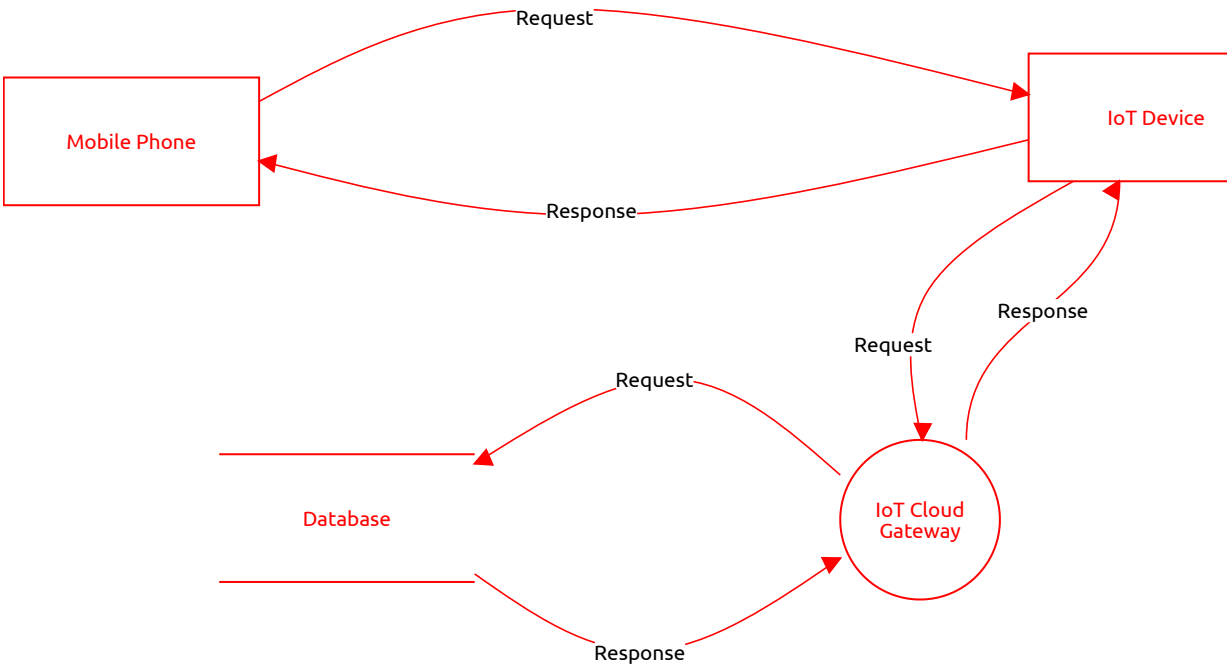
Threat model report for APPLY: Risk modelling

Owner:
Francesco Galassi
Reviewer:
Contributors:

High level system description

simple IoT system with an IoT device that is controlled by a mobile device and connects to a database in the cloud through an IoT cloud Gateway

Risk


Request
Mobile Phone
IoT Device
Response
Request
Response
Request
Database
IoT Cloud
Gateway
Response

Mobile Phone (External Actor)

Description:

Phone controlled

Tampering, Open, High Severity

Description:
Take control of the mobile hardware and/or software with a virus or app to gain control, grant access or alter any behaviour

Mitigation:
encrypt phone / protect it with passwords or activate remotely a factory reset in case of emergency

TDoS

Denial of service, Open, High Severity

Description:
A Telephony Denial of Service (TDoS) attack is an attempt to make a telephone system unavailable to the intended users. (Source cisecurity.org)

Mitigation:
block any connection, have the possibility to restore working previous version of compromised

MDM elevation of privilege vulnerability

Elevation of privilege, Open, Medium Severity

Description:
An elevation of privilege vulnerability exists when Windows Mobile Device Management (MDM) Diagnostics improperly handles junctions. An attacker who successfully exploited this vulnerability could bypass access restrictions to delete files. (source msrc.microsoft.com)

Mitigation:
use a more secure OS / update the system frequently

sensitive data leaked

Information disclosure, Open, Medium Severity

Description:
Sensitive data are not encrypted may be easy to steal

Mitigation:

encrypt sensitive data

Database (Data Store)

Description:

Unathorised access

Information disclosure, Open, Medium Severity

Description:
An attacker could make a query call on the database

Mitigation:
authenticate all queries

avoid restrictions and damage data

Elevation of privilege, Open, Medium Severity

Description:
An attacker gettign access to the database with high privileges could avoid any block and even delete data

Mitigation:
backup regularly and grant right permissions for the right people

IoT Cloud Gateway (Process)

Description:

Accessing DB credentials

Information disclosure, Open, High Severity

Description:
An attacker might access to the DB credentials

Mitigation:
Encrypt the DB credentials and expire/replace the credential regularly

IoT Device (External Actor)

Description:

Simulate connection from mobile phone

Spoofing, Open, High Severity

Description:
Disguising a communication from an unknown source as being from a known, trusted source while coming from an attacker.

Mitigation:
Implement security checks for connections to ensure data exchange only from trusted devices

execution of malicious code

Tampering, Open, Medium Severity

Description:
Attackers can execute malicious code into the iOT device

Mitigation:
sanitise any code, data variable inserted

DoS

Denial of service, Open, High Severity

Description:
DoS attack might prevent getting a conenction to/from this device

Mitigation:
protect against DoS e.g. allowing only specific IPs

Request (Data Flow)

Description:

data captured from connection

Information disclosure, Open, Medium Severity

Description:
attackers might sniff traffic or start a man in the middle attack if connections are not protected

Mitigation:
encrypt connection, use safe protocols

Request (Data Flow)

Description:

data captured from connection

Information disclosure, Open, Medium Severity

Description:
attackers might sniff traffic or start a man in the middle attack if connections are not protected

Mitigation:
encrypt connection, use safe protocols

Response (Data Flow)

Description:

data captured from connection

Information disclosure, Open, Medium Severity

Description:
attackers might sniff traffic or start a man in the middle attack if connections are not protected

Mitigation:
encrypt connection, use safe protocols

Request (Data Flow)

Description:

data captured from connection

Information disclosure, Open, Medium Severity

Description:
attackers might sniff traffic or start a man in the middle attack if connections are not protected

Mitigation:
encrypt connection, use safe protocols

Response (Data Flow)

Description:

data captured from connection

Information disclosure, Open, Medium Severity

Description:
attackers might sniff traffic or start a man in the middle attack if connections are not protected

Mitigation:
encrypt connection, use safe protocols

Response (Data Flow)

Description:

data captured from connection

Information disclosure, Open, Medium Severity

Description:
attackers might sniff traffic or start a man in the middle attack if connections are not protected

Mitigation:
encrypt connection, use safe protocols