Security Assessment of Modern Data Aggregation Platforms in the Internet of Things

Hunor Sándor*, Béla Genge**, Zoltán Gál***

*Technical University of Cluj-Napoca, Department of Computer Science
**Petru Maior University of Tg. Mureş, Department of Informatics
***University of Debrecen, Center for Informatics Services
e-mail: hunor.sandor@cs.utcluj.ro, bela.genge@ing.upm.ro, zgal@unideb.hu

Abstract—With the popularity of the Internet of Things on the rise, sensor networks have become essential parts of traditional Information and Communication Technology (ICT) infrastructures in a wide variety of applications. However, their increasing complexity, inter-connectivity, and pervasive implementation, exposes these infrastructures to a large variety of security threats. As a result, practical security analysis needs to be performed to evidentiate the possible vulnerable points in IoT infrastructures. In this work we consider a typical architecture of a data aggregation platform with publish-subscribe support composed of interconnected sensor and ICT infrastructures. We present a comprehensive threat analysis by considering the availability, integrity, and confidentiality security objectives. We describe the experimental results of a case study performed on a real, laboratory-scale implementation of an IoT-based application. Finally, we demonstrate that modern IoT-based software are susceptible to cyber attacks that use traditional attack vectors and recently reported vulnerabilities, e.g., Heartbleed and Shellshock.

Keywords—Sensor Data Aggregation, Heterogeneous Infrastructures, Threat Analysis, Attack Tree.

1. Introduction

Internet of Things (IoT) is one of the most discussed subject in modern Computer Science. It reshapes the way that we perceive the traditional Internet, its scale and pervasive nature. The IoT paves the way towards the implementation of complex cyber-physical systems, and it provides direct applications to improve the quality of life. In this respect, we find different implementations starting from smart houses, to smart cities [3][11], and health care [17], e.g., smart hospitals. IoT is present in heterogeneous form in all these applications, making a bridge between “the things”, e.g., sensors and actuators, and the users.

One of the key emerging challenges in this new field of science is the magnitude of data that is actually generated by large-scale installations. In fact, the coupling of traditional Information and Communication Technologies (ICT) hardware and software with various sensors and sensor networks may lead to unprecedented network topology sizes. Moreover, with each new extension of this pervasive infrastructure a significant amount of data may be generated. As a result, ICT hardware and software needs to be properly designed and configured to handle a huge amount of data. This needs to be processed, stored, and finally retrieved.

Subsequently, we believe that a key task within

this context is the management of data life-cycle which must measure precisely the "time of birth and death" of data with various granularity. On top of the aforementioned issues, IoT enabling technologies need to account for security properties associated to data crossing different organizational boundaries.

One of the most frequently undertaken approach aimed at addressing these challenges is the adoption of *data aggregation* hardware and software. Data aggregation can be performed in two different ways: aggregation without, and with loss of information. In the former case the data is only unified and arranged, while in the latter case additional operations are performed on the data, e.g., statistical analysis, to "concentrate" it. The result in both cases is an ordered collection of information, which can be applied in further tasks, e.g., surveys or decision making. In particular cases the information freshness is a critical factor; therefore, a basic requirement of IoT platforms is that the aggregated data needs to reach end users in near real-time. To ensure this property the *publish-subscribe* methodology is seen as a promising solution.

The complexity of data aggregator platforms with publish-subscribe support (hereinafter called DA-PS platform) exposes these infrastructures to a large variety of security threats. As a result, the protection of the system is indispensable. Essentially, the most significant security objectives that a specific DA-PS platform needs to achieve are: availability, integrity, and confidentiality (AIC).

This work analyzes the significance and applicability of AIC in the context of data aggregation platforms. Unlike traditional approaches originating mainly from the field of Wireless Sensor Networks (WSN) [13], the study presented in this work progresses beyond the limitations of WSN by assuming a larger, and interconnected system architecture. Here, classic WSN nodes forward data to industry-grade data aggregation hardware, which are able to gather data through different communication media/protocols and to forward data to publish-subscribe nodes. The main novelty of this work is that it provides intrinsic details and findings on a real-world case study encompassing industrial data aggregation and publish-subscribe hardware/software as well as ZigBee WSN nodes.

The remaining of this paper is organized as follows. Section 2 provides a brief overview of related work. Then, Section 3 presents the general DA-PS platform architecture, categorizes and describe the threats related to the platform, after which section 4 presents a case study of a real DA-PS platform, and finally, in section 5, the conclusion is formulated.

2. Related Work

A wide range of studies discuss the data aggregation inside the WSNs. A large variety of data aggregation methods have been proposed with the requirements to assure the data integrity and/or confidentiality [13][14][15][19].

On the other hand, only few works discuss the possibility of interconnection of WSNs with other ICT infrastructures. The paper [20] proposes an IoT gateway to make the bridge between WSNs and traditional communication networks. In the [4] the performance of a lightweight publish-subscribe based WSN integration framework is analyzed for smart grid communication. The work [7] presents an experimentation platform for smart grids using publish-subscribe service for the information delivery. [2] discusses the WSN in the context of critical infrastructures, e.g., SCADA systems, and provides a security analysis on several WSN standards. Furthermore, in several studies [1][8][9] the WSN data to cloud concept is presented, which essentially consists of aggregating the data, produced by different

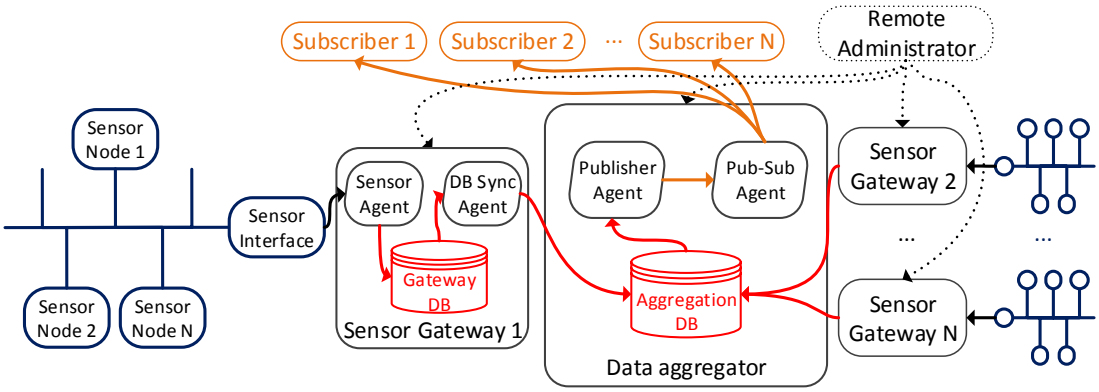

Fig. 1. General DA-PS platform architecture

WSNs, into the cloud with the goal to apply further operations on it.

Conversely, the study at hand provides intrinsic details and analysis of a complex scenario, following the security aspect of the data aggregation from the sensor nodes to the end users.

3. System Architecture and Threat Analysis

In this section we present the typical architecture of a DA-PS platform, and we provide a systematic approach to analyze its main security properties.

3.1. System Architecture

Fig. 1 illustrates the general architecture of a DA-PS platform. The platform is structured according to a two-layer architecture: the sensor layer, and the aggregation layer. The former is composed of sensors interconnected through a local network, e.g., industrial buses or wireless mesh networks, and the latter is a complex ICT infrastructure. The sensor layer is composed of several sensor networks. Each of these embodies several interconnected Sensor Nodes (SN), and a single Sensor Interface (SI). On the aggregation layer we find a centered Data Aggregator to which the Sensor Gateways (SG) are directly connected. The interconnection between the two layers is realized using one-to-one connections between the SIs and SGs. The Subscribers (SB) are the clients which connect to the DA-PS platform through the centralized DA.

Irrespective of the SN that generated it, data is transmitted to the SI. From here, it is forwarded to the SG, where it is temporarily stored for further processing. In the next step the data is centralized at DA. Finally, using a publish-subscribe service the data is delivered to the SBs.

In this context data aggregation is performed on two levels: (i) on the first level the data from the SNs is aggregated in a pre-configured SG; and (ii) on the second level the data from the SGs is aggregated to the centralized DA.

The data handling inside the SGs and the DA is performed by software agents: (i) the Sensor Agent collects the sensor data streams from the SI and stores them in the SG database; (ii) the DB Synchronizer Agent polls the SG database and synchronizes the sensor data to the DA database; (iii) the Publisher Agent polls the DA database and publishes every new sensor data to the Publish-Subscribe Agent; and (iv) the Publish-Subscribe Agent receives the published data and forwards it

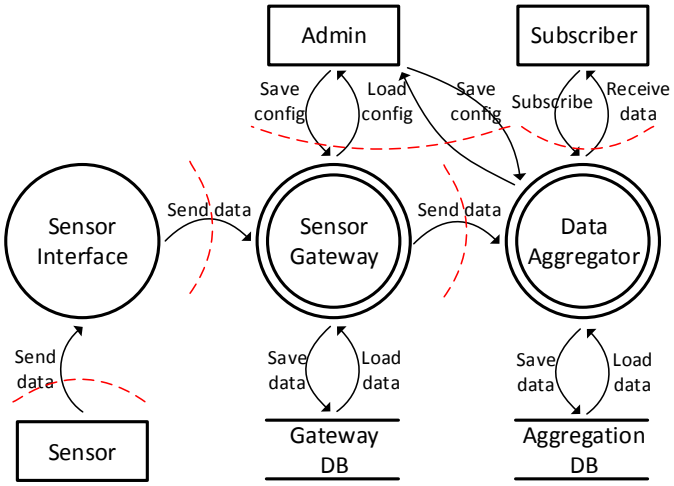

Fig. 2. Data flow diagram

to the subscribed clients.

3.2. Threat Analysis

Following traditional threat analysis techniques as a first step we identify the main assets that need to be protected. In this particular scenario the most significant asset is the aggregated data. Therefore, we mainly study the DA-PS architecture from the perspective of data flows. Fig. 2 illustrates the data flows of the previously presented DA-PS platform. The rectangles represent the external entities; the rectangles without side borders indicate the data stores; the circles are processes, and the double circles are collections of processes that handle the data; finally, the arrows represent the data flows, while the red dashed lines the privilege boundaries.

In the next step, in order to determine the threats, we adopted the STRIDE approach [10] because it provides a general categorization for threats. According to STRIDE the possible threats in a DA-PS are: spoofing, tampering, repudiation, information disclosure, denial of service (DoS), and elevation of privileges. In this work we extend this list with: unauthorized code execution, physical access, and Operating System (OS) related threat categories. These denote a group of threats whose effects can be disassembled to STRIDE groups, but these gain a new significance in a unified form.

The adoption of traditional ICT hardware and software in the architecture of modern IoT enables the execution of well-known cyber attacks against a new kind of cyber-physical system. Therefore, it should be noted that a considerable amount of threats discussed in the remainder of this paper are not necessarily restricted to IoT platforms. Instead, these are generic cyber-security threats, but due to the complexity of IoT and to its interconnection with the physical dimension, cyber attacks may have severe impact on the normal functioning of IoT systems.

TABLE 1 tabulates the possible threats, their possible target points, and feasible effects on availability (A), integrity (I), and confidentiality (C) in a DA-PS platform.

3.2.1. Spoofing

Spoofing allows users to masquerade and to impersonate other users in order to gain access to possibly critical resources. Results of spoofing attacks may affect the confidentiality, integrity, but also the availability properties of certain assets.

In case of sensor networks spoofing can be applied for node replication or for malicious node insertion. It could result in the disclosure of the forwarded information and may enable the possibility for false data injection. Furthermore, a malicious node can cause considerable transmission delay and packet losses by performing selective routing.

Spoofing is a common threat also in ICT infrastructures and may affect the SGs and the DA. A general manifestation of it may be the authentication

TABLE 1
Threats, targets and effects in a DA-PS platform

Threats \ Targeting points	SN and SI	SN to SN	SI to SG	SG	SG to DA	DA	DA to SB	SB
Spoofing	A, I, C	-	-	A, I, C	-	A, I, C	-	-
Tampering	I	I	I	I	I	I	I	-
Repudiation	-	-	-	I, C	-	I, C	-	-
Information disclosure	C	C	C	C	C	C	C	C
Denial of service	A, I	A, I	-	A, I	A	A	A	A
Elevation of privileges	-	-	-	I, C	-	I, C	-	-
Unauthorized code execution	-	-	-	C, I	-	C, I	-	C
Physical access	A, I, C	-	-	A, I, C	-	-	-	C
OS related threats	-	-	-	A, I, C	-	A, I, C	-	C

of malicious entities using credentials acquired as the result of an information disclosure, e.g., stealing passwords. It is a common situation when the default authentication credentials are not changed or weak passwords are used. These are sensible to brute-force attacks, but the leakage of the credentials can also occur as result of phishing, social engineering or other data snooping attacks.

The single interface dedicated for the external user access in the DA-PS platform is the publish-subscribe interface, on which the user authentication is indispensable to control the access to confidential data. Nevertheless, external access to the other components of the platform may not be totally prohibited, because the possibility for remote administration and maintenance is a basic requirement for all of the modern ICT systems. The unauthorized access to the remote administration interfaces is a critical threat, because it can be the enabler of further attacks, e.g., by inserting backdoors or redirections.

To protect the system against spoofing, various methodologies may be adopted. For example, cryptographic protocols can be used to protect communications and to authenticate different nodes. However, special care needs to be placed on the energy and hardware limitations of SN, which may pose significant challenges in the implementation of these advanced features.

3.2.2. Tampering and Information Disclosure

The possibility to intercept or to tamper the stored/transmitted data, as well as the injection of specially forged data packets are considerable threats. Furthermore, the large variety of known buffer overflow bugs in commonly used software libraries may make it possible for the information from the memory to be directly snooped. In addition, local communication on short range data buses, e.g., RS232, SPI or I2C, inside or between the components is generally unprotected and therefore subject to interception or altering. In this context it may be specific to SN to SI and SI to SG data lines.

A significant attack dedicated for information disclosure and tampering is the well-known man-in-the-middle (MITM) attack where a malicious third party, by inserting itself into the communication data line, may snoop, modify, or inject false data packets. Consequently, it may cause information disclosure, which violates the confidentiality, or it is able to corrupt or selectively forward the data

packets, which affects the data flow integrity. On the other hand, replay attacks can tamper the communication by inserting outdated data in the system.

The fact that both of the aforementioned attacks are feasible on all the communication channels of a DA-PS platform shows their high degree of exposure. A well known protection technique against the tampering and information disclosure is the use of different encryption schemes on the targeted data. In addition, the advanced identity validation in both communication endpoint is a basic requirement, otherwise through an MITM attack the attacker can gain access to the encrypted data. Fortunately, most modern devices provide support for modern cryptographic operations. In this respect for the traditional ICT-like components of the IoT platform we mention the Transport Layer Security (TLS), which is an established enabler of secure point-to-point communication channels, and it can be effectively applied on the SG-DA and DA-SB data lines of the DA-PS platform. Unfortunately, due to the limited resources of the IoT devices the public-key cryptography is less applicable for the sensor network components of the architecture at the hand. Instead, the symmetric-key cryptography, e.g., AES encryption, is a widely used solution. In addition, for this, advanced key distribution mechanisms and/or policies are required to assure the secure delivery of the symmetric keys to the embedded IoT devices.

It has to be noted that many security threats were reported regarding to the different implementations of TLS, e.g., the OpenSSL Project. For example, the *Heartbleed* bug [5] enables for the remote users to read the memory of a server, which by itself is a considerable threat affecting the confidentiality, but the information acquired this way, e.g., passwords, may drive to other threats, e.g., spoofing, repudiation or elevation of privileges. Another example of TLS vulnerability is the *Poodle* exploit [12], which profits from the fallback to the SSLv3 protocol to initiate a MITM attack. In this respect, the selection and maintenance of the security tools employed in the system is a key factor in the overall system security.

Furthermore, the usage of the Secure Shell (SSH) is a best-practice for the remote administration, but that may infer new vulnerability points to the system. For example, SSH uses the Diffie-Hellman key exchange algorithm for securing the communication, which is vulnerable to MITM attacks [6]. The application of the MITM attack on remote administration channels is a particular case, because it can provide full access to the system for an attacker, e.g., security, OS or networking configurations.

3.2.3. Repudiation

Repudiation is a malicious action with the goal to hide or change the authoring information of other prohibited operations. It also can be extended to perform data manipulation using a copied identity-assurance token. This, in combination with other threats, e.g., spoofing or tampering, can be a considerable threat in case of SGs and the DA, because it may drive to undetectable intrusions, data or configuration modifications and information retrievals.

The effects of the repudiation can be mitigated by implementing adequate logging features inside the software components and recording the initiator, the time and the summary of the data manipulations. Similarly, the auditing is an approved practice against the repudiation threat.

3.2.4. Denial of Service

Denial of Service (DoS) can appear in two forms in a DA-PS platform: (i) targeting the data exchange

between the components, e.g., consuming the bandwidth or interrupting the connection; or (ii) consuming the resources of the services in the system components, e.g., connection slots of the publish-subscribe broker or the DA database. This makes the targeted component temporary or persistently unavailable, thus violating its availability. It should be noted that even if a DoS attack is not able to affect data content, it affects the integrity of the data flows by causing packet losses.

The solutions against the DoS could be widely various depending on the type and the targeted resource of the attack. For instance, in case of the ICT components of the system the definition of a rule set for the communication flows, e.g., firewall rules or traffic shapers, and blocking the flows that do not respect these, could be a direction to mitigate the effects of certain types of DoS attacks. On the other hand, the server-like components of the platform can be run in more clusters, which may increase the resistance of the system against the DoS attacks that target the system resources. Furthermore, on the sensor layer, the usage of custom traffic related rules and filters, e.g., forwarding filters, may be a solution to control the effects of the DoS attacks. In addition, for WSNs the implementation of the automatic switching between the parallel channels of the physical layer in case of channel overload can help to avoid the communication degradation caused by a DoS attack in several cases.

3.2.5. Elevation of Privileges

In a DA-PS platform the data flows tend to be on predefined paths and the software agents are responsible for the data moving. In case of poorly configured access rights, there is an increased risk towards the insertion of unauthorized data flows. For example, in a DA-PS platform, the access rights to the databases have to be limited, otherwise a malicious agent can snoop or tamper the stored data. Thereby, the Sensor Agent may only write and the Publisher Agent may only read data. On the other hand, in absence of the user authorization a malicious subscriber may violate the data integrity by publishing false data. In this respect, a general solution against the elevation of privileges is the definition of advanced access control rules inside all the software modules that are in contact with the assets.

3.2.6. Unauthorized Code Execution

The capability to receive commands from other components of the system may open the way for unauthorized code execution inside the software modules. A common case is when a remote software can send carefully crafted commands to a software module with database access, to run unauthorized database queries, which may cause information disclosure or tampering. In our context this may be a specific threat for the SGs and the DA. In addition, similar cases can occur as result of software bugs, e.g., the recently discovered *Shellshock* bug [18] in the GNU Bash. Thereby, the software quality of the data manipulation agents has to be carefully reviewed before the deployment/adoption to avoid these kind of threats.

3.2.7. Physical Access

Physical access is an emphasized threat in the case of IoT systems, because the system has numerous components exposed in uncontrolled environments. As result of the physical access the attacker can gain full access to the persistent storage of the affected component. This directly cause the disclosure and the tampering of the confidential information, e.g.,

sensor data, but physical access can also be a starting point for further attacks, e.g., MITM attack, by changing the configurations and inserting redirections or node replication by stealing credentials. This fact has increased significance in case of SGs and SNs in a DA-PS platform. To deal with this type of threat the protection of persistent data, e.g., by means of database encryption, might seem the obvious solution. However, in this case the encryption keys are usually stored on the same persistent storage device and, if not properly protected, an attacker can access these keys and the sensitive sensor data.

3.2.8. OS related threats

Most significant parts of the system at hand are built on top of modern OS. As a result, the components of DA-PS platform inherit all advantages that originate from adopting a generic, and cost-effective commodity software. Nevertheless, traditional OS are known to foster critical software vulnerabilities, e.g. *Shellshock*, which in the present context may drive to unauthorized access to confidential resources, e.g. sensor database, configuration files. Multiple features inside a DA-PS platform are based on the mechanisms and tools provided by the OS, e.g., networking, right handling or resource management. These mechanisms may require competent configuration to provide the documented security features, thereby the shortage of it may leave open vulnerability points. In this respect, the proper selection of the type and version of OS and the running components, as well as their correct configurations is the key mitigation technique for these types of threats.

4. Case Study

This section presents a case study of a real implementation of a DA-PS platform following the architecture presented on Fig. 1 and analyses all of the platform components based on the list of threats described in the previous section.

4.1. Assumptions

The sensor level of the platform is implemented using the ZigBee specification for low-power wireless mesh communication. In the experimental platform a SN is composed of a ZigBee End Device or Router, mounted on an embedded system which contains one or more sensors of different types. The ZigBee Coordinator resides in the center of the WSN, communicates with the other ZigBee nodes and acts as a SI. As Sensor Nodes and Sensor Gateway an out-of-the-box commercial solution was used whose name and vendor we purposefully omit. It provides out-of-the-box Sensor Agent and Sensor Synchronized Agent implementations as well as an internal MySQL database. These types of SGs are dedicated commercial hardware devices, but they contain a commodity PC with a Linux OS, and as a result, these have many ICT-like characteristics.

A casual PC is placed in the role of the DA with a MySQL database. Inside the DA, the Message Queue Telemetry Transport (MQTT) protocol is used for the publish-subscribe service which is a light-weight M2M messaging protocol over TCP/IP using client-server architecture. The MQTT standard is only a transport protocol, therefore providing appropriate security features is the responsibility of the implementers. Due to this fact the security of the system mainly depends on the unstandardised features and the code quality of the broker implementation. Considering these, as MQTT broker implementation the Mosquitto software was chosen

and the SBs and the Publisher Agent are custom applications written in Java, both of these using the Paho software library.

The experimental DA-PS platform is composed of two ZigBee sensor networks connected to two SGs whose data is aggregated in the central DA. The SNs measure the environmental temperature, humidity and the air pressure and the SBs are weather monitoring mobile apps which list the actual and the history of the weather information.

4.2. Security Assessment of the ZigBee Layer

The ZigBee standard provides two security levels, the network layer and application layer security, both of these based on the 128-bit AES encryption. Nonetheless, data intercepting, tampering or injection can occur as a result of spoofing. The disclosure of a security key may drive to node replication or can enable unauthorized nodes to join the network allowing the data to be snooped or modified. In this respect, the policies for storing and distributing the AES keys determines the protection level of this communication layer against tampering and information disclosure. An acceptable solution against this threat can be the usage of off-site configured Trust Center keys, a technology defined by the ZigBee specification, which are used to securely distribute the keys applied to communication data encryption.

The sensor nodes of the experimental DA-PS platform are placed in an uncontrolled environment, therefore the physical access to them is achievable. This may drive to information disclosure, e.g., snooping the credentials, which can be the starting point for further attacks, e.g. malicious node insertion. Fortunately, the ZigBee modules we adopted in this experiment incorporate measures against this situation on their configuration interfaces, e.g., write-only credentials, but with advanced equipments the credentials can be extracted directly from the chip. To protect against this situation the definition of a method that periodically changes the credentials inside the ZigBee nodes can be a solution.

On the other hand, DoS is a significant threat to the ZigBee communication, because it may cause packet losses or link interruptions. Fortunately, the IEEE 802.15.4 standard that defines the physical and MAC layer for the ZigBee provides multiple physical channels and implements Clear Channel Assessment techniques and using these the ZigBee coordinator can select the favourable channel for communication. This helps to mitigate the effects of DoS attacks.

4.3. Security Assessment of the Aggregation Layer

On the aggregation layer in the experimental platform the communication between the components is secured using TLS, therefore the standard information snooping or tampering techniques, e.g., sniffing or packet injection, in most cases are less likely to succeed. However, given recent vulnerabilities on TLS implementations, attacks on TLS might still be possible, given a vulnerable configuration/implementation.

4.3.1. Sensor Gateway

A close analysis of SGs revealed that most of the threats are related to an extremely outdated Linux OS version. Unfortunately, this OS version is subject to a vast number of recently discovered and critical vulnerabilities, e.g., *Heartbleed*, *Poodle* and *Shellshock*. As a result, we strongly believe that an attacker might adopt several different attack vectors to compromise a SG.

A specific example in this sense are the remote administration features embodied in each SG. In this respect remote administration is available by means of a custom Web interface. This in turn can execute `bash` commands with `root` privileges that allow administrators complete (remote) control over the SG. While the advantages of such a tool are obvious from a purely administrative point of view, traditional security recommendations clearly state that such measures should be avoided. In this scenario, the remote Web browser provides advanced capabilities not only for administrators, but for malicious actors as well. Furthermore, by considering the outdated OS together with the highly privileged application, an attacker might take full advantage of the scenario. For example, by just considering one of the most recently reported `bash` vulnerabilities, i.e., *Shellshock*, an attacker can launch unauthorized code executions on the SGs, which may open back-doors and ultimately lead to complete system compromise, e.g., spoofing, tampering, repudiation, information disclosure or elevation of privileges. Another exploitable vulnerability that may be used in this scenario is *Poodle*, which enables the successful execution of a MITM attack on the administration data lines.

For all the above mentioned vulnerabilities the most simple mitigation approach is an OS update. Unfortunately, official updates are not available for this SG model, but standard Linux updates can be performed from the official repository of the used Linux distribution.

In terms of communication interface, a significant threat is the susceptibility to DoS attacks. This may lead to the interruption of communications, and to dropped critical administrative data packets. SGs communicates only with previously known external entities, therefore, by using firewall rules, the malicious data flows can be blocked. This is a powerful technique for protection against DoS attacks.

Given their deployment in outdoor scenarios, SGs are susceptible to physical tampering. In this context, attackers with physical access to SGs may write in the contents of the internal storage device and may change configurations such as sensor data credentials. Most importantly, attackers may install back-door malicious software which can enable remote control and monitoring of SG activities in the attempt to undertake other SG as well. Even more disturbing, as revealed by our experiments, the ZigBee receiver is connected to the on-board PC through RS232 bus within SGs. Here, despite the encryption of data in the ZigBee network, unencrypted data is available to applications. The software level protection, e.g., file system encryption, against the physical access is not effective and the hardware is a finalised commercial product, therefore the avoidance of the physical access is a requirement to assure the overall system security.

4.3.2. Data Aggregator

In the experimental scenario the DA runs up-to-date Linux OS and the possibility for physical access to it is negligible. However, it serves the external connection requests, receives data packets from remote entities and also provides remote administration interface via SSH, therefore it is exposed for other types of threats like a SG.

In this context the DoS is a considerable threat, because it may cause the unavailability of the aggregated data. For example, a burst of connection and/or authentication attempts may consume the open connection slots of the MQTT broker, making the connection of authentic clients impossible. Furthermore, the input slots for the SGs represent another target point for DoS attacks, on which the data aggregation process can be obstructed. In addi-

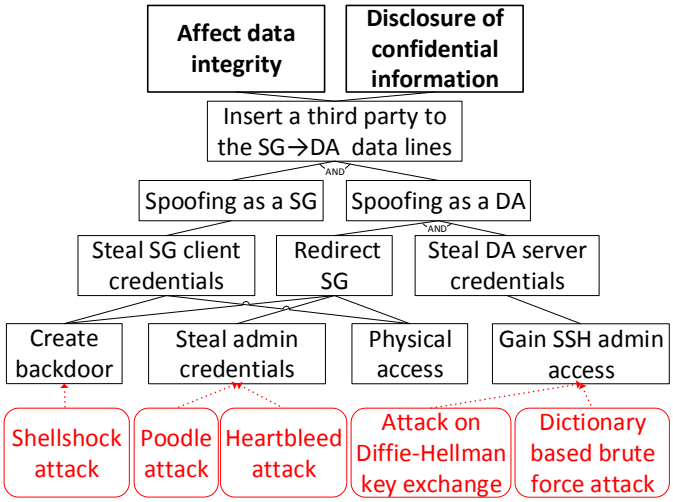

Fig. 3. Attack tree for MITM attack between SGs and the DA

tion, bursts of subscribe requests may consume the memory and the CPU time of the DA, which may slow down the data delivery to the clients. These unfavourable effects can be mitigated by defining adequate rules for the communication interactions, e.g., firewall rules for the connection attempts, bandwidth limitations, and/or blacklists.

On the other hand, the capability for remote administration via SSH may be a considerable enabler of different attacks. For example, an improperly hardened SSH service may drive to a MITM attack on the configuration line, which may provide access for the attackers with administrator privileges to the DA. Furthermore, the probability for a successful brute force attack, e.g., dictionary based attack, may reach a considerable level if the passwords are not adequately selected in the DA. A strong solution to secure the administration lines can be the usage of Virtual Private Network (VPN).

4.3.3. Real Attack Scenario

Based on the analysis from this section we provide an example of an attack aimed at affecting the data flow integrity and the disclosure of confidential information in the same time.

Fig. 3 represents a real attack scenario to accomplish the aforementioned tasks. For the representation of the scenario we apply the attack tree model proposed by Schneier [16], and to keep the attack tree as simple as possible, we represent only the feasible sub-tasks on it.

The example presents a way to reach the aimed goals by inserting a third party to the communication between the SGs and the DA. For this, two main sub-tasks have to be accomplished: spoof as a SG and a DA in the same time. The former task can be achieved in different ways by profiting from the large variety of vulnerabilities exposed by the SG. For example, using the *Shellshock* vulnerability a back-door can be opened on the SG to provide further access. Through this, the client certificate used for the TLS handshake can be cloned which opens a direct way for spoofing as a SG. The latter task can be completed, for example, starting from a MITM attack on a SSH administration line. This is achievable by profiting from the vulnerability of the Diffie-Hellman key exchange algorithm and it opens a direct way to obtain the server certificate of the DA. Using it, the attacker can spoof itself as a DA.

5. Conclusion

In this paper we have proposed a general architecture for sensor data aggregation IoT platforms composed of sensor networks interconnected with traditional ICT infrastructures, with data delivery support based on publish-subscribe. The complexity of these platforms exposes them to a large variety of security threats, therefore we have formulated a comprehensive threat analysis considering the availability, integrity and confidentiality security objectives. Using the STRIDE approach in an

extended form we have categorized the possible threats against the studied platform and based on these we have performed a case study on a real platform with the proposed architecture. Finally, we have presented a real attack scenario targeting the integrity and the confidentiality of the data flows in the platform.

Acknowledgment

The work of B. Genge was supported by the European Social Fund under the responsibility of the Managing Authority for the Sectoral Operational Programme for Human Resources Development, as part of the grant POSDRU/159/1.5/S/133652.

The work was partially supported by the TÁMOP-4.2.2.C-11/1/KONV-2012-0001 project. The project has been supported by the European Union, co-financed by the European Social Fund.

References

[1] K. Ahmed and M. Gregory, "Integrating wireless sensor networks with cloud computing," in *Mobile Ad-hoc and Sensor Networks (MSN), 2011 Seventh International Conference on*. IEEE, 2011, pp. 364–366.

[2] C. Alcaraz and J. Lopez, "A security analysis for wireless sensor mesh networks in highly critical systems," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol. 40, no. 4, pp. 419–428, 2010.

[3] T. Bakıcı, E. Almirall, and J. Wareham, "A smart city initiative: the case of barcelona," *Journal of the Knowledge Economy*, vol. 4, no. 2, pp. 135–148, 2013.

[4] N. Bressan, L. Bazzaco, N. Bui, P. Casari, L. Vangelista, and M. Zorzi, "The deployment of a smart monitoring system using wireless sensor and actuator networks," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 49–54.

[5] Z. Durumeric, J. Kasten, D. Adrian, J. A. Halderman, M. Bailey, F. Li, N. Weaver, J. Amann, J. Beekman, M. Payer *et al.*, "The matter of heartbleed," in *Proceedings of the 2014 Conference on Internet Measurement Conference*. ACM, 2014, pp. 475–488.

[6] A. C. Geary, "Analysis of a man-in-the-middle attack on the diffie-hellman key exchange protocol," DTIC Document, Tech. Rep., 2009.

[7] B. Genge, P. Haller, A. Gligor, and A. Beres, "An approach for cyber security experimentation supporting sensei/iot for smart grid," in *2nd International Symposium on Digital Forensics and Security*, 2014.

[8] B. Genge, A. Beres, and P. Haller, "A survey on cloud-based software platforms to implement secure smart grids," in *Power Engineering Conference (UPEC), 2014 49th International Universities*. IEEE, 2014, pp. 1–6.

[9] M. M. Hassan, B. Song, and E.-N. Huh, "A framework of sensor-cloud integration opportunities and challenges," in *Proceedings of the 3rd international conference on Ubiquitous information management and communication*. ACM, 2009, pp. 618–626.

[10] S. Hernan, S. Lambert, T. Ostwald, and A. Shostack, "Threat modeling-uncover security design flaws using the stride approach," *MSDN Magazine-Louisville*, pp. 68–75, 2006.

[11] J. M. Hernández-Muñoz, J. B. Vercher, L. Muñoz, J. A. Galache, M. Presser, L. A. H. Gómez, and J. Pettersson, *Smart cities at the forefront of the future internet*. Springer, 2011.

[12] B. Möller, T. Duong, and K. Kotowicz, "This poodle bites: Exploiting the ssl 3.0 fallback," 2014.

[13] S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview," *Computer Networks*, vol. 53, no. 12, pp. 2022–2037, 2009.

[14] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure data aggregation in wireless sensor networks: Filtering out the attacker's impact," *Information Forensics and Security, IEEE Transactions on*, vol. 9, no. 4, pp. 681–694, 2014.

[15] Y. Sang, H. Shen, Y. Inoguchi, Y. Tan, and N. Xiong, "Secure data aggregation in wireless sensor networks: A survey," in *Parallel and Distributed Computing, Applications and Technologies, 2006. PDCAT'06. Seventh International Conference on*. IEEE, 2006, pp. 315–320.

[16] B. Schneier, "Attack trees," *Dr. Dobbs journal*, vol. 24, no. 12, pp. 21–29, 1999.

[17] F. Touati, R. Tabish, and A. Ben Mnaouer, "Towards u-health: an indoor 6lowpan based platform for real-time healthcare monitoring," in *Wireless and Mobile Networking Conference (WMNC), 2013 6th Joint IFIP*. IEEE, 2013, pp. 1–4.

[18] D. A. Wheeler, "Shellshock," http://www.dwheeler.com/essays/shellshock.html, 2014, [Online; accessed 22-February-2015].

[19] M. Yoon, M. Jang, H.-I. Kim, and J.-W. Chang, "A signature-based data security technique for energy-efficient data aggregation in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2014, 2014.

[20] Q. Zhu, R. Wang, Q. Chen, Y. Liu, and W. Qin, "Iot gateway: Bridgingwireless sensor networks into internet of things," in *Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on*. IEEE, 2010, pp. 347–352.