SECURITY VULNERABILITIES AND RISKS IN INDUSTRIAL USAGE OF WIRELESS COMMUNICATION

S. Plosz, A. Farshad, M. Tauber
Austrian Inst. of Technology
2444 Seibersdorf, Austria
{ sandor.plosz.fl, markus.tauber, arsham.farshad.fl }@ait.ac.at

C. Lesjak, T. Ruprechter
Infineon Technologies Austria
8020 Graz, Austria
{ christian.lesjak, thomas. ruprechter }@infineon.com

N. Pereira
Polytechnic Institute of Porto
4200-072 Porto, Portugal
nap@isep.ipp.pt

Abstract

Due to its availability and low cost, the use of wireless communication technologies increases in domains beyond the originally intended usage areas, e.g. M2M communication in industrial applications. Such industrial applications often have specific security requirements. Hence, it is important to understand the characteristics of such applications and evaluate the vulnerabilities bearing the highest risk in this context. We present a comprehensive overview of security issues and features in existing WLAN, NFC and ZigBee standards, investigating the usage characteristics of these standards in industrial environments. We apply standard risk assessment methods to identify vulnerabilities with the highest risk across multiple technologies. We present a threat catalogue, conclude in which direction new mitigation methods should progress and how security analysis methods should be extended to meet requirements in the M2M domain.

1. Introduction

Wireless communication has recently gained foothold in the industrial environment. It is frequently used as interface of machine-to-machine (M2M) communication, especially due to the recent wide availability of smart-devices, such as smart-meters that are being installed on a large scale to implement smart-energy grids. Smart-meters measure energy consumption in households and make it available to utility providers, which use this information to manage the energy grid more efficiently, and offer advanced services. In addition, M2M communication introduces new threats due to, for example, the resource constrains of the devices, or their deployment which needs to be considered. Representative use cases can be found in the Arrowhead [1] project in which this work is being conducted.

To uncover the most common communication technologies, the type of information communicated between machines and their level of confidentialities in industrial M2M communications, we have conducted a survey among some of our Arrowhead partners. The Arrowhead M2M use cases include aircraft maintenance, automation in mining industry, self-condition monitoring mobile machinery and condition monitoring for transportation systems, smart-services in the automotive sector and smart-grid use cases. Based on our survey, we focused on identifying security threats in the machine to machine (M2M) context using the following wireless technologies: IEEE802.11 (Wireless LAN, WLAN), IEEE802.15.4 (ZigBee) and Near Field Communication (NFC). For WLAN, the vulnerabilities of both Pre-RSN (IEEE802.11) and RSN (IEEE802.11i) networks are described.

Near field communication (NFC) is a set of standards for wireless data and power transfer over very short distances up to approximately 10 cm. An NFC connection establishes automatically when two NFC devices get in close proximity. Albeit NFC is no pure M2M communication, we assume it to be an enabler for use cases such as initial node set-up, ad-hoc interaction with a node, and connection handover to other M2M channels such as WLAN.

The IEEE 802.15.4 is a standard intended for low power wireless networks. This standard only specifies the lower physical and medium access control (MAC) layers, and many higher-level specifications were defined to operate on top of 802.15.4, such as ZigBee [19], ISA100.11a [20], WirelessHART [21], and 6LoWPAN [22]. Out of these available 802.15.4 standards, we will focus on ZigBee, as it is one of the most popular standards usually associated with 802.15.4 to provide network and transport layers.

The building blocks of this paper are as follows: We review the security features and related security issues of WLAN, NFC and ZigBee technologies. We identify threats to these standards in the industrial context, and describe them in threat catalogues, which is a contribution in its own right. We adapt an ETSI guideline with likelihood and impact assessments to carry out a structured risk analysis and identify the most critical threats in the technologies. This identification is a valuable contribution to the area of M2M communication as it allows steering the development of appropriate mitigation mechanism. A pragmatic additional benefit of our work,

[1] www.arrowhead.eu

on which we comment in our conclusions, is the applicability of security analysis methods.

2. Related work

M2M communication is involved in different areas including healthcare, remote maintenance and control, vehicular telematics and smart grids [1]. Each of the mentioned applications has specific security requirements and different security threats and vulnerabilities. For example, [2] presents a comprehensive survey of cyber security issues for the Smart Grid; enumerating the security requirements, potential network vulnerabilities and attack countermeasures.

As M2M concepts mainly emerged from Wireless Sensor Networks (WSNs), most of the publications in the literatures try to answer challenges for WSN security. A recently published IETF draft [3] reviews aspects and functionalities that are required for the secure IP-based solution of the Internet of Things (IoT).

In [5] a threat analysis has been carried out for WiMax following ETSI guidelines. Previous studies concerning WLAN security like [7] however mainly highlight possible vulnerabilities and attacks and their countermeasures for enterprise and home/office environments. Security issues and risk analysis of vulnerabilities of WLAN in the context of M2M communication are not studied as far as we are aware of.

Previous work on the security of NFC relates to consumer use cases and payment, and mainly focuses on vulnerabilities and attacks. No risk assessment is known to us yet, especially in the industrial context [8]. Revealed a number of implementation errors and bugs in various NFC software stacks. The authors in [9], [10], [11] investigate the possibility of eavesdropping NFC communication up to 10 m in theory and 30-240 cm in experiments. Furthermore, [9] assume the feasibility to corrupt or modify data transmitted via the NFC link. An analysis of the NFC Signature RTD by [12] showed a number of design weaknesses, which circumvent the intended integrity and authenticity properties. Major issues with NFC connections are relay attacks (e.g., in [13], [14]), where the very short range of NFC is extended using another communication channel.

An analysis of known 802.15.4 and ZigBee vulnerabilities in the context of industry environments was presented in [23]. Another collection of security issues, dedicated to ZigBee networks, can be found in [24], where threats at the routing and application layer are described, and it also shows inefficiencies in managing both the network key and devices certificates. Several vulnerabilities of 802.15.4 were described in [25] especially describing AES-CTR flaws. Other works (e.g. [26][27]) have focused on 802.15.4 MAC layer attacks. Noticeably, to our knowledge, no risk assessment of 802.15.4/ZigBee vulnerabilities in the context of M2M communication exists.

3. Security features and issues of wireless technologies

Threat analysis and risk assessment are essential parts for identifying the impact on security objectives and proposing an optimum security solution/policy which has received less attention for M2M applications previously. The following security objectives for information security in general and wireless communication specifically can be identified [6]:

Confidentiality: Communication data is protected against interception of unauthorized parties.

Authentication & Access control: Only authenticated users get access to the network. Users know with which entity they are communicating with (authenticated user/machine).

Data Integrity: Data is not modified by unauthorized parties.

Availability: Network services are available and are not broken down because of attacks.

Both threat analysis and risk assessment processes are very dependent to the application and context of deployment of the technology. For example in the office environment, confidentiality is the most important security feature compared to the integrity and availability whereas in an industry environment availability is the most critical so security policies must give privilege to rules preventing attacks targeting the availability, such as DoS attacks [4]. Also, for mission- and safety-critical automation systems authentication & access control are crucial [28].

3.1. Wireless LAN

To provide the main objectives in WLAN communication, the IEEE 802.11 standard proposed WEP (Wired Equivalent Privacy) in 1999 with intention of providing confidentiality and integrity of communication over WLAN. In 2004, an amendment to the standard published to mitigate known problems with security issues in the IEEE802.11. In IEEE 802.11i amendment, two general classes of security were proposed:

Pre-RSN Security: The legacy security capabilities developed in the original IEEE 802.11 specification. Two types exit:

- Open system: this can be misused easily for unauthorized access by MAC address spoofing of a rogue AP
- Shared key authentication and WEP confidentiality protection: this one is as insecure as open system authentication. WEP based authentication can be easily compromised which threatens confidentiality and integrity of the communication. Key management is another hurdle in this approach, especially in large network setups. Rogue AP, dictionary attack, eavesdropping of authentication frames and breaking the pass key are some of the main attacks against the shared key authentication.

RSN Security: includes a number of security mechanisms to create Robust Secure Networks. Two data origin authentication, integrity check and confidentiality protocols are proposed in the 802.11i amendment: TKIP and CCMP. The latter one is FIPS compliant as it uses an 128bit AES block cipher. TKIP has vulnerabilities because it uses the RC4 stream cipher engine as used by WEP, which can be broken. WPA can be cracked in less than a minute with a man-in-the-middle attack.

3.2. Near Field Communication (NFC)

An NFC connection is not natively protected by any cryptographic mechanisms. Yet, its rather limited communication distance is assumed to provide a certain level of security. Currently, as the NFC specifications mainly cover the pure data link, applications utilizing this link need to take care of securing the communication channel. Until today, only two native approaches securing the NFC link are published:

- NFC-SEC and NFC-SEC-01 (ECMA 385 and 386) standardize a general security framework and ECDH and AES based primitives for a secure, yet unauthenticated channel via NFC. Therefore, NFC-SEC is vulnerable to man-in-the-middle attacks, as no entity authentication is possible due to the missing pre-installed secret [15].
- The Signature RTD [16] provides integrity and authenticity for content read from NFC tags. It is not suitable for peer to peer communication, and does not provide confidentiality. Design weaknesses were discovered in [12].

Furthermore, the NFC Forum does not provide a specification to protect peer communication and to provide authenticity, integrity and confidentiality in a secure channel. Yet, there is effort in research considering this issue. An approach denoted LLCPS [17] uses SSL/TLS on the NFC LLCP layer.

3.3. 802.15.4/ZigBee

The 802.15.4 standard provides security for incoming and outgoing traffic by allowing higher layers to define the type of protection to be implemented at the MAC layer. The protection implemented employs AES for symmetric key cryptography, and defines several security modes (AES-CTR, AES-CBC-MAC, AES-CCM), providing data confidentiality, data authenticity, and replay protection. This standard does not say how symmetric keys are defined. This is a task for upper layers, such as ZigBee.

ZigBee defines network routing, transport primitives (unicast, broadcast and groupcast), network organization, address conflict resolution functionalities, and also defines a set of standard application services (such as device and service discovery, or standard definition of application messages). Security wise, ZigBee includes features related to authentication and encryption, and key definition and establishment.

Table 1 Threat categories

Eavesdropping (ED)	Attacker passively monitors the network communications for capturing communicating data and authentication credentials. (passive)
Man-in-the-Middle (MiM)	Attacker intercepts the path of communications between two legitimate parties, thereby obtaining authentication credentials and data. (active)
Masquerading (MQ)	Attacker impersonates an authorized user and gains certain unauthorized privileges. (active)
Message Modification (MM):	Attacker actively alters a legitimate message by deleting, adding to, changing, or reordering it. (active)
Message Replay (MR)	Attacker passively spoofs transmission frames and retransmits them, acting as if the attacker is a legitimate user. (active and passive)
Traffic Analysis (TA)	Attacker passively monitors transmissions to identify communication patterns and participants. (passive)
Physical Attack/Firmware Replacement (PA)	Attacker has physical access to the device and can replace firmware or steal credential information like static keys. (active)
Routing Attack (RA)	A network layer attack where attacker tries to manipulate routing table to misdirect traffic in WMN and WSN networks. (active)
Authentication Attacks (AA)	Intruders use these attacks to steal legitimate user identities and credentials. Dictionary attacks and brute force attacks are two common attacks in this category. (active)
Availability/Denial of Service Attacks (DoS)	Attacks attempt to inhibit or prevent legitimate use of the wireless communication services, including DoS attacks. (active)

ZigBee defines a special node called the *Trust Center* (TC), which is responsible for storing the keys for the network, configure devices with its keys, and authorize a device into the network. Three methods for key exchange are defined: (i) pre-installation of the key in the device, for example at deployment time; (ii) transport, when the TC sends the key (this might happen in an unsecured way, if a secured manner is not available); (iii) establishment, when the TC negotiates with end devices how to establish the keys, without transporting them. In this latter method, three methods of key establishment exist: (a) Symmetric Key Key Establishment (SKKE), (b) Certificate-based Key Establishment (CBKE), and (c) Alpha-secure Key Establishment (ASKE), and three types of keys exist: master key, network key and link key. The master key is used to establish keys and it is shared pairwise between two devices. The network key, shared amongst all nodes in the network, is used to secure broadcast communications. The link key is used to secure unicast communication between two devices.

4. Threats' Catalogue

A threats' catalogue comprises the list of known threats. They are categorized based on the main categories of attacks for wireless communication shown in Table 1 [3]. Active attacks are those carried out by transmitting or replaying traffic while passive ones are only based on listening traffic. In the next subsections some of the known threats are listed for the examined wireless technologies which will be assessed in the subsequent sections.

4.1. Wireless LAN

Based on the categories presented in Table 1 we list of some of the known threats present in WLAN communication in Table 2 [29].

Table 2 Threats' catalog for WLAN

Name	Type	Description
WEP Shared Key Cracking	AA	802.11 shared key authentication with a cracked shared key or default WEP keys.
WPA-PSK Cracking	AA	Recovering a WPA PSK from captured key handshake frames using dictionary attack tools.
Application Login Theft	AA	Capturing application layer credential information such as email account and password by capturing clear text transmissions.
AP Theft	DoS	Physically removing an AP from a public space.
RF Jamming	DoS	Transmitting noise at the same frequency as the target WLAN.
802.11 Beacon Flood	DoS	Generating thousands of counterfeit 802.11 beacons to make it hard for stations to find a legitimate AP.
802.11 Data Deletion	DoS	Jamming an intended receiver to prevent delivery while simultaneously spoofing ACKs for deleted data frames.
Intercept TCP sessions/SSL,SSH tunnels	MiM	Intercept TCP sessions or SSL/SSH tunnels in the evil twin AP.
Evil Twin AP	MQ	Masquerading as an authorized AP by beaconing the SSID to lure users.
Bit-flipping or Message Forgery in WEP	MM	Attacker can change bits in the frame body and correct the CRC integrity check part of the frame that can pass the integrity check. Attacker use bit flipping to compromise the security stream key.
802.11 Frame Injection	MR	Crafting and sending forged frames.
Device Cloning	PA	Including a backdoor in the cloned device.
Selective Forwarding	RA	Selectively forward frames to the next hop.

4.2. NFC

NFC is a direct point-to-point data and power transfer link between two end points, hence a networking mechanisms is neither required nor available. Thus, most network related attacks do not apply to NFC. Furthermore, it differentiates a number of end point device types, namely: reader, contactless card and tag. In our industrial M2M context, we only consider NFC as an interface into a node, which can be accessed using a portable reader device, in order to establish a connection with this node when the reader is in close physical proximity. The threats we identified for this NFC scenario are listed in Table 3 [9], [10], [11], [13], [14].

Table 3 Threats' catalog for NFC

Name	Type	Description
Portable reader device theft	DoS	An attacker steals or destroys a genuine reader device. This may cause service interruption as the device is not available to the operator. The attacker may also reverse engineer the device or extract data from it.
Clone or modify portable reader device	PA	An attacker creates a manipulated reader device, which may maliciously act against a node.
Capturing the RF signal from distance	ED	An attacker captures the data transmitted via the NFC link from a greater than the intended distance of < 10 cm.
Modify or insert data on NFC link	MM	An attacker modifies the data transmitted via the NFC link, or inserts data before a legitimate entity may answer.
Jam or block RF signal	DoS	An attacker blocks any communication using a jammer.
Corrupt data on RF link	DoS	An attacker manipulates the data on the NFC link in order to make it unusable.
Wormhole attack or relay attack	MR/RA	An attacker relays the NFC connection via a greater distance, using two additional NFC devices connected via an alternative channel (e.g., WLAN). This kind of attack is known for contactless cards, yet it is also feasible for our scenario.
Destroy, remove or steal node	DoS	An attacker removes or physically destroys the node, either to make it unavailable or to further inspect it.
Rogue node	PA	An attacker manipulates the firmware or software of a node in a malicious way, causing it to misbehave against NFC readers and potentially attacking or infecting readers.
Unauthorized access to node	AA	An attacker communicates with a node via the NFC interface using a manipulated reader and gains access to the functionality provided via the NFC interface.

4.3. ZigBee

Table 4 presents a list of known threats in 802.15.4/ZigBee [23], [25], [26], [27].

Table 4 Threats' catalog for ZigBee

Name	Type	Description
RF Jamming	DoS	Transmitting noise at the same frequency as the target wireless network.
Network Flood	DoS	Send a large number of large packets. An attacker can seriously degrade the network.
Rogue Node	MiM	A rogue router or coordinator can introduce corrupted packets, or discard them.
Device Cloning/Firm. Replacement	PA	Including backdoor to the cloned device. Firmware or software may be updated to add new functionalities or features.
802.15.4 Frame Injection	MR	Crafting and sending forged frames.
Security parameter extraction by physical access	PA	Nodes that are accessible by unauthorized users are susceptible to be compromised for extracting security keys and other security configurations.
Sinkhole/Blackhole Routing	RA	It happens when an attacker encourage all nodes traffic routing through his node and drops them.
Selective Forwarding	RA	Selectively forward frames to the next hop.
Network Traffic Analysis	TA	Passively listen to traffic and try to infer different information.
False Battery Life Extension	DoS	An attacker can pretend to be in battery life extension mode to dominate channel access.
False association	DoS	An attacker sends forged association packets, depleting the ZigBee coordinator's memory.
False disassociation	DoS	An attacker sends forged disassociation packets, causing nodes to be dropped out of the cluster.
False ACK	MQ)	Attacker sends false ACK packets letting the sender think messages have been correctly received when they might have not.
AES-CTR replay protection	DoS	Taking advantage of the replay protection mechanism, an attacker may cause legit packets to be perceived as repeated and discarded.
AES-CTR packet corruption	DoS	An attacker might forge a packet with invalid payload, but valid CRC, wasting the resources of the node.
Plaintext key capture	ED	In some ZigBee implementations, network and/or master keys might be communicated in plaintext.
Key capture with SKKE	ED	In a network using SKKE, an attacker with the master key can guess pairwise link keys.

PANId conflict	DoS	A coordinator detecting a repeated PANId will trigger a conflict resolution procedure, reducing network availability.
Beacon Synchronization DoS	DoS	An attacker may cause collisions on broadcasted beacons and hence severely hinder the MAC mechanism.
GTS DoS	DoS	An attacker can synchronize with the broadcasted beacons and use this timing to cause collisions on the GTS, which are assumed to be collision-free.

5. RISK ASSESSMENT

We will now apply threat and risk assessment methodologies to evaluate threats in the M2M context. Such methodologies are either quantitative or qualitative. Quantitative based approaches rely on the historical data and provide a numerical level of risk that represents the probability of a threat to successfully happen. Qualitative approaches only show a symbolic level of risk. They are very dependent on the knowledge and experience in one hand, and on the point of view of who carries out the assessment, on the other hand. We have chosen a qualitative approach, as we do not have historical data about specific applications of the wireless technologies available.

For risk assessment, we adopted the ETSI guidelines [18] with modifications to make them more general. These guidelines can be easily adopted, based on the specific requirements for different use cases. We explicitly consider the impact of each threat on three main security objectives (e.g., confidentiality, integrity and availability) separately. It helps to apply risk assessment based on the importance of the three objectives for specific use cases. It needs be noted that all metric definitions are based on the ETSI guidelines unless it is mentioned otherwise.

Risk assessment comprises of two assessments, likelihood and impact, which are described in the following subsections.

Table 5 Likelihood of an attack as a function of attacker motivation and difficulty of perpetrating the attack.

Difficulty Motivation	None	Solvable	Strong
Low	Unlikely		
Moderate	Likely	Possible	Unlikely
High		Likely	

5.1. Likelihood assessment

ETSI defines three discrete levels for categorizing the likelihood of an attack happening associated to a given threat: unlikely, possible and likely. To evaluate attack likelihood the following two factors are considered:

Motivation for the attack that drives an attacker is very dependent on the use cases. For example vandalism are less likely motivation for attacking network of an industry plant. The most common motivations for an attack are opportunity and greed. The interest level of a motivation can be high, moderate or low.

Table 6 Impact level based on the scale and detectability of an attack/threat

		Detectability and Recoverability		
		Low	Moderate	High
Scale levels	Node	Moderate	Minor	Minor
	WAN	Significant	Significant	Moderate
	EN	Significant	Significant	Moderate

Technical difficulty for perpetrating the attack refers to the barriers in carrying out an attack. The level of difficulty is very dependent on a standard's age, for example WEP was supposed to be a robust protocol and difficult to break when it was proposed; yet it is now very easy to attack. Technical difficulty for implementing a threat can be either strong, solvable or none. Based on above risk factors, likelihood levels are defined in Table 5.

5.2. Impact assessment

This method evaluates the impact of an attack if it happens. We define the impact of the attack based on its scale or scope that affects communication security of the network, and the possibility of detecting and recovering from effects of the attack. The two metrics are explained in the following.

Scale level shows the scale of network that will be affected by an attack. There can be a machine/node under attack or the attack may expand to the entire enterprise network. The scale level can be one of the following:

1. Node: Attack only affects the node under attack or user(s) of that node. It does not have serious influence on the communication of other nodes.
2. Wireless Access Network (WAN): Attack also affects other nodes in the same service set or ad-hoc/mesh network.
3. Enterprise Network (EN): Effects on whole enterprise network including the wireless access network.

Detectability and Recoverability: Impact of threat depends on whether it can be detected easily and how easy is to recover from the effects of the attack. Based on the scale of attack and ability to detect and recover from it, the impact of a threat is defined in Table 6.

Table 7 Risk assessment guideline based on the impact and likelihood metrics

		Likelihood		
		Unlikely	Possible	Likely
Impact	Significant	Minor	Major	Critical
	Moderate	Minor	Major	Major
	Minor	Minor	Minor	Minor

In our study, the impact metric for each main security objective is assessed separately (based on the recommendations of the ISO 27005 guideline). It is used to do risk assessment for each security objective separately and realize threats with the highest risk based on the application use cases and their most important security requirements.

Table 8 Risk assessment applied to the threat catalogue for different security objectives

							Impact on				Risk			
Technology	Name of threats'	Technical difficulty	Motivation level	Likelihood	Scale	Detectability	Confidentiality	Availability	Data integrity	Authentication & access control	Confidentiality	Availability	Data integrity	Authentication & access control
WLAN	WEP Shared Key Cracking	None	High	Likely	WAN	Low	Significant	Minor	Minor	Minor	Critical	Minor	Minor	Minor
	WPA-PSK Cracking	None	High	Likely	WAN	Low	Significant	Minor	Minor	Minor	Critical	Minor	Minor	Minor
	Application Login Theft	None	High	Likely	Node	Low	Moderate	Minor	Minor	Significant	Major	Minor	Minor	Critical
	AP Theft	None	Low	Unlikely	WAN	High	Moderate	Moderate	Minor	Significant	Minor	Minor	Minor	Minor
	RF Jamming	None	Low	Unlikely	WAN	Low	Minor	Significant	Minor	Minor	Minor	Minor	Minor	Minor
	802.11 Beacon Flood	None	Low	Unlikely	WAN	High	Minor	Moderate	Minor	Minor	Minor	Minor	Minor	Minor
	802.11 Data Deletion	None	Low	Unlikely	Node	Moderate	Minor	Minor	Minor	Minor	Minor	Minor	Minor	Minor
	Intercept TCP sessions/SSL, SSH tunnels	None	High	Likely	Node	Low	Moderate	Minor	Moderate	Moderate	Major	Minor	Major	Major
	Evil Twin AP	None	High	Likely	WAN		Moderate	Moderate	Moderate	Significant	Major	Major	Major	Critical
	Bit-flipping or Message Forgery in WEP	None	Low	Unlikely	Node	Low	Minor	Minor	Moderate	Minor	Minor	Minor	Minor	Minor
	802.11 Frame Injection	None	Low	Unlikely	Node	Low	Minor	Minor	Moderate	Moderate	Minor	Minor	Minor	Minor
	Device Cloning	Solvable	High	Likely	Node	Low	Moderate	Minor	Moderate	Moderate	Major	Minor	Major	Major
	Selective Forwarding	None	Low	Unlikely	WAN	Low	Minor	Significant	Minor	Minor	Minor	Minor	Minor	Minor
NFC	Portable reader device theft	None	High	Likely	Node	Moderate	Minor	-	-	Minor	Minor	-	-	Minor
	Clone or modify portable reader device	Solvable	Moderate	Possible	Node	Low	Moderate	-	-	Moderate	Major	-	-	Major
	Capturing the RF signal from distance	Solvable	Low	Unlikely	WAN	High	Moderate	-	-	-	Minor	-	-	-
	Modify or insert data on NFC link	High	Low	Unlikely	WAN	High	-	-	Moderate	-	-	-	Minor	-
	Jam or block RF signal	Solvable	Low	Unlikely	WAN	High	-	Moderate	-	-	-	Minor	-	-
	Corrupt data on RF link	High	Low	Unlikely	WAN	High	-	Moderate	Moderate	-	-	Minor	Minor	-
	Wormhole attack (relay attack)	Solvable	Moderate	Possible	EN	Moderate	-	-	-	Significant	-	-	-	Major
	Destroy, remove or steal node	None	High	Likely	Node	Moderate	-	Minor	-	-	-	Minor	-	-
	Rouge node	Solvable	High	Likely	Node	Low	Moderate	Moderate	Moderate	Moderate	Major	Major	Major	Major
	Unauthorized access to node	Solvable	High	Likely	EN	Low	Significant	-	-	Significant	Critical	-	-	Critical
802.15.4/ZigBee	RF Jamming	None	Low	Unlikely	WAN	Low	Minor	Significant	Significant	Minor	Minor	Minor	Minor	Minor
	Network Flood	None	Low	Unlikely	WAN	High	Minor	Significant	Significant	Minor	Minor	Minor	Minor	Minor
	Rogue Node	None	High	Likely	Node	Moderate	Moderate	Minor	Moderate	Significant	Major	Minor	Major	Critical
	Device Cloning/Firm. replacement	None	High	Likely	Node	Low	Moderate	Minor	Moderate	Significant	Major	Minor	Major	Critical
	802.15.4 Frame Injection	None	Low	Unlikely	WAN	Low	Moderate	Minor	Moderate	Minor	Minor	Minor	Minor	Minor
	Security parameter extraction by physical access	None	High	Likely	WAN	Low	Moderate	Minor	Minor	Significant	Major	Minor	Minor	Critical
	Sinkhole/Black-hole Routing	None	Low	Unlikely	WAN	Low	Minor	Significant	Minor	Minor	Minor	Minor	Minor	Minor
	Selective Forwarding	None	Low	Unlikely	WAN	Low	Minor	Significant	Minor	Minor	Minor	Minor	Minor	Minor
	Network Traffic Analysis	None	Low	Unlikely	WAN	Low	Moderate	Minor	Minor	Minor	Minor	Minor	Minor	Minor
	False Battery Life Extension	None	Low	Unlikely	WAN	Moderate	Minor	Moderate	Minor	Minor	Minor	Minor	Minor	Minor
	False association packets	None	Low	Unlikely	WAN	Moderate	Minor	Significant	Minor	Minor	Minor	Minor	Minor	Minor
	False disassociation packets	None	Low	Unlikely	WAN	Low	Minor	Significant	Minor	Minor	Minor	Minor	Minor	Minor
	False ACK	None	Low	Unlikely	WAN	Low	Minor	Minor	Significant	Minor	Minor	Minor	Minor	Minor
	AES-CTR replay protection	None	Low	Unlikely	WAN	Moderate	Minor	Significant	Minor	Minor	Minor	Minor	Minor	Minor
	AES-CTR packet corruption	None	Low	Unlikely	WAN	Low	Minor	Significant	Minor	Moderate	Minor	Minor	Minor	Minor
	Plaintext key capture	None	High	Likely	WAN	Low	Significant	Minor	Significant	Significant	Critical	Minor	Critical	Critical
	Key capture with SKKE	Solvable	Low	Unlikely	WAN	Low	Significant	Minor	Significant	Significant	Minor	Minor	Minor	Minor
	PANId conflict	None	Low	Unlikely	WAN	Low	Minor	Moderate	Minor	Minor	Minor	Minor	Minor	Minor
	Beacon Synchronization DoS	None	Low	Unlikely	WAN	Moderate	Minor	Significant	Moderate	Minor	Minor	Minor	Minor	Minor
	GTS DoS	None	Low	Unlikely	WAN	Low	Minor	Significant	Moderate	Minor	Minor	Minor	Minor	Minor

6. RESULTS

We performed risk analysis on the identified vulnerabilities. In the ETSI methodology, a threat is ranked as *critical* under the following conditions: if it is likely and has high impact, if it is likely and has medium impact, or if it is possible and has high impact. A threat is only assessed as *major* if it is possible and has medium impact. Based on the ETSI guidelines and the defined risk levels from Table 7, the risk is critical when the attack is likely to happen and its impact is significant. If it is unlikely to happen or its impact is minor, the risk is also minor.

In Table 8 the risk of all identified attacks in each technology is evaluated based on the impact on security objectives and considering the guideline specified in Table 7.

6.1. Wireless LAN

In risk assessment, values assigned to risks needs to be justified. E.g., WEP shared key cracking can be done by eavesdropping to the traffic for few seconds so the difficulty level is chosen solvable. The motivation of this attack is high as it can reveal encrypted information to the attacker which can be valuable. By revealing the shared key, traffic of all nodes connected to that specific AP the key can be decrypted. Detectability and recoverably is chosen moderate as detecting the attack is impossible as it is a passive attack unless the attacker tries to connect to the AP. This attack is recoverable by changing the shared key in all nodes connected to the AP which in some scenarios like IoT might not be a straightforward process. The impact of this attack on the availability and integrity of the communication is also minor.

WPA-PSK key cracking can be easily achieved by capturing hand shake traffic and deploying dictionary attack tools such as Aircrack. The consequence and impact of revealing the shared key is similar to what is mentioned for WEP key cracking attack.

6.2. Near Field Communication

Our risk assessment for NFC is given in Table 8. As a major outcome, unauthorized access to a node via the NFC interface is most critical. This is due to the fact that currently no NFC standards for authentication and access control exist. Henceforth, proprietary application-layer security mechanisms are necessary.

The proximity property of NFC can be circumvented with relay attacks, which are orthogonal to any security protocol and feasible with rather cheap consumer devices. Albeit these attacks typically aim at contactless cards, they might also apply to our industrial use case.

Manipulated readers or rogue nodes pose another major threat. Those devices may be used by an attacker to maliciously interact with the other communication entities.

We see only minor risks for an attack on the actual air link of an NFC connection. Existing literate demonstrates eavesdropping on distances less than one meter [10], only one case reports of ranges up to 2.4 m [11]. Given this rather short distances it is hard for an attacker to stay undetected in real-world industrial scenarios. An adversary always needs to be physically close to its target, and action from a distance is not possible for NFC, so detection is likely by the human operator that is initiating the legitimate NFC communication.

We see no network related issues in NFC links, as communication always takes place between exactly two ends. No network traffic analysis or routing attacks apply henceforth, in contrast to WLAN.

6.3. 802.15.4/ZigBee Communication

The results of the risk assessment for 802.15.4/ZigBee communication is included in Table 8. A few major threats are identified in this table. A rogue node can impact severely on the confidentiality of the network as it can capture communications, compromising confidentiality, data integrity and access control. In the analysis, we consider that a rogue node will not impact availability severely to stay undetected. Device cloning and firmware replacement has similar risk to a rogue node.

Typical installations have communication keys hard-coded into the radio, and these are hardly ever changed. Thus, an attacker with physical access to a device can eventually extract communication keys and other security parameters to seriously impact on confidentiality and access control.

Some installations of 802.15.4 might transfer network keys in plain text, and this is highly unadvisable. One procedure to reduce the complexity of key deployment is to, whenever possible, deploy keys in an out-of-band secure manner.

7. Conclusion

We were interested in improving security assessment methods because traditional M2M systems are now getting integrated with distributed systems and the first step to make such systems secure is to apply security assessment. Therefore we have collected the vulnerabilities of different wireless technologies in the M2M context in threat catalogues and performed a risk analysis on them of which the methodology is based on ETSI guidelines. Our work concentrated on presenting a structured approach, and therefore we limited the description of results for only the most relevant subset of identified threats. In order to identify the most critical risks, it is essential to define the most important security goals and objectives based on the security requirement study. Based on the classification of our example use cases we identify two classes of security objectives:

1. Where confidentiality is the most important security objective such as technical maintenance applications.
2. Where availability is the most important security objectives such as monitoring and sensing applications which cannot tolerate disruption in communication.

We have created and presented a vulnerability catalogue to understand the risks present. We have seen that some of the security risks relate more to the M2M world (e.g. security parameter extraction and modification) while others to the distributed systems world. In the future we aim to create combined vulnerability catalog which would help to understand and analyze the effects of the M2M and distributed system related risks and to find new mitigation methods.

Furthermore a drawback of the used risk assessment method is that it has to be performed manually. In the future we aim to address practical implications to risk assessment to ease its usability.

Acknowledgment

This work was partially supported by Portuguese National Funds through FCT (Portuguese Foundation for

Science and Technology) and by ERDF (European Regional Development Fund) through COMPETE (Operational Programme 'Thematic Factors of Competitiveness'), within project(s) FCOMP-01-0124-FEDER-037281 (CISTER), and by the EU ARTEMIS JU funding, within ARROWHEAD project, ref. ARTEMIS/0001/2012, JU grant nr. 332987 (ARROWHEAD). We would also like to thank Pál Varga for inspiring discussions and guidance.

References

[1] G. Wu, S. Talwar, K. Johnsson, N. Himayat, K. D. Johnson, “M2M: From Mobile to Embedded Internet.” IEEE Communications Magazine, 2011: 36-43.

[2] W. Wang, Zhuo Lu, “Cyber security in the Smart Grid: Survey and challenges.” Computer Networks, 2013: 1344–1371.

[3] S. Kumar, S. Keoh, R. Hummen, R. Struik, “Security Considerations in the IP-based Internet of Things”, Internet-Draft, IETF, 2013.

[4] “Operational Guidelines for Industrial Security”, Siemens AG, 2013

[5] M. Barbeau, “Wireless Security in the Home and Office Environment”, Technical Reports, Carlton University. 2010.

[6] M. Gast, “802.11n: A Survival Guide”, O'REILLY, 2012.

[7] M. Barbeau, “WiMax/802.16 Threat Analysis”, Montreal, Quebec, Canada: Q2SWinet, 2005. 8—15

[8] C. Mulliner, Collin. "Vulnerability analysis and attacks on NFC-enabled mobile phones." Availability, Reliability and Security, 2009. ARES'09. International Conference on. IEEE, 2009.

[9] E. Haselsteiner and K. Breitfuß. "Security in near field communication (NFC)." Workshop on RFID security. 2006.

[10] H. Kortvedt and S. Mjolsnes. "Eavesdropping near field communication." The Norwegian Information Security Conference (NISK). 2009.

[11] R. Zhou and G. Xing. "nShield: A Noninvasive NFC Security System for Mobile Devices."

[12] M. Roland, J. Langer, and J. Scharinger. "Security vulnerabilities of the NDEF signature record type." Near field communication (NFC), 2011 3rd International Workshop on. IEEE, 2011.

[13] G. Hancke. "A practical relay attack on ISO 14443 proximity cards." Technical report, University of Cambridge Computer Laboratory (2005): 1-13.

[14] Z. Kfir and A. Wool. "Picking virtual pockets using relay attacks on contactless smartcard." Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on. IEEE, 2005.

[15] R. Meindl. “NFCIP-1 security standard protects near field communication”, 4th ETSI Security Workshop, 2009.

[16] NFC Forum, “Signature Record Type Definition Candidate Technical Specification”, April 2013.

[17] P. Urien, "LLCPS: A new security framework based on TLS for NFC P2P applications in the Internet of Things." Consumer Communications and Networking Conference (CCNC), 2013 IEEE. IEEE, 2013.

[18] ETSI, “Telecommunications and internet protocol harmonization over networks (TIPHON) release 4; protocol framework definition; methods and protocols for security; part 1: Threat analysis”, Technical Specification ETSI TS 102 165-1 V4.1.1, 2003.

[19] ZigBee Alliance, “ZigBee Specification”, 2012, online: http://www.zigbee.org/Standards/.

[20] ISA100 Standards Committee, “ISA100. 11a, Release 1–An Update on the First Wireless Standard Emerging from the Industry for the Industry”, 2007

[21] Song, J., Han, S., Mok, A., Chen, D., Lucas, M., & Nixon, M., “WirelessHART, Applying Wireless Technology in Real-Time Industrial Process Control”, Real-Time and Embedded Technology and Applications Symposium, (pp. 377-386), 2008

[22] Hui, J. D., “6LoWPAN: Incorporating IEEE 802.15. 4 into the IP architecture. IPSO Alliance”, White Paper, 2009

[23] R. Bradley, T. Morris. "Analysis and mitigation of vulnerabilities in short-range wireless communications for industrial control systems." International Journal of Critical Infrastructure Protection 5, no. 3 (2012): 154-174.

[24] D., Gianluca, M. Tiloca. "Considerations on security in zigbee networks.", In Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), 2010 IEEE International Conference on, pp. 58-65. IEEE, 2010.

[25] N. Sastry, D. Wagner. "Security considerations for IEEE 802.15. 4 networks.". Proceedings of the 3rd ACM workshop on Wireless security. ACM, 2004.

[26] R. Sokullu et al. "An investigation on IEEE 802.15. 4 MAC layer attacks", Proc. of WPMC, 2007.

[27] S. S. Jung, M. Valero, A. Bourgeois, R. Beyah. "Attacking beacon-enabled 802.15. 4 networks", In Security and Privacy in Communication Networks, pp. 253-271. Springer Berlin Heidelberg, 2010

[28] D. Dzung, M. Naedele, T. P. Von Hoff, M. Crevatin, “Security for Industrial Communication Systems”, Proceedings of the IEEE (Volume:93, Issue: 6), June 2005

[29] L. Phifer, “Wireless attacks, A to Z.” *www.techtarget.com.* n.d., online: http://searchnetworking.techtarget.com/feature/Wireless-attacks-A-to-Z.