This project has received funding from Horizon 2020, European Union's Framework Programme for Research and Innovation, under grant agreement No. 831138

Deliverable D5.1
Threat analysis and security services description

Work Package 5 – IoT and content delivery security

SCENE Project

Grant Agreement No. 831138

Call H2020-EIC-FTI-2018-2020 "Fast Track to Innovation"

Topic EIC-FTI-2018-2020 – Fast Track to Innovation (FTI)

Start date of the project: 1 December 2018

Duration of the project: 24 months

Disclaimer

This document contains material, which is the copyright of certain SCENE contractors, and may not be reproduced or copied without permission. All SECENE consortium partners have agreed to the full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information. The reproduction of this document or of parts of it requires an agreement with the proprietor of that information. The document must be referenced if used in a publication.

The SCENE consortium consists of the following partners.

No.	Name	Short Name	Country
1	VISIONWARE - SISTEMAS DE INFORMAÇÃO, SA	VISIONWARE	Pt
2	JCP-CONNECT SAS	JCP-C	FR
3	ALMAVIVA - THE ITALIAN INNOVATION COMPANY SPA	ALMAVIVA	IT
4	COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES	CEA	fr
5	AZIENDA METROPOLITANA TRASPORTI CATANIA SPA	CAT	It

Document Information

Project short name and number	SCENE (AMD-831138-1)
Work package	WP5
Number	D5.1
Title	Threat analysis and security services description
Version	V1.0
Responsible partner	CEA
Type[1]	R
Dissemination level[2]	PU
Contractual date of delivery	28.02.2019
Last update	28.02.2019

[1] **Types. R:** Document, report (excluding the periodic and final reports); **DEM:** Demonstrator, pilot, prototype, plan designs; **DEC:** Websites, patents filing, press & media actions, videos, etc.; **OTHER:** Software, technical diagram, etc.

[2] **Dissemination levels. PU:** Public, fully open, e.g. web; **CO:** Confidential, restricted under conditions set out in Model Grant Agreement; **CI:** Classified, information as referred to in Commission Decision 2001/844/EC.

Document History

Version	Date	Status	Authors, Reviewers	Description
v0.1	29.01.2019	Draft	BP, CEA	Initial version, definition of a structure and partners responsibilities
v0.2	22.02.2019	Draft	BP, CEA	Data flow diagram presentation, first version of threat analysis, first recommendations, integration of new official SCENE template
v0.3	25.02.2019	Draft	BP, CEA	Update of threat analysis with DREAD notation, description of main security services description
v0.4	26.02.2019	Draft	BP, CEA	Improve the layout of the document, finalize security services description, introduction
v0.5	27.02.2019	Draft	BP, AO, CEA	Review of Introduction, Chapter 3 and 4
v0.6	27.02.2019	Final Draft	BP, CEA	Improve layout and add details for Chapter 2, conclusion
v0.7	27.02.2019	??	??	General review
V0.8	28.02.19	Final Draft	MS, VW	General review
V1.0	28.02.2019	Delivery	MS, VW	Final review

Acronyms and Abbreviations

Acronym/Abbreviation	Description
SCENE	Smart City on the Edge Network Enhancements
IG	Intelligent Gateway
SP	Service Platform
IoT	Internet of Things
QoS	Quality of Service

Contents

List of Figures

List of Tables

1 INTRODUCTION

This report presents a catalogue of threats likely to impact the SCENE platform.

The chosen threat analysis methodology is the STRIDE-per-interaction methodology[3]. This method is based on the data flow analysis. Thus, this report is based on a summarized view of deliverable D2.1 focused on the data flow between each module. Chapter 2 presents this summary in tabular form and then the representative data flow diagram of SCENE platform done regarding these tables.

Chapter 3 is the threat analysis synthesis based on this data flow diagram. This synthesis is classified among the six categories specified by the STRIDE-per-interaction method (**S**poofing, **T**ampering, **R**epudiation, **I**nformation Disclosure, **D**enial of service, **E**levation of privileges). Then, different risks are identified in each category, a note is given using the DREAD[4] notation and the description of either the causes or the countermeasures are presented.

Chapter 4 presents recommendation of different security services with their descriptions to prevent most of the identified threats. Then Chapter 5 concludes the report.

It should be noted that the product threat catalogue reflects the state of the system specification knowledge as defined by SCENE partners via technical meetings and a careful review of D2.1, prior to 28 February 2019.

[3] Shostack, A. (2014). *Threat modeling: Designing for security*. John Wiley & Sons.

[4] Meier, J. D. (2003). *Improving web application security: threats and countermeasures*. Microsoft press.

2 DATA FLOW DIAGRAM REFINEMENT

In order to proceed an efficient threat analysis on SCENE platform, the different modules interactions and data flow need to be refined. This chapter proposes to make a Data Flow diagram which is going to be the main input for the threat analysis.

2.1 General architecture

Figure 2.1 presents the general architecture of the SCENE platform as it has been proposed for the project submission. It presents four main components:

- SCENE Dashboard
- SCENE Service Platform
- SCENE Intelligent Gateway
- Smart City sensors

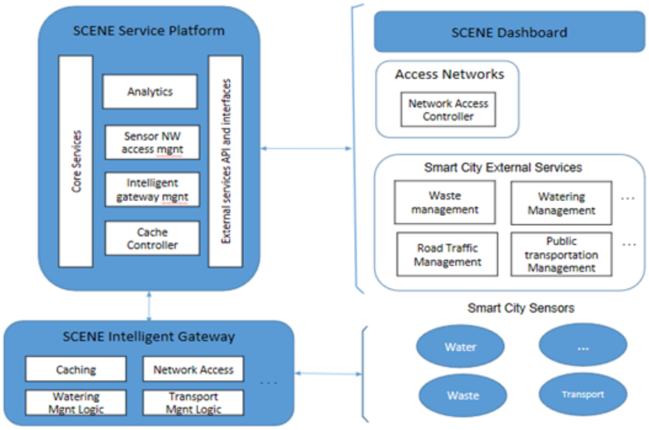


Figure 2.1 SCENE proposal general architecture

This deliverable is directly related to D2.1, which specifies the different requirements and architecture design of the system. Thus, Figure 2.2 comes from this deliverable and presents a first technical high-level architecture.

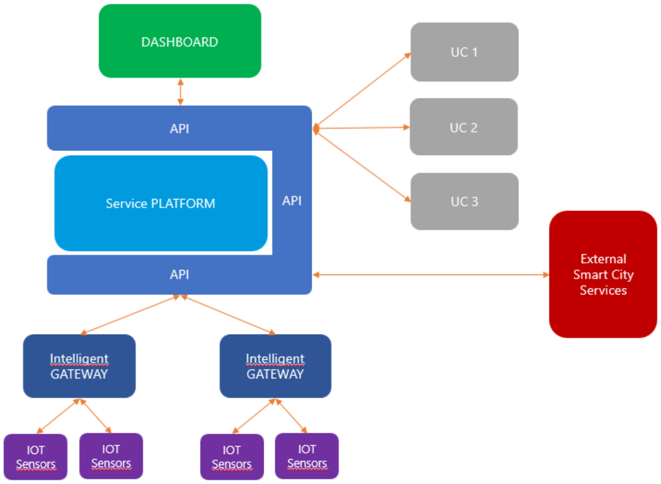


Figure 2.2 SCENE high-level architecture proposed in D2.1

In this high-level architecture, Use Cases and Third-parties are presented as external components of the Service Platform. That is why the next section is adding a fifth component. The user interaction is also added to consider the real interaction with the Dashboard.

2.2 Different modules interaction

2.2.1 Global overview

Table 2.1 presents the different modules interactions.

Interaction (Y/N)	*Service Platform*	*Intelligent Gateway*	*Sensors*	*Dashboard*	*Third parties*	*User*
Service Platform	Y	Y	N	Y	Y	N
Intelligent Gateway	Y	Y	Y	N	N	Y
Sensors	N	Y	Y	N	N	N
Dashboard	Y	N	N	N	Maybe	Y
Third parties	Y	N	N	Maybe	N	Y
User	N	Y	N	Y	Y	N

Table 2.1 Different SCENE modules interactions

Relevant interactions are detailed in the next sections.

2.2.2 Interaction Service Platform ↔ Intelligent Gateway

Service Platform and Intelligent Gateway interactions are detailed in Table 2.2.

Service Platform ↔ Intelligent Gateway	
Brief description	Service Platform and Intelligent Gateway communicate each other by API layer. From IGW to SP, exchanged data is composed of IOT data coming from sensors, requests to send data to an External Service, telemetry data, status, … From SP to IGW, there are flows about configuration data for IGW, configuration data for Sensors, APP to be installed inside IGW,
Communication medium	API

Involved protocol	To be defined	
	Service Platform → Intelligent Gateway	Service Platform ← Intelligent Gateway
Presence of traffic	Y	Y
Capabilities	• Configure gateway • Configure sensors • Upload application	• Upload IoT data • Upload specific data to specific services (ex: Third Parties application) • Upload telemetry data • Upload gateway status

Table 2.2 Service Platform and Intelligent Gateway interactions

2.2.3 Interaction Service Platform ↔ Dashboard

Table 2.3 is describing the different interactions between the Dashboard and the Service Platform.

Service Platform ↔ Dashboard		
Brief description	This is a first indication. More information will come from design tasks. Dashboard is the web UI interface for managing SCENE platform	
Communication medium	API	
Involved protocol	To be defined	
	Service Platform → Dashboard	Service Platform ← Dashboard
Presence of traffic	Y	Y
Capabilities	• Send analytics • Raise specific alerts	• Configure sensors • Configure platform • Configure gateway • Query analytics

Table 2.3 Service Platform and Dashboard interactions

2.2.4 Interaction Service Platform ↔ Third Parties

Table 2.4 focused on the particular interactions between Service Platform and Third Parties. These interactions will be particularly analyzed in order to limit threats from uncontrolled areas.

Service Platform ↔ Third Parties		
Brief description	Third Parties interact with SCENE platform for sending configuration data/commands to be dispatched to their sensors, APPs to be installed on IGW, configuration data/commands for their IGW-installed-APPs. Service Platform may forward IOT data from specific sensors to particular External Parties	
Communication medium	API	
Involved protocol	To be defined	
	Service Platform → Third Parties	Service Platform ← Third Parties
Presence of traffic	Y	Y
Capabilities	• Push specific data to specific application	• Install application on the gateway • Configure/Command gateway • Configure/Command specific sensors

Table 2.4 Service Platform and Third Parties interactions

2.2.5 Interaction Intelligent Gateway ↔ Smart City Sensors

Table 2.5 shows the state of our knowledge on the interactions between Intelligent Gateway and Smart City Sensors.

Intelligent Gateway ↔ Smart City Sensors		
Brief description	Intelligent Gateway and Smart City Sensors	
Communication medium	• BLE: Service bluez for controlling BLE • WIFI: authsae package for securing the mesh network • Others to be defined	
Involved protocol	To be defined	
	Intelligent Gateway → Smart City Sensors	Intelligent Gateway ← Smart City Sensors
Presence of traffic	Y	Y
Capabilities	• Request data collection • Manage sensors	• Upload IoT data

Table 2.5 Intelligent Gateway and Smart City Sensors interactions

2.3 Data Flow Diagram

In Figure 2.3, all the previous tables are summarized to prepare the Data Flow diagram corresponding to the already known modules interactions.

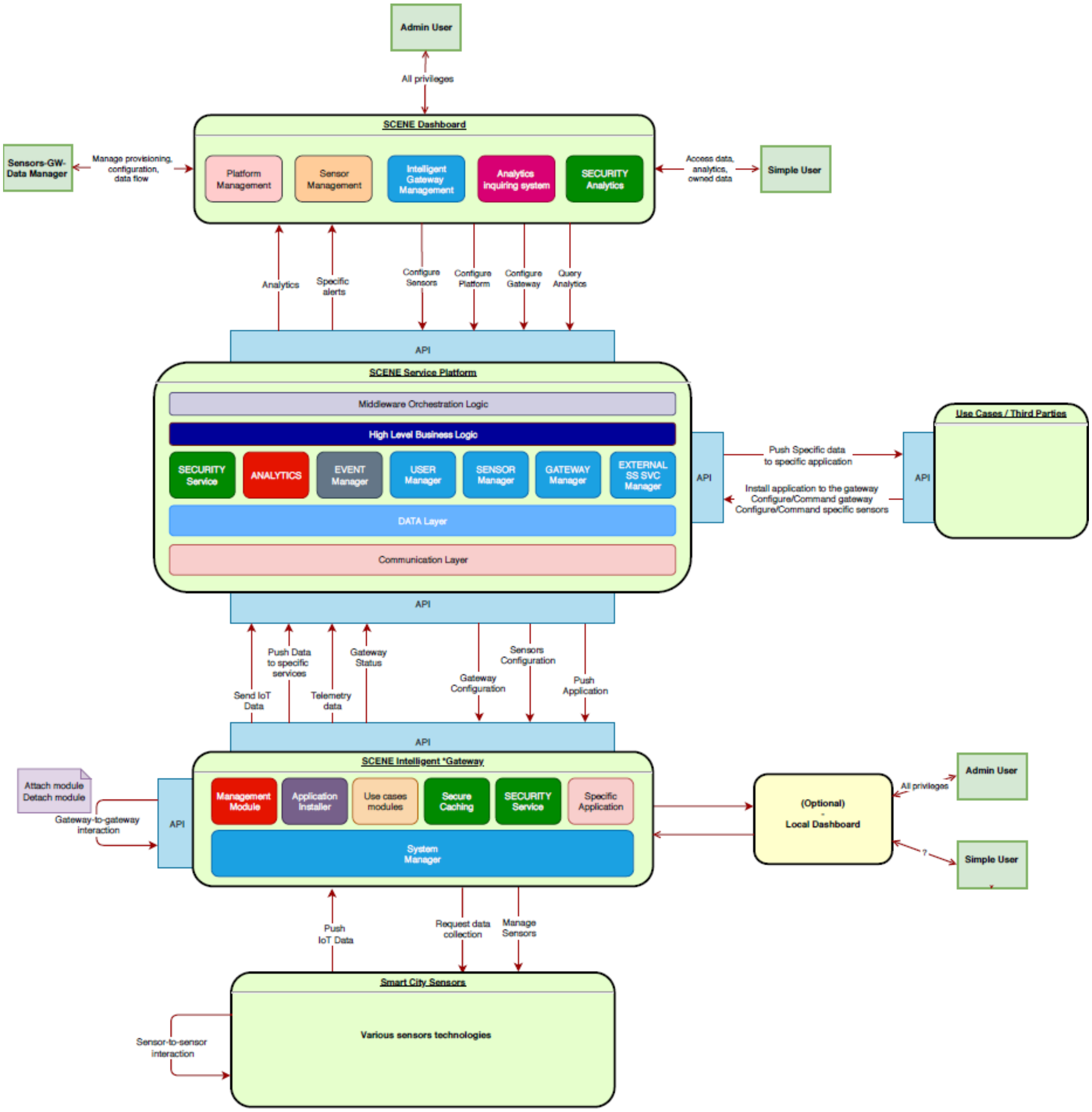


Figure 2.3 SCENE Data Flow Diagram

This Data Flow Diagram will be used in the next section to proceed the threat analysis.

3 THREAT ANALYSIS

3.1 Introduction to STRIDE-per interaction method

STRIDE / DREAD[5] is an approach for threat analysis, made by Microsoft and dedicated to ICT (Information and Communications Technology) for analysing the security of an application.

STRIDE-per interaction method is a structured way to classify risks sources into six categories:

- ***S****poofing*: The attacker poses as someone else or something else.
- ***T****ampering*: The attacker modifies data transmitted between a legitimate user and the application.
- ***R****epudiation*: The attacker may deny having done an action while it was effectively done.
- ***I****nformation Disclosure*: The attacker may become aware of sensitive data.
- ***D****enial of Service*: The attacker may prohibit the use of all or part of the service.
- ***E****levation of Privilege*: The attacker may obtain unjustified rights.

For each categories of STRIDE-per interaction method, several risks can be identified. These risks are evaluated using the DREAD methodology. DREAD proposes five different evaluation criteria:

- ***D****amageability*: The nuisance capacity of a threat reflects the damage that the assessed threat is likely to cause (0: no damage; 10: extremely harmful).
- ***R****eproducibility*: The reproducibility of a threat reflects the ease with which an attack can be reproduced. The attack may only be possible when an extraordinary combination of circumstances occurs (0) or can be launched in a very wide variety of contexts (10).
- ***E****xploitability*: The exploitability of a threat reflects its difficulty in implementation. To ensure consistency with how the other DREAD criteria are assessed, exploitability rated at zero is considered to reflect a very difficult attack to implement while exploitability rated at 10 reflects a very simple attack to implement.
- ***A****ffected users*: The number of affected users is noted as follows: zero indicates that no user is affected, while 10 indicates that the entire system is affected.
- ***D****iscoverability*: Discoverability affects the overall criticality of a threat in that an attack whose implementation is very easy to discover (rated 10) is much more critical than an attack whose implementation may remain unknown (rated 0).

[5] Microsoft Corporation. 2003. “Threat Modeling.” http://msdn.microsoft.com/en-us/library/ff648644.aspx.

3.2 Threat analysis

Table 3.1 presents the threat analysis of SCENE platform following the STRIDE-per-interaction method presented in 3.1.

Risk category	Risk	DREAD Notation	Causes	Countermeasures	
Spoofing	Identity spoofing from an IG to another IG	7/3/2/7/2	Credentials lost or stolen	Credentials protection (force authentication by user AND secured storage)	Authentication based on cryptographic access control
			Credential disclosure using cryptanalysis (really critical because reproducible)		
			Session key disclosure using cryptanalysis	Session key refreshing	
			Implantation of a cryptographic material in the device (ex: root certificate) which make possible the false authentication of non-authorized equipment	Secured storage of certificates	
	Identity spoofing from an IG to the service platform	8/3/2/8/2	Credentials lost or stolen	Credentials protection (force authentication by user AND secured storage)	Authentication based on cryptographic access control
			Credential disclosure using cryptanalysis (really critical because reproducible)		
			Session key disclosure using cryptanalysis	Session key refreshing	
	Identity spoofing from the service platform to an IG	9/3/2/9/2	Credentials lost or stolen	Credentials protection (force authentication by user AND secured storage)	Authentication based on cryptographic access control
			Credential disclosure using cryptanalysis		

			Session key disclosure using cryptanalysis	Session key refreshing	
	Identity spoofing from a sensor to the IG	5/3/2/5/2	Credentials lost or stolen		Authentication based on cryptographic access control
			Credential disclosure using cryptanalysis		
			Session key disclosure using cryptanalysis	Session key refreshing	
	Identity spoofing from the IG to a sensor	6/3/2/6/2	Credentials lost or stolen		Authentication based on cryptographic access control
			Credential disclosure using cryptanalysis		
			Session key disclosure using cryptanalysis	Session key refreshing	
	Relay attack	10/3/2/10/2	Unsecured transfer/exchange of authentication information	Secure key exchange protocols	
	Equipment lost or stolen containing its valid credentials	7/7/10/1/7	Human negligence / malicious activity	Protect equipment credentials (unlock only by user authentication AND secure storage) Revocation of the equipment itself and/or its credentials	
	Equipment lost or stolen containing valid credentials of other equipments	7/7/10/2/7	Key shared between equipment (symetric cryptography)	Protect equipment credentials (unlock only by user authentication AND secure storage) Asymetric cryptography	

	Equipment compromised	8/5/7/1/5	Credentials lost or stolen Poor material and software security	Equipment revocation
	Compromise, loss or theft of super user credentials	10/3/3/10/3		Secure credential management (physical protection, access policy, logs)
	Replay attack	7/9/5/5/5	Unsecured transfer/exchange of authentication information (e.g. security breaches in the key exchange protocol: credential not/lowly protected, identity misbinding, etc.)	Transactions/exchanges updated in security protocols (update by sequence number, by nonces or by timestamps)
Tampering	Blind alteration of the exchange data	7/5/3/5/3	Hacking of communications (e. g. MitM) and/or radio equipment (data) Fuzzing	Secure cryptographic communication
	Malicious alteration of the exchange data	10/8/7/10/3	Hacking of communications (e. g. MitM) and/or radio equipment (data) Revealing the key of the session authenticated by cryptanalysis	Secure cryptographic communication
Repudiation	Responsible of malicious action not identified (ethical/legal problems)	8/8/8/8/3	Lack of electronic signature	Authenticate and Identify triplet (User, equipment, action) Logs
Information Disclosure	Disclosure of the equipment presence	1/9/1/9/9	Listening of radio communication	Stealth of radio communication
	Disclosure of the equipment localisation	5/7/5/5/5	Listening of radio communication + Triangulation	Stealth of radio communication
	Identification of an equipment	7/5/5/5/3	Recognition of identifying elements although the communication is encrypted Breakage of cryptographic protection	Privacy

	Tracing the successive locations of the same equipment (even under pseudonym)	7/3/7/3/1	Association of different pseudonyms as belonging to the same equipment	Unlinkability system
	Disclosure of the configuration of the communicating application and/or existence/description of services	7/3/7/3/1	Hacking of communications and/or radio equipment (data)	Application element fully encrypted
	Partial disclosure of the content of the information exchanged	5/3/5/3/1	Encrypted flow analysis	Flow obfuscation
	Full disclosure of the content of the information exchanged	10/5/7/7/1	Cryptanalysis on encrypted messages	Strong encryption method
			Obtaining the session key as a result of the disclosure of authentication credentials	
Denial of Service	Unable to establish communication	9/3/3/10/3	Radio interference	Reduction of the range of radio communications
	Interruption of an established communication	7/3/5/7/5	Radio link saturation	Augmention of radio link capacity
		7/3/7/7/5	Excessive use of communication equipment	Timeout for specific connection, diminution of QoS for certain users
Elevation of privilege	Unauthorized use of equipment / equipment subsystems	10/3/9/10/1	illegal acquisition of access rights Malicious Third Parties	Authentication Strong separation of capabilities

Table 3.1 STRIDE-per interaction of SCENE project

The threat analysis has raised many threats for the complex SCENE platform. These different threats will have to be prevented using different security services.

4 SECURITY SERVICES DESCRIPTION

This Chapter aims to define the different security services required to prevent attacks raised by the threat analysis (Table 3.1).

4.1 Security by design

The first security services that SCENE platform could provide are linked to a careful development.

4.1.1 Coding

SCENE project should follow the OWASP Secure Coding Practices[6] to provide a first security level based on the “security by design” principle.

4.1.2 Protocol security

It will be ensured that the proposed security system natively meets the requirements of "security by design" especially in terms of protocols integration; the proposed protocols should not be vulnerable to attacks as listed in Table 3.1 (e.g. denial of service, man in the middle...).

4.1.3 Content storage

Intelligent Gateway and Service Platform could store sensitive data based on sensors or analytics of sensors data. This data must be cared using data security mechanisms to prevent:

- Clear access: data should be encrypted using strong encryption mechanism
- Data tampering: a signature mechanism should be proposed for sensitive data
- Unintended permissions: a data access policy should be define with a strong user authentication policy (recommended in 4.2.1.1)

4.1.4 Third-party interaction

Particular attention should be paid to the implementation of platform accessibility to third parties. Indeed, the provision of application upload functionalities must offer a segmentation between the core of the platform and these third-party applications to prevent any eventual privilege escalation.

A mechanism for analysing these applications or at least a verification procedure should be implemented to prevent these risks.

4.1.5 Stealth (optional)

The stealth service prevents the disclosure of the presence and/or location of equipment. Different variations of the stealth service are to be considered depending on whether the equipment under consideration is out of communication, searching for another equipment to communicate with or in communication. This service is provided at the radio level and could be optional for SCENE platform or used for specific sensors.

[6] OWASP. 2017. “OWASP Secure Coding Practices - Quick Reference Guide” https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide

4.2 API security & general security architecture

The major high-level communication of the platform are using API. So particular attention must be paid to the API security.

4.2.1 API security services

API communication will have to provide the following security services in order to protect SCENE project against as many threats as possible:

- Source authentication
- Data integrity
- Data confidentiality
- Non-repudiation
- Perfect forward secrecy

4.2.1.1 Source authentication

This service ensures that a message whose source identifier has been modified or crafts by an attacker which try to spoof a legitimate address will be rejected by its destination.

When this service is offered, messages that are not part of an authentication procedure or an initial communication establishment are exchanged in an authenticated session. Such a session is defined as having started with an authentication procedure and being protected against spoofing and alteration by means of an access control mechanism. This mechanism provides that each message sent by either participant must be transmitted together with a fingerprint. The fingerprint is calculated using a session key established during the authentication phase from the message itself, including its source and destination identifiers. Both communication participants must at least know the session key - it can also be known by a third party server for practical reasons (the server intervenes during the authentication procedure).

4.2.1.2 Data integrity

The integrity of the data exchanged is provided as part of the access control service described in the previous point (4.2.1.1). The data exchanged in the context of an authenticated session is therefore protected against alteration.

4.2.1.3 Data confidentiality

The confidentiality service ensures that the content of a message will be made inaccessible to a potential interceptor, being transmitted in encrypted form from the source to the destination.

4.2.1.4 Non-repudiation

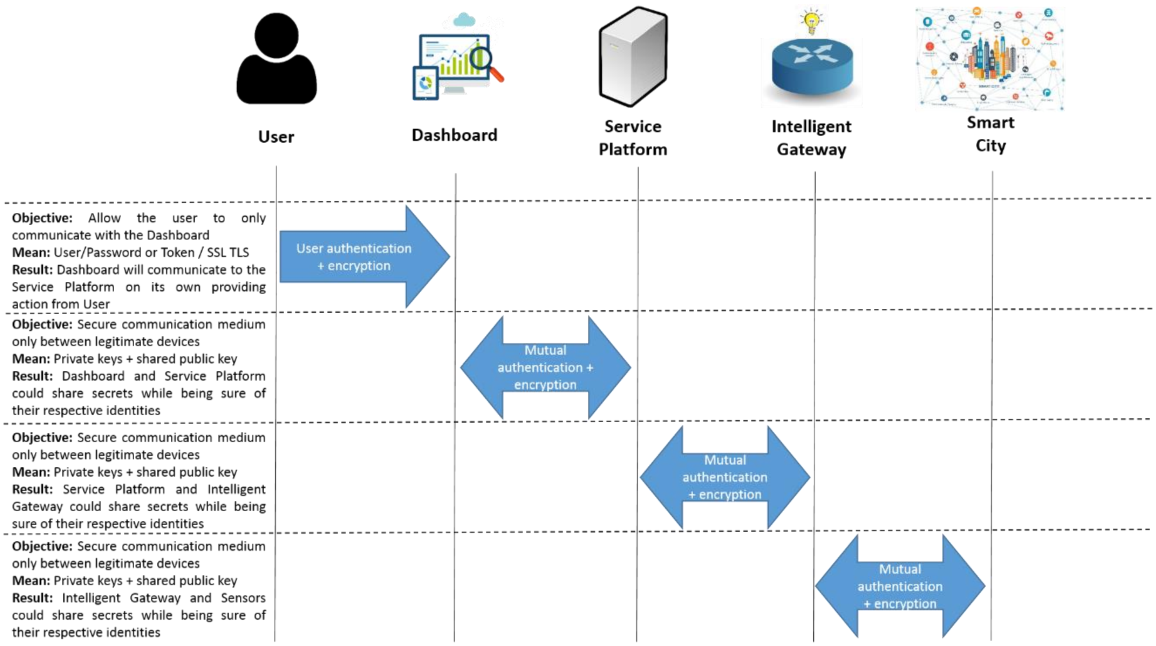
The non-repudiation service implies the responsibility of a user regarding an action. It proves from whom the malicious action has been done. It could be provided either using digital signature or an authenticated role-based management with a logging system.

4.2.1.5 Perfect forward secrecy

This service concerns a session key established as part of a key establishment protocol. This protocol is offering the perfect forward secrecy service when the session key remains secret even if the long-term secrets of the participants in the key establishment are later disclosed (that means that the attacker could have been able to listen to all the messages exchanged under this protocol).

4.2.2 General communication security architecture

Figure 4.1 presents the general communication security pattern that is recommended for the SCENE project.


User
Dashboard
Service Platform
Intelligent Gateway
Smart City
User authentication + encryption
Mutual authentication + encryption
Mutual authentication + encryption
Mutual authentication + encryption

Objective: Allow the user to only communicate with the Dashboard
Mean: User/Password or Token / SSL TLS
Result: Dashboard will communicate to the Service Platform on its own providing action from User

Objective: Secure communication medium only between legitimate devices
Mean: Private keys + shared public key
Result: Dashboard and Service Platform could share secrets while being sure of their respective identities

Objective: Secure communication medium only between legitimate devices
Mean: Private keys + shared public key
Result: Service Platform and Intelligent Gateway could share secrets while being sure of their respective identities

Objective: Secure communication medium only between legitimate devices
Mean: Private keys + shared public key
Result: Intelligent Gateway and Sensors could share secrets while being sure of their respective identities

Figure 4.1 General security architecture

A refine version for particular elements is proposed in the following sections in order to specify the key components.

4.2.2.1 User ↔ Dashboard specific security services

The communication between User and Dashboard have to provide the following security services.

4.2.2.1.1 Refresh session keys

This service allows you to regularly renew the current session keys, in order to protect them against the risk of cryptanalysis.

4.2.2.1.2 Credentials revocation

This service ensures that credentials that have become invalid can no longer be used to establish a secure session.

4.2.2.2 Recommended authentication method for other modules

The following scheme is recommended for other communications: two devices establishing secure communication with each other must implement a mutual authentication procedure in which each device proves to its partner its identity. It is indeed an authentication of each device, and not of the users of the communicating devices. On the other hand, it is recommended that if an equipment is operated, this equipment cannot be able to carry out such an authentication procedure if its user has not previously authenticated itself to it.

4.3 Smart City security

The security of the smart city is special because of the chosen architecture for the SCENE platform. Indeed, in this architecture, sensors will not always be within an Intelligent Gateway range. Moreover, even if the range is ensured, for the moment there is no guarantee that the Intelligent Gateway, which is going to be within range next time, is aware of previous Intelligent Gateway knowledge on the monitored network.

Therefore, Smart City security will have to handle these different challenges to be acceptable and to detect outside attacker to enter the Smart City sensors network. The already suggested solution are:

- Signature-based detection: By relying on attack signatures, characterized by the messages they imply, this service should make possible to recognize an attack in action.
- Anomaly-based detection: According to a model of the normal traffic/data structure behaviour, anomaly-based detection will allow to detect unknown attack. Then, it could be assumed that uncertainties about the data presence will be compensated.

Particular attention should have to be paid to the accessible data for the both anomaly-based and signature-based detection module.

4.4 Gateway security

The Gateway security will be provided from both signature-based detection and anomaly-based detection.

The service description could not already be defined because the scope of Intelligent Gateway and sensor interaction key indicators is not available. It will depend on how they really interact. This definition is required to perform the gateway security service.

5 CONCLUSION

After, a review of the different modules interactions, this deliverable offers the presentation of the SCENE platform Data Flow diagram. Based on this Data Flow diagram, the threat analysis of the platform has been done using the STRIDE-per-interaction method. These threats relate to the availability, integrity and confidentiality of communication channels. In order to address these threats, security services description have been then proposed.

This study and the already highlighted security services will be then used to prepare the deliverable D5.2, “Specification of SCENE security framework”. This deliverable will have to address the security services as well provided by the APIs as the intelligent gateway self-protection mechanisms as smart city protection.

Should the need arise, this document may be reviewed in order to reflect changes in the design or the architecture of the system that have impact on the threat model.