attacks, it is recommended that the measures described in the good practice report and the security tests present in the full report are followed to ensure authenticity, integrity, privacy, authenticity and confinement of the data.

VM Escape Attacks Diagram

Goal:Gain the root privilege OR |- 1. VMs attack hypervisor | AND | |- 1. Placement | |- 2. Extracting information |- 2. VMs attack the hosts | AND | |- 1. Placement | |- 2. Extracting information

Cross VM Attacks (Sid-Channel attacks)

Side-channel attacks are used to extract cryptographic keys from a victim device or process in a virtualized layer of the cloud ecosystem where a Cross-VM attack exploits the nature of multi-tenancy, which enables that VMs belonging to different customers may co-reside on the same physical machine.

Definition

The side-channel attack takes advantage of low-bandwidth message channels in a system to leak sensitive security information. There is no doubt that this type of attack exists and is real for today's computer systems, including modern smartphones and tablets. Here we highlight the cache-based side-channel attacks that have been used to steal cryptographic information from a single OS. Furthermore, the weak link is in the fact that cryptographic algorithms usually have data-dependent memory access patterns, giving the possibility of being revealed by the observation and statistical analysis of hits / errors from the associated cache. Recent research has shown attackers can build up cross-VM side channels to obtain sensitive information. However, currently these channels are mostly based on shared CPU cache, networks, CPU loads and so on. These attacks are generally categorized into one of three classes:

- · Time-driven side-channel attack;
- · Trace-driven side-channel attacks;
- Access-driven side-channel attacks.

Technical Impact

- · Modify and Read Memory;
- Read Files or Directories;
- · Modify Files or Directories;
- Execute Unauthorized Code or Commands;
- Gain Privileges or Assume Identity;
- Bypass Protection Mechanism;
- Read Application Data;
- Modify Application Data;
- Hide Activities.

Risk Analysis

· High Risk.

Likelihood of Exploit

• Low.

Attacker Powers

- · Steal cryptographic information;
- · Extract cryptographic key;
- · Obtains confidential data or sensitive information.

Recommendations

In order to ensure that the mobile application is resilient or immune to the side-channel attacks, it is recommended that the measures described in the good practice report and the security testing present in the full report are followed.

Cross VM Attacks Diagram

Goal: Gain access over another VM running on the same hypervisor

OR

|- 1. Time-driven side-channel attack | AND

|- 1. Exploit hypervisor vulnerability |- 2. Access another VM |- 3. Extract confidential information, file and documents |- 2. Trace-driven side-channel attack | AND |- 1. Exploit hypervisor vulnerability |- 2. Access another VM |- 3. Extract confidential information, file and documents |- 3. Access-driven side-channel attack | AND |- 1. Exploit hypervisor vulnerability |- 2. Access another VM |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents |- 3. Extract confidential information, file and documents

Malware Injection Attacks

This type of attack occurs whenever a user can install malware on a mobile device. In addition, this type of attack can be carried out remotely or locally.

Definition

Attacks on the cloud and mobile application-level ecosystem can affect the integrity and confidentiality of data and applications through different strategies. E.g., by injecting malware. Malware can be virus, worm, trojan, rootkit and botnet.

Technical Impact

- Execute Unauthorized Code or Commands;
- · Read Application Data.

Risk Analysis

Critical Risk.

Likelihood of Exploit

Medium.

Attacker Powers

- Access and steal users confidential data;
- Obtain root permissions on mobile devices and control the mobile device;
- Directly affect the computational integrity of mobile platforms along with the application.

Recommendations

To ensure that the mobile application is resilient or immune to malicious Malware Injection attacks, it is recommended that the measures described in the good practice report and the security tests present in the full report are followed to ensure authenticity, integrity and authenticity of the data.

Malware Injection Attacks Diagram

```
Goal: Exploiting system's vulnerability and manages authorization

AND
|- 1. Creating a malware
|- 2. Infecting mobile devices
| OR
| |- 1. M2D: Market-borne attacks
| |- 2. A2D: Application-borne attacks
| |- 3. Web-borne attacks
| |- 4. SMS to device attacks
| |- 5. Network to device attack
| | OR
| | |- 1. Device to device
| | |- 2. Cloud to device
| |- 6. USB to device attacks
```

Tampering Attacks

In this type of attack an attacker preforms physical modifications on the hardware where the software is implemented.

Definition

This type of attack occurs whenever an unauthorized user has physical access to the device. When this access is realized, it is possible to loss, leakage, access or unintentionally disclose of the data or applications to unauthorized users, if the mobile devices are misplaced, lost or theft.

Technical Impact

Read and Modify Application Data.

Attacker Powers

- · Sending high malicious traffic stream;
- · Huge messages to targeting mobile devices to make unused or reducing the capability;
- · Access and steal users confidential data.

Recommendations

To ensure that the mobile application is resilient or immune to malicious Tampering attack, it is recommended that the measures described in the good practice report and the security tests present in the full report are followed to ensure authenticity, integrity, privacy and authenticity of the data.

Tampering Attacks Diagram

Goal: To compromise the system or system component

OR

- I- 1. Penetration
- I- 2. Monitoring
- l- 3. Manipulation
- l- 4. Modification
- I- 5. Substitution