# Security Aspects of Short-Range Wireless Communication – Risk Analysis for the Healthcare Application

Antti Evesti, Jani Suomalainen, Reijo Savola
*VTT Technical Research Centre of Finland*

## Abstract

*Short-range wireless communication applications have become common nowadays. Healthcare systems based on them hold a remarkable promise for the costly treatment of chronic diseases. Healthcare applications utilize various wireless communication technologies in order to achieve a good connectivity, which is essential in ubiquitous computing. Weak security in wireless networks may ruin the security of the whole application, and even cause life-threatening conditions in healthcare. Therefore, it is of utmost importance to understand risks, threats, possible vulnerabilities and security assumptions made in these technologies. In this paper, we study Bluetooth, ZigBee, NFC, and Wi-Fi from the security point of view in ubiquitous health applications. In the study, we emphasize security aspects starting from the physical communication layer, yet take the needed holistic view to security effectiveness considerations via application of a Risk Analysis process.*

## 1. Introduction

Application of wireless short range network technologies is constantly growing. They make it possible to create easy-to-deploy networks. No predefined and wired infrastructure is needed. In this kind of networks, , new devices, e.g. input devices, sensors and tags, can be configured to be part and can join the network in a flexible and efficient way . In addition, Ubiquitous computing technologies make objects able to connect to each other. In turn, this expands utilisation of various networks. Wireless short range technologies are widely utilised to offer these required network connections. In ubiquitous computing, it is common that device capabilities, communication requirements and application domains vary from a simple temperature measurement to safety critical control systems and health applications.

In the wireless communication, the communication medium is open, and thus, there are not any physical restrictions to transmit or receive communication signals. Hence, two typical threats in the wireless communication are jamming and eavesdropping [1]. In addition, each communication technology contains own specific threats. Lacks in security protocols make devices vulnerable for masquerading, man-in-the-middle and user tracking attacks. Furthermore, it is common that in the short range communication devices are restricted from performance, battery lifetime and input capabilities. These restrictions cause design compromises, which reduce the achieved security. Hence, security weaknesses have to be taken into account when the particular communication technology is applied in applications. Security weaknesses in a healthcare application may ruin users' privacy and in the worst case put users' lives in danger. Hence, risks caused due to the selected communication technique have to be identified and analysed carefully.

This paper studies security challenges of Bluetooth, ZigBee, NFC, and Wi-Fi technologies. In particular, security mechanisms and well-known threats of technologies are described. Based on the study, security implications for health applications that utilize Bluetooth, ZigBee, NFC, and Wi-Fi are discussed by means of the risk analysis. Consequently, the paper results facilitate practitioners to select the most secure communication technique for their purposes. Previous studies have analysed wireless security solutions from different points of view. For instance, Baker compares Bluetooth and ZigBee security in [2] from the industrial perspective. In this study, we start to study security from the physical layer viewpoint and apply risk analysis in the ubiquitous healthcare application.

This article is the extended version of our previously published conference paper [3]. The following extensions are made for the original publication: i) Wi-Fi is included for the analysis. The original version does not contain this communication technique. ii) Risk analysis (RA) section is extended. Now, the risk analysis process experimentally applied in our work is described in more detail. The process contains phases for security objectives, controls and metrics definition, which are not part of classical RA schemes. This extension facilitates practitioners to utilise the process in their own development. Moreover, risk analysis results are now exemplified with possible vulnerabilities, security controls and metrics.

The paper is structured as follows: Section 2 describes background information. Security characteristics of studied technologies are presented in Section 3. Afterwards, Section 4 presents risk

Copyright © 2014, Infonomics Society 

analysis from the communication perspective in the healthcare application. Finally, conclusions close the paper.

## 2. Background

### 2.1 Security in Wireless Communication

Security in short-range wireless networks is based on elements on various layers of communication. Confidentiality, authenticity and integrity are typically secured with cryptographic algorithms and security protocols on physical, link, network or application layers. Availability can be secured on the physical layer with spread spectrum technologies, e.g. frequency hopping and direct sequence spread spectrum, which makes radio signals more difficult to follow, intercept and jam.

Ubiquitous wireless networks consist typically of low-cost devices, including wearable or implantable health sensors and non-medical devices with small batteries and limited UI capabilities. These energy and user interaction restrictions lead to compromises in the security architectures and protocols, e.g. by selecting weaker algorithms or ignoring security in communication. Furthermore, it is challenging to establish security relationships for devices without pre-shared keys or capabilities for inputting passkeys. Consequently, security standards for wireless communication have adopted different security pairing models.

Fortunately, the limited range of wireless communication can offer a security advantage. Intuitively, the attacks, where an attacker must be in close proximity to hear and intercept communication, are more difficult to implement and easier to detect, particularly in controlled physical spaces like homes. On the other hand, proximity can also give a false sense of security as signal-to-noise ratio in longer distances may be underestimated and attackers may invent stealth invasion means. Recently, the research on information-theoretic security has promised new opportunities to achieve high security with low processing costs – without requiring expensive cryptographic algorithms. For instance, secrecy coding [4] and intentional jamming [5] solutions have been proposed for controlling signal-to-noise ratio towards potential eavesdroppers without interfering legitimate transmissions. Further, radio access technologies, such as frequency hopping and interleaving, can be secured by keeping hopping sequences and scrambling keys confidential [6]. Integrity and authenticity can be addressed with distance bounding [7] or RF fingerprinting [8] solutions. Physical proximity of devices and location dependent characteristics of radio signals are used to establish secret keys and trust between devices [9-11].

### 2.2 Ubiquitous health application example

In the ubiquitous environment, the same application is able to utilize various communication techniques. This sub-section presents a motivating example that shows how the Bluetooth, ZigBee and NFC relate to a ubiquitous healthcare application, i.e. a telecare application. The term telecare refers a situation where elderly people are supported with technology in order to support their living at a home as long as possible.

Figure 1 shows an imaginary situation in a home telecare environment. The home environment contains Bluetooth, ZigBee and NFC devices alike, and in addition, the server that maintains devices and connections. ZigBee sensors are utilised for safety purposes, e.g. an occupancy detector to recognize if the occupant has left the house in unusual time. Health monitoring devices collect data from the occupant – the collected data is delivered via the server to a nurse for further analysis. The health monitoring devices can be based on both Bluetooth and ZigBee. For the health monitoring, the occupant identifies herself by means of NFC. This ensures that health data is connected to the right person, e.g. in a situation when a spouse utilizes the same monitoring devices. Furthermore, the environment contains an NFC tag to establish a call for the nurse, which facilitates occupant's possibilities to get help when needed. During the call, the Bluetooth video camera is utilised to offer additional information for the nurse.

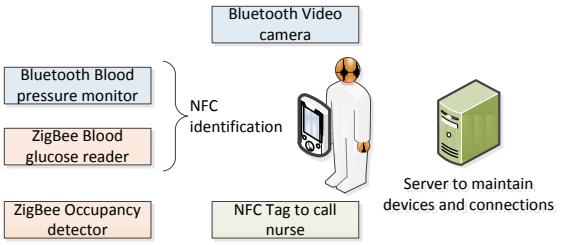


**Figure 1. Example telecare situation**

The home telecare case contains various wireless connections, which together facilitates occupants living in home. However, a security breach in any of these connections is able to cause significant harm. The exposure of medical data or treatment information is a serious privacy violation. Furthermore, inaccurate data, which is manipulated, delayed or originates from the wrong person, is able to cause incorrect diagnosis and treatments. Even minor breaches are able to ruin occupants' and nurses' trust for the system, which reduces the utilisation of the whole system.

Several researchers have defined security requirements (e.g. [12,13]) and frameworks (e.g. [14,15]) for ubiquitous and wireless healthcare

Copyright © 2014, Infonomics Society

applications. However, thorough risk analyses on how well existing ubiquitous technologies (including standards, practical implementations and potential enhancements) would fulfil these requirements are not done.

### 2.3 Systematicity via security metrics

Sufficient Security effectiveness (SE) is the ultimate goal of security work. SE is the assurance that the stated security objectives (SOs) are met in the target system and the expectations for resiliency in the use environment are satisfied, while the system does not behave other than intended [16]. The security controls resulting from SOs and risk management activities should aim at sufficient SE.

Security is very difficult to manage without suitable tools in real-world applications due to the complexity of nowadays's systems, value networks and use scenarios. Models based on security metrics are an effective tool for security engineering and decision-making.

Security metrics should be capable of offering effective evidence of SE. This means that they should express how effectively actual risks are mitigated in the system [17]. Sufficient and high-quality risk knowledge is a pre-requisite for security metrics development. It is not possible to measure security as a whole, but it is feasible to measure factors contributing to it [18]. In [18], we proposed basic and integrated strategies for *security measurement objective decomposition* for top-down risk-driven security metrics development and management. The basic strategies address security configuration correctness, direct partial security effectiveness and software and system quality. The integrated strategies support compliance with best practices and regulations, pure security effectiveness, and security effectiveness tradeoffs.

In ubiquitous health applications, the main security objectives concern authentication at different levels, authorization, data integrity and confidentiality, privacy and availability [19]. Metrics development should address separately end user authentication, sensor authentication, and the service provider user authentication [17]. In the end-user authentication, communication is patient-centric, and includes e.g. paramedic, smart home and mobility scenarios. Service provider user authentication involves use of several communication channels. Privacy measurement in healthcare system is needed because healthcare data is strictly regulated. It should be noted that in some paramedic scenarios, all security objectives cannot fully be met – availability concerns can override them. This should be also reflected to security metrics.

## 3. Security of Bluetooth, ZigBee and NFC

### 3.1 Bluetooth

Bluetooth establishes wireless ad-hoc networks by means of short range radio. The Bluetooth network is called a piconet, which uses a master-slave structure as presented in Figure 2 Bluetooth is applied to connect peripherals to computers and mobile devices. Bluetooth development is started already in 1994. IEEE Standard 802.15.1 [20] covers physical and MAC layers while the Bluetooth specifications [21] cover higher layers in the protocol. The latest core specification version is 4.0, which appeared in 2010. The communication range with the Bluetooth is from 10 cm to 10m (extendable up to 100m). Bluetooth uses 2.4 GHz band with frequency hopping spread spectrum (FHSS) modulation technique. FHSS brings some additional security related to the observation and capturing of communication. However, FHSS cannot be thought as the main countermeasure against eavesdropping because solving the hopping sequence, which is send in clear text, does not require much resources. The Bluetooth uses packet based communication, where each packet contains access code, header and payload. The access code carries the address of the master node. Thus, in the overlapping piconets, where a slave receives two packets, the slave can identify which packet is intended for it by means of the access code.

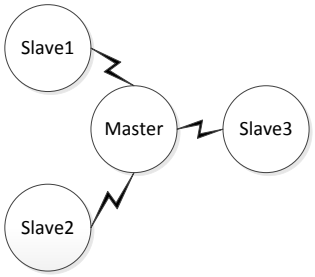


**Figure 2. Bluetooth piconet**

In the Bluetooth, Link Manager Protocol (LMP) manages security features of the Bluetooth link [22]. Consequently, security services are enforced on the link layer. The Bluetooth supports authentication, confidentiality, integrity and authorization security objectives. Authentication of Bluetooth devices bases on challenge-response mechanisms – and it can be utilized to offer one way or mutual authentication of devices. For the authentication purposes, a link key is required, which is established by pairing devices. Secure Simple Pairing (SSP) standard proposes alternative means for pairing by: comparing (or inputting) strings, which devices display; using out-of-band solution (e.g. touching NFC devices); using PIN in legacy devices; or just connecting devices without security checks (unauthenticated

Copyright © 2014, Infonomics Society 

mechanism). The link key is utilised also in encryption to achieve communication confidentiality. In typical implementations, authorisation and trust are closely related in the Bluetooth, i.e. devices are either trusted or untrusted. Trusted devices have full access to services from other devices, whereas each request from untrusted devices must be explicitly authorised by the end-user. [23]

Bluetooth contains four security modes – supported modes vary between Bluetooth versions. Mode 1 does not use any security mechanisms. Mode 2 provides service level security (after link establishment), whereas, mode 3 supports link level security (before link establishment). Lastly, mode 4 supports service level security by utilizing SSP to get the link key. Added to these four security modes, Bluetooth security is affected by three encryption modes and three service security levels. Firstly, encryption mode 1 defines that encryption is not used, while mode 2 defines that communication to particular address is encrypted. Finally, encryption mode 3 enforces encryption to all traffic. In contrast, service security levels focus on authentication and authorization. Level 1 requires authentication and authorization alike, while, in level 2 authorisation is not mandatory. Service security level 3 does not require authentication at all and access is automatic. [23] Hence, Bluetooth contains several models and levels for security. Together these different parameters increase probability of implementation errors that might ruin achieved security.

## 3.2. ZigBee

ZigBee aims to create a network for low data rate and long battery life requirements, e.g. for purposes to send periodic data from a sensor to other device. In ZigBee devices, battery life has to be at least two years. The ZigBee is applied for instance in a home automation and the collection of medical data. The ZigBee network is a mesh network and the communication range is up to 75 meters. The development started in 1998 and its IEEE standard 802.15.4 [24] appeared in 2003. The ZigBee Alliance [25] that defines the ZigBee specification is established in 2004. Two stack profiles for the ZigBee exist, i.e. ZigBee and ZigBee PRO. The first one is intended for home and light commercial usage, while the latter one is intended for situations with higher security requirements.

Figure 3 shows network topologies utilised in ZigBee networks – C denoted a ZigBee coordinator whereas R means a ZigBee router. In the star structure all communication goes through the coordinator. In the tree structure communication goes up and down, while in the mesh structure even the horizontal communication is possible. The ZigBee coordinator is the most capable device with several tasks. For the security purposes, the coordinator acts as a trust centre and stores security keys. The coordinator authenticates joining devices, manages network keys and enables end-to-end security between devices. Added to coordinators and routers, ZigBee network can contain ZigBee end devices, which are the simplest nodes in the network.

ZigBee uses security offered by IEEE 802.15.4, i.e. security for the physical and MAC layers. Standard supports alternative physical layers, providing spread spectrum and thus some potential for making signal interception attacks more difficult. Key definition and management take place in the higher layers defined by the ZigBee Alliance. In ZigBee, replay attacks are mitigated by utilizing counters to check freshness of input /output traffic in each device. Authentication is supported in device and network level alike. The utilisation of common network key supports network level authentication, while, individual devices are authenticated by means of link keys. Communication integrity is supported with Message Integrity Codes (MIC). AES with 128 bit keys is utilised to achieve communication confidentiality. Encryption occurs in the network level and between devices. In ZigBee, the security of network depends on a master key. Thus, achieving the master key threatens the whole network. Moreover, Link keys and Network keys are utilised in the ZigBee network.

Previous studies have investigated ZigBee security from the protocol (IEEE 802.15.4) and manufacturers' implementation viewpoints [26]. The most security risks were found from the manufacturers' implementations, as predictable. The main categories of attacks against ZigBee networks are physical attacks, key attacks and replay / injection attacks. ZigBee supports long battery life but jamming attacks are able to ruin this feature. For example, in [27] Vidgren et al. present how to prevent the utilisation of a sleep mode in order to causes power failures. Moreover, the utilisation of key attacks is presented in [26,27]. Key attacks utilise commercial traffic analysing devices and analysing tools to obtain the network key.

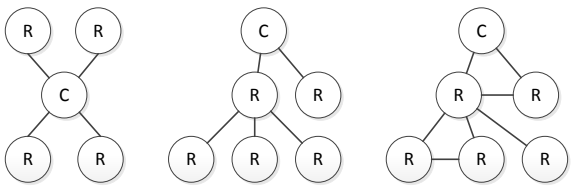


**Figure 3. Star, tree and mesh structures in ZigBee**

## 3.3. NFC

NFC is intended to create a close proximity communication between two devices. The NFC Forum [28] is established in 2004 and it is standardized by ISO/IEC in [29]. NFC bases on Radio-Frequency Identification (RFID) by

Copyright © 2014, Infonomics Society 

supporting a two-way communication. NFC can be utilised to create other connections, e.g. to establish a Bluetooth connection by touching NFC devices. In addition, NFC is applicable for contactless payment, sharing contacts or starting some application by touching a tag. NFC utilises 13.56 MHz radio band and a typical communication range is few centimetres. NFC itself does not contain protection against eavesdropping or message modifications. Consequently, if confidentiality or integrity is required appropriate controls have to exist in the application or physical layer.

In NFC, physical features of RF signal offer some security, i.e. short range and direction of signals. In other words, it is assumed that user is able to notice if the attacker participates to the communication. Several physical layer security solutions have also been proposed to enhance security of NFC communication. To protect confidentiality, solutions controlling eavesdroppers' signal-to-noise ratio with *artificial noise and secrecy coding* have emerged e.g. in [30-32]. Haselsteiner et al. [33] proposed a key extraction solution, which is based on eavesdropper inability to determine direction of NFC transmissions. Active attacks have been addressed in [34] with *distance bounding* protocol and in [35] with *integrity codes.* Distance bounding is based on detecting round-trip delays caused by active man-in-the-middle attackers. Integrity codes use observation that attackers cannot easily change NFC transmitted '1' bits into a '0' and, hence, communication can be coded to detect tampering. *Fingerprinting* methods to detect counterfeits and cloned devices are proposed in [36,37].

Madlmayr et al. [38] describe following seven threat types for the NFC: Denial of Service (DoS), Relay data transferred over the RF, Skimming of applications in the secure element, Managing in-device security, Transactions over NFC peer link, Issues due to the fixed unique ID and Phishing. In other words, absent controls for authentication, integrity and confidentiality are security challenges related to NFC applications. However, from the integrity viewpoint data corruption is much easier than data modification as described in [33]. In [11] Cavoukian describes NFC threats from different usage scenario viewpoints with applicable mitigation techniques. Moreover, author identifies following residual risks: risks arising from modified or misbehaving tag, risks arising from poor application implementation and risks arising from interoperability problems in hardware and platform.

### 3.4. WiFi

Wireless Fidelity (WiFi) is a widely used wireless local area network technology defined by IEEE. WiFi's security specification - WiFi Protected Access 2 (WPA2) [39] – defines authentication procedures and alternative security protocols for confidentiality, authenticity, and integrity.

In WiFi security architecture, an authenticator (typically an access point) controls which supplicants (terminals) are allowed to access the network. In larger multi-user deployments, authenticators can be connected to centralized authentication, authorization, and accounting services. In the WiFi protocol stack, the security mechanisms locate between the medium access control layer and the physical layer. Both unicast and multicast communication can be secured using pairwise and group keys, respectively. Key establishment on smaller networks is based, typically, on pre-shared secrets. Additionally, alternative mechanisms, which have been specified in WiFi Protected Setup (WPS) [40], include: 8 digit PIN entry, 'push button' model, and out-of-band channels such as NFC.

In the early 2000 various vulnerabilities [41] were found from predecessors of WPA2. More recently, weaknesses have been pointed out also in WPA2 and WPS. These include for example, a WPA2 insider attack called 'Hole196') [42] and a brute-force attack against some WPS implementations [43]. Also, as WPS 'push button' mechanism is unauthenticated, it is vulnerable for man-in-the-middle attacks - any nearby device may establish a key with another if the user has conditioned the device by pressing a button. A man-in-the-middle attack succeeds if an attacker can intercept communication from another device so that the base station sees only one device, the attacker, wishing to connect.

In many cases, application and physical layer approaches complement the WiFi security. Application layer approaches provide end-to-end security for long-range connections. In the physical layer, different radio access technologies (such as spread spectrum) have a potential to complicate signal interception and jamming attacks. However, various physical layer attacks have been published (e.g. [44,45]) and physical layer cannot be considered secure. The WPA2 protects only payload part of the communication and leaves identifiers and header information unprotected [46]. Consequently, the use of static cleartext addresses in advertising and registration procedures leaves users vulnerable for tracking attacks. Similarly, unprotected capability and channel state information, which are needed for establishing a wireless channel, make communication vulnerable for interception and denial of service attacks. In the future, new physical layer approaches may be adopted to increase WiFi security including more protected channel establishment [45] and beamforming to control users' and eavesdroppers' signal-to-noise ratios [46].

Copyright © 2014, Infonomics Society 

## 4. Risk analysis

This section describes our RA method and analyses risks in wireless applications. First, the RA method is described in sub-section 4.1. Thereafter, the method is utilized for ubiquitous healthcare application – presented in sub-section 2.2 – in order to analyze its risks.

### 4.1. Applied risk analysis process

The Risk Analysis is a process to find all relevant security risks for a product under the investigation. The Risk Analysis makes it possible to select security controls systematically and with justifications. The most important security concepts for the RA process are presented in Figure 4. An asset (as defined by Common Criteria [47]) is an entity that someone presumably places value upon. Hence, the asset can be almost anything that needs protection. A threat is potential for an accidental or intentional security violation [48]. Threats are enabled by vulnerabilities. Based on [48] a vulnerability can be defined as a property or weakness in a system or its environment that could cause a security failure. Lastly, security controls are a means to protect assets and to support the particular security objective by mitigating risks. For an asset different security objectives are required due to potential threats. Security controls decrease and threats increase the risks

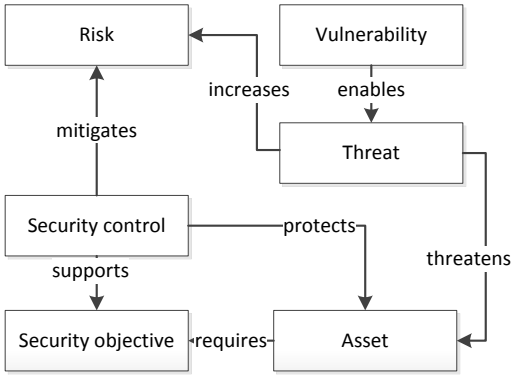


**Figure 4. Concepts**

It should be noted that the literature includes various RA methods, such as [48] and [49]. However, the description of their use for security engineering, security decision-making and security monitoring remains often vague. In the following, we describe our RA process that has been successfully utilized experimentally in our RA projects, enhanced with support for the above-mentioned use.

Figure 5 presents the steps of the risk analysis process. The first step is *Risk identification*. Often, the Risk identification is a brainstorming session where stakeholders with different backgrounds identify risks. It is of utmost importance that risk identification contains technical, business and end-user perspectives. Without all these aspects present at sufficient level, the RA results do not enable informed security decision-making. Conceptually (cf. Figure 4), the Risk identification step produces risks and threats alike.

Next, the identified risks are prioritized. The prioritization is performed by estimating severity and probability of occurrence values for each identified risk, resulting to a risk index estimate. The severity value indicates how serious consequences are if the risk is realized. In contrast, the probability value indicates how often the risk realizes. From the concept viewpoint, the Risk prioritization utilizes information about vulnerabilities and assets (cf. Figure 4). As the final output, the Risk prioritization produces the list of risks in the importance order.

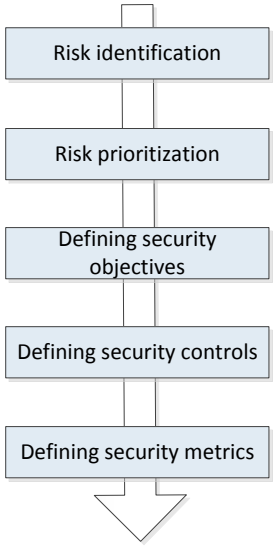


**Figure 5. Risk analysis process**

In the third step security objectives are defined. Security objectives describe what kind of security is required from the system. In other words, objectives are high level security requirements for the system. Security objectives are often classified into confidentiality, integrity, availability, authentication, authorization and non-repudiation categories. The objectives can relate to users (e.g. user authentication), services (e.g. service availability), communication (e.g. communication confidentiality), etc. Security objectives for the system are defined based on risk prioritization results. For instance, the identified risk *Measurement result is modified* may cause the security objective *Data storage integrity*. The security objective definition starts from the most critical risks. However, it is common that risks have interdependencies with each other. A particular challenge is that, risk that has got low priority in the Risk prioritization phase can be an enabler for other more critical risks. Consequently, risk interdependencies have to be analyzed and taken into

Copyright © 2014, Infonomics Society

account during the security objective definition. They should be also revised in an iterative way after the brainstorm-driven RA explained here. Iteration is needed when there are impactful changes in (i) design and implementation information, (ii) use scenarios of the target system, or (iii) the threat landscape.

The fourth step is to define security controls. As depicted in Figure 4 security controls support security objectives, and in addition, protect assets. Consequently, security controls mitigate security risks. On the one hand, security controls can be technical means to support the particular security objective. For instance, the utilization of encryption in the communication supports communication confidentiality. On the other hand, security control can be a process that defines practices how the designed product has to be used. As a simple example, it can be defined that passwords are not written in a paper. Hence, defined security controls are implemented in the designed product, or alternatively, security controls steer the utilization of the product after the implementation.

The last step defines security metrics. By means of the security metrics it is possible to build a feedback loop for the Risk analysis process. Hence, metrics are utilized to recognize residual risks. It is common that all risks are not identified in the first round, or alternatively, defined security objectives do not cover all identified risks. Thus, metrics are intended to recognize deviations between the achieved and required security. The feedback produces by security metrics are utilized in the next risk analyzing round.

## 4.2 RA for ubiquitous healthcare application

We have performed risk analysis for the healthcare application presented in sub-section 2.2. In the risk analysis over 50 security risks were identified – varying from business aspects to specific technologies.

**Table 1. Risks**

| ID | Risk |
|---|---|
| 1 | Risk arising from network failure |
| 2 | Risk arising from DoS |
| 3 | Risk arising from configuration error |
| 4 | Risk arising from data integrity |
| 5 | Risk arising from improper access control |
| 6 | Risk arising from authentication problems |
| 7 | Information disclosure |

Table 1 lists risks from the network viewpoint. The majority of risks are enablers for other risks, i.e. other risks arise due to the network risks. Examples of security vulnerabilities, countermeasures and security metrics related to these risks in wireless networks can be found from Table 2.

The risk analysis reveals that the properly working network is the backbone for the ubiquitous healthcare application. Therefore, risks arising from network failures are in the first priority. Several reasons are able to cause network failures, and thus, it is difficult to eliminate this risk as the whole. Hence, it is mandatory to include mechanisms to detect and recover from network failures. In a telecare application detecting network failures remotely is more reasonable mitigation technique for network failures than building a redundancy, which cause unreasonable costs for patients.

DoS (called jamming in lower network layers) is also a critical risk. This risk might be realized in lower or higher network layers. In the higher layers, server is loaded heavily, and thus legitimate users are not able to get service. In contrast, jamming in the lower layers causes that the communication channel is reserved and devices are not able to send data. In addition, active attacker might follow and jam frequency hopping of a communication channel. Bluetooth and ZigBee act in the same frequency band, and thus, in theory an appropriate jamming device prevents the utilisation of both networks. Similarly, Bluetooth and ZigBee devices are able to affect each other, as well as other devices acting in the same frequency band. However, an intentional jamming attack requires a modified device, which reduces a probability of this risk. On the other hand, Bluetooth or ZigBee device can be utilised for critical monitoring purposes, which in turn increases consequences of risk realization. For the ZigBee devices DoS / jamming attacks are able to ruin battery lifetime, which causes power failures. In contrast, preventing jamming in NFC is difficult. NFC contains a collision detection mechanism, which helps to recognize jamming. However, this does not help a user whose NFC bandwidth is reserved when she tries to get help via the healthcare application.

Risk #3 relates to configuration errors. Bluetooth and ZigBee contain various configuration parameters and key management issues. Improper network configuration may cause that achieved security is lower than required, or alternatively, sensors send measurement data for a wrong server etc. In order to decrease the probability of configuration errors applications and updates have to be tested thoroughly.

Copyright © 2014, Infonomics Society 

**Table 2. Examples of Vulnerabilities, Controls and Metrics for Risks in Wireless Networks**

| Risks | Example s of vulnerabilities | Examples of security controls | Metric examples |
|---|---|---|---|
| Network failure | - Incompatible implementations or protocols<br>- Hardware issues | - Redundancy<br>- Detecting network failures remotely | - Statistics on frequency, duration and costs of network failure |
| DoS | - Wideband jamming<br>- Unprotected MAC layer headers enabling unauthenticated queries and revealing device capabilities<br>- Unprotected physical channel information enabling jamming of particular user channel / data<br>- Unintentional interference | - Spread spectrum and frequency hopping techniques<br>- Physical layer security mechanisms (information theoretic secrecy)<br>- Jamming detection | - Work required to jam / intercept communication? (‘jamming’ bits / bandwidth)<br>- Consequence of unauthenticated request (consumed processing time / battery power)<br>- Attacker positioning – direction and distance of attack transmissions |
| Configuration error | - Security policy configuration mechanisms (application layer) enabling insufficient security | - Easy and tested configuration mechanisms<br>- Educating users | - Incident statistics – e.g. rate of reported policy configuration errors (incidents/year) |
| Data integrity | - Vulnerabilities in security protocol (e.g. WEP, WPA and earlier Bluetooth versions) | - Cryptographic protocols | - Entropy of secret keys (bits) |
| | - Known vulnerabilities against insiders | - Pair-wise security, reliable key management, user authentication<br>- Security logs | - Incident statistics (e.g. incidents/year) |
| Improper access control | - Application layer issues in access control | - Mechanisms for enforcing access control and defining access policies | - Statistics on found security vulnerabilities enabling breaches<br>- Statistics on reported policy configuration errors (incidents/year) |
| Authentication problems | - Brute force attacks (e.g. vulnerability in WPS PIN model)<br>- Replay injection attacks<br>- Support for weak legacy security protocols (bidding down attacks) | - Mature authentication mechanisms | - Best known attacks against authentication protocols (calculations needed to break a crypto key passively or amount of active guesses)<br>- Entropy of secret keys (bits) |
| | - Bogus base stations and man-in-the-middle attacks (e.g. due to unauthenticated pairing models such as WPS ‘push button’ model) | - Intrusion detection solutions (e.g. identifying devices by fingerprinting wireless signals) | - Accuracy of intrusion detection system to fingerprint attacker’s hardware or location (false positive and false negative %) |
| | - Improper credential management (e.g. weak WiFi passwords) | - Advanced pairing mechanisms<br>- Policies enforcing password quality | - Entropy of identifiers and secret keys (bits) |
| Information disclosure | - Unprotected physical and link layer information enabling interception of particular user data<br>- Vulnerabilities in security protocol<br>- Insider attacks<br>- Privacy attacks - tracking use of unprotected identifiers | - Cryptographic protocols<br>- Physical layer secrecy mechanisms (e.g. information theoretic secrecy via beamforming or artificial noise)<br>- Device or application specific access control mechanisms | - Secrecy rate – amount of information that can be transmitted securely (bits/s)<br>- Overhead due to security i.e. total bandwidth – secrecy rate (bit/s)<br>- Attack visibility (is attacker forced to actively communicate or are passive attacks possible)<br>- Physical layer assumptions – e.g. eavesdropper’s distance from transmitter or receiver (cm)<br>- Entropy of secret keys – the amount of information in a key depends on the size of the key and quality of random sources (bits) |

Risk arising from data integrity may also have various consequences. For instance, nursing staff do not get the correct opinion from the patient, or alternatively, alarms are not triggered. Bluetooth and ZigBee contain mechanisms for communication integrity, whereas NFC does not support it. In NFC data corruption is much probable integrity problem than data modification [33]. This is due to challenge to change the particular bit from the wireless signal. Similarly, in Bluetooth and ZigBee it can be assumed that message modification during the communication is quite unlikely. To avoid integrity risk arising from the physical layer it is reasonable to utilise integrity checking in higher network layers.

Improper authentication and access control are source for several risks with varying consequences. Investigated techniques do not concentrate on user’s authentication or access control. Instead means to authenticate and authorize communicating devices and networks are available in Bluetooth and ZigBee. In contrast, NFC does not support these security objectives as such, but those can be offered by

Copyright © 2014, Infonomics Society 

utilising higher layers from the communication stack. In the usage example in the sub-section 2.2 it is reasonable to authenticate tags in order to avoid bogus tags with a harmful functionality.

Lastly, the risk of information disclosure relates also for the short range communication. In the healthcare applications, transmitted data contains privacy related medical information. Consequently, the communication confidentiality has to be ensured. Again, Bluetooth and ZigBee contain supporting mechanisms. However, appropriate configuration is required. The lack of communication confidentiality in NFC is not a problem in the presented case due to intended communication does not contain medical data.

## 5. Discussion and future work

The communication techniques analysed in this paper are widely utilised in ubiquitous computing and its applications. Viable communication techniques are essential building blocks for ubiquitous computing and its applications. Nowadays, the ubiquitous applications are utilised also in critical applications like healthcare. Therefore, security requirements of applications are getting more attention. In a ubiquitous computing the utilised communication technique influences potential risks and achieved security. It is not enough to consider performance, battery life time, price, etc., but security implications have to be also perceived. Consequently, the software designer has to take security into account when selecting the communication technique. Firstly, supported security objectives and known vulnerabilities set restrictions for the selection. Thereafter, other aspects can be utilised to categorise different techniques. For example, maturity, known use cases with the communication technique, updating frequency and availability/openness for security assessments. However, it is probable that one technique is not able to fulfil all requirements in the ubiquitous environment – as visible in the example in the sub-section 2.2. Therefore, it is reasonable to combine different communication techniques to one application. In that case, it is important to explicitly define how each technique will be used and what information is transmitted. Applying various communication techniques makes it possible to select the most suitable solution for each communication situation. Nevertheless, applying more than one communication technique is also able to affect negatively for the achieved security, e.g. interferences of signals. However, this risk is minor compared to its advantages and can be minimised by means of proper testing.

In this paper, we utilised our applied risk analysis process for the ubiquitous health application. Risk analysis process ensures that security controls are selected systematically and justification for each selection is visible. The prioritisation of risks facilitates to concentrate the most critical risks at first. It is possible to perform risk analysis in a general level for the designed product – before any communication technique is selected. However, mapping identified risks to communication techniques makes it possible to compare techniques. This kind of analysis result is valuable information for the security designer.

From the viewpoint of lower network layers, studied technologies do not offer much support for security, i.e. Bluetooth, ZigBee, NFC or Wi-Fi do not contain security mechanisms in the physical layer. In other words, support for security objectives is built in higher layers – starting from the protocol definitions. One reason for this is that supporting all security objectives by means of physical layer mechanisms is not possible. On the other hand, some risks can be also realized from the application layer. For instance, the utilisation of default passwords is a remarkable risk even on the lower layers but which cannot be mitigated by means of physical layer mechanisms. Hence, an appropriate password change policy on the application layer is able to increase security on the lower layers also. Therefore, as the cross-cutting quality, security has to be supported through all layers in order to achieve security in the ubiquitous application.

From the ubiquitous computing viewpoint, Bluetooth, ZigBee and NFC are reasonable techniques. Each technique can be applied in the ubiquitous applications as long as known security restrictions are taken into account already at design-time and compared to the requirements from the application domain. For example, in ZigBee wake-up time is shorter and battery life-time longer than in Bluetooth, which supports its utilisation in applications that require this kind of availability. In all cases it is reasonable to utilise minimum communication ranges and directed antennas in order to minimise outsiders' possibilities to recognise wireless traffic.

## 6. Conclusions

We analysed security challenges and solutions of Bluetooth, ZigBee, NFC, and Wi-Fi technologies. The focus of the analysis was lower network layers. According to the analysis, the main threats at the physical layer are jamming and eavesdropping. However, it is visible that these communication techniques do not offer physical layer mechanism to mitigate these threats. On the other hand, these threats can be mitigated by utilising upper layer mechanisms. Bluetooth, ZigBee, NFC, and Wi-Fi are widely applied in various ubiquitous computing applications.

Copyright © 2014, Infonomics Society 

In addition, we carried out a risk analysis for a healthcare application, which utilises above mentioned communication techniques. Risk analysis revealed that risks arising from networking are enablers for other risks, and thus, it is vital to mitigate recognised risks. The risk analysis method applied was also described. The method includes application of its results to security engineering, decision-making and monitoring via use of security metrics.

## 7. Acknowledgements

The work presented here has been carried out in three research projects: PHYLAWS – PHYsical Layer Wireless Security FP7 project, ASSET – Adaptive Security for Smart Internet of Things in eHealth project, and SASER-Siegfried Celtic-Plus project (2012–2015). The projects are funded by the European Commission, The Research Council of Norway, Tekes – the Finnish Funding Agency for Technology and Innovation and VTT Technical Research Centre of Finland. We wish to thank our colleagues involved in these projects for their helpful discussions and comments.

## 8. References

[1] Yi-Sheng Shiu; Shih-Yu Chang; Hsiao-Chun Wu; Huang, S. C. -.; Hsiao-Hwa Chen. Physical layer security in wireless networks: a tutorial. Wireless Communications, IEEE 2011, 18, 66-74.

[2] Baker, N. ZigBee and Bluetooth strengths and weaknesses for industrial applications. Computing & Control Engineering Journal 2005, 16, 20-25.

[3] Evesti, A.; Suomalainen, J.; Savola, R. Security Risks in the Short-range Communication of Ubiquitous Application. In Proceedings of the 9th International Conference for Internet Technology and Secured Transactions (ICITST), London UK, 9-12 December, 2013.

[4] Bloch, M.; Barros, J. Physical-Layer Security: From Information Theory to Security Engineering, Cambridge University Press 2011.

[5] Negi, R.; Goel, S. Secret communication using artificial noise. In Proceedings of the 62nd Vehicular Technology Conference, Dallas, Texas, 25th-28th September, IEEE, 2005, pp. 1906-1910.

[6] Asif Khan, M.; Jeoti, V.; Shahid Manzoor, R. Secure Interleaving - Physical Layer Security Enhancement of OFDM Based System. In Proceedings of the 1st International Conference ICeND 2011, Dar-es-Salaam, Tanzania, 3rd-5th August, Springer Berlin Heidelberg, 2011, pp. 349-361.

[7] Brands, S.; Chaum, D. Distance-Bounding Protocols. In Proceedings of the Advances in Cryptology - Workshop on the Theory and Application of Cryptographic Techniques, Lofthus, Norway, 23rd-27th May, Springer Berlin Heidelberg, 1994, pp. 344-359.

[8] Ureten, O.; Serinken, N. Wireless security through RF fingerprinting. Canadian Journal of Electrical and Computer Engineering **2007,** 32, 27-33.

[9] Mathur, S.; Miller, R.; Varshavsky, A.; Trappe, W.; Mandayam, N. ProxiMate: proximity-based secure pairing using ambient wireless signals. In Proceedings of the MobiSys´11, Bethesda, Maryland, USA, 28th June - 1st July, ACM, 2011, pp. 211-224.

[10] Varshavsky, A.; Scannell, A.; LaMarca, A.; Lara, E. Amigo: Proximity-Based Authentication of Mobile Devices. In Proceedings of the 9th International UbiComp Conference, Innsbruck, Austria, 16th-19th September, Springer Berlin Heidelberg, 2007, pp. 253-270.

[11] Cavoukian, A. Mobile Near Field Communications (NFC) "Tap ´n Go" Keep it Secure & Private. **2011,** 1-19.

[12] Meingast, M.; Roosta, T.; Sastry, S. Security and Privacy Issues with Health Care Information Technology. In Proceedings of the 28th Annual International Conference of the Engineering in Medicine and Biology Society, New York, USA, 30th August - 3rd September, IEEE, 2006, pp. 5453-5458.

[13] Ameen, M.; Liu, J.; Kwak, K. Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. J.Med.Syst. **2012,** 36, 93-101.

[14] Garcia-Morchon, O.; Falck, T.; Heer, T.; Wehrle, K. Security for pervasive medical sensor networks. In Proceedings of the 6th Mobile and Ubiquitous Systems: Networking & Services, Toronto, Canada, 13rd-16th July, IEEE, 2009, pp. 1-10.

[15] Kotz, D.; Avancha, S.; Baxi, A. A privacy framework for mobile health and home-care systems. In Proceedings of the SPIMACS´09, Chicago, USA, 13rd November, ACM, 2009, pp. 1-12.

[16] National Institute of Standards and Technology - Jansen, W. Directions in Security Metrics Research. **2009**.

[17] Savola, R. M.; Abie, H. Metrics-driven security objective decomposition for an e-health application with adaptive security management. In Proceedings of the International Workshop on Adaptive Security & Privacy Management for the Internet of Things (ASPI´13), Zurich, Switzerland, 8th September, ACM, 2013, pp. 6:1-6:8.

[18] Savola, R. M. Strategies for security measurement objective decomposition. In Proceedings of the Information Security for South Africa (ISSA), Johannesburg, Gauteng, 15th-17th August, IEEE, 2012, pp. 1-8.

[19] Savola, R. M.; Abie, H.; Sihvonen, M. Towards metrics-driven adaptive security management in e-health IoT applications. In Proceedings of the BodyNets '12, Oslo, Norway, 24th-26th September, ICST, 2012, pp. 276-281.

Copyright © 2014, Infonomics Society 

[20] IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements. - Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs). IEEE Std 802.15.1-2005 (Revision of IEEE Std 802.15.1-2002) **2005,** 0_1-580.

[21] Bluetooth Specification. https://www.bluetooth.org/en-us/specification/adopted-specifications, 2013, Accessed April/22 2013.

[22] Siva Ram Murthy, C.; Manoj, B. S. Ad Hoc Wireless Networks Architectures and Protocol, Prentice Hall 2004.
23. Padgette, J.; Scarfone, K. Guide to Bluetooth Security. NIST. **2011,** .

[24] IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs). IEEE Std 802.15.4-2011 (Revision of IEEE Std 802.15.4-2006) **2011,** 1-314.

[25] ZigBee Alliance. http://www.zigbee.org/, Accessed April/22 2013.

[26] Bowers, B. ZigBee Wireless Security: A New Age Penetration Tester's Toolkit. http://www.ciscopress.com/articles/article.asp?p=1823368, 2012, Accessed 05/22 2013.

[27] Vidgren, N.; Haataja, K.; Patino-Andres, J. L.; Ramirez-Sanchis, J. J.; Toivanen, P. Security Threats in ZigBee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned. In Proceedings of the 46th Hawaii International Conference on System Sciences, Wailea, USA, IEEE, 2013, pp. 5132-5138.

[28] NFC Forum. http://www.nfc-forum.org/home/, Accessed April/25 2013.

[29] ISO/IEC 18092:2013 Information technology -- Telecommunications and information exchange between systems -- Near Field Communication -- Interface and Protocol (NFCIP-1). **2013,** 1-44.

[30] Castelluccia, C.; Avoine, G. Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags. In Proceedings of the 7th IFIP WG 8.8/11.2 International Conference CARDIS´06, Tarragona, Spain, 19-21 April, Springer Berlin Heidelberg, 2006, pp. 289-299.

[31] Savry, O.; Pebay-Peyroula, F.; Dehmas, F.; Robert, G.; Reverdy, J. RFID Noisy Reader How to Prevent from Eavesdropping on the Communication? In Proceedings of the Cryptographic Hardware and Embedded Systems - CHES 2007, Vienna, Austria, 10-13 September, Springer Berlin Heidelberg, 2007, pp. 334-345.

[32] Chai, Q.; Gong, G. BUPLE: Securing Passive RFID Communication through Physical Layer Enhancements. In Proceedings of the 7th International Workshop, RFIDSec, Amherst, USA, 26th-28th June, Springer Berlin Heidelberg, 2012, pp. 127-146.

[33] Haselsteiner, E.; Breitfuß, K. Security in near field communication (NFC) - Strengths and Weaknesses. In Proceedings of the Workshop on RFID Security, Graz, Austria, 12-14 July, 2006, pp. 11.

[34] Hancke, G. P.; Kuhn, M. G. An RFID Distance Bounding Protocol. In Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks, Athens, Greece, 5th-9th September, IEEE, 2005, pp. 67-73.

[35] Capkun, S.; Cagalj, M.; Rengaswamy, R.; Tsigkogiannis, I.; Hubaux, J.; Srivastava, M. Integrity Codes: Message Integrity Protection and Authentication over Insecure Channels. Transactions on Dependable and Secure Computing **2008,** 5, 208-223.

[36] Danev, B.; Heydt-Benjamin, T. S.; Capkun, S. Physical-layer Identification of RFID Devices. In Proceedings of the USENIX Security Symposium, Montreal, Canada, 10th-14th August, 2009, pp. 199-214.

[37] Periaswamy, S. C. G.; Thompson, D. R.; Jia Di. Fingerprinting RFID Tags. Transactions on Dependable and Secure Computing **2011,** 8, 938-943.

[38] Madlmayr, G.; Langer, J.; Kantner, C.; Scharinger, J. NFC Devices: Security and Privacy. In Proceedings of the Third International Conference on Availability, Reliability and Security, 2008, Barcelona, Spain, 4-7 March, 2008, pp. 642-647.

[39] IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements. http://standards.ieee.org/getieee802/download/802.11i-2004.pdf, 2004, .

[40] Wi-Fi Alliance. Wi-Fi Protected Setup. Web site. http://www.wi-fi.org/knowledge-center/faq/how-does-wi-fi-protected-setup-work, Accessed January / 31 2014.

[41] Tews, E.; Beck, M. Practical Attacks Against WEP and WPA. In Proceedings of the Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16-18 March, ACM, 2009, pp. 79-86.

[42] Ahmad, S. WPA Too! http://www.defcon.org/images/defcon-18/dc-18-presentations/Ahmad/DEFCON-18-Ahmad-WPA-Too-WP.pdf, 2010, Accessed January / 31 2014.

[43] Viehböck, S. Brute forcing Wi-Fi Protected Setup - When poor design meets poor implementation. http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf, 2011, Accessed January / 31 2014.

[44] Bellardo, J.; Savage, S. 802.11 Denial-of-service Attacks: Real Vulnerabilities and Practical Solutions. In Proceedings of the 12th Conference on USENIX Security Symposium - Volume 12, Washington, DC, USENIX Association, 2003, pp. 2-2.

Copyright © 2014, Infonomics Society 

[45] Clancy, T. C. Efficient OFDM Denial: Pilot Jamming and Pilot Nulling. In Proceedings of the International Conference on Communications (ICC), Kyoto Japan, 5-9 June, IEEE, 2011, pp. 1-5.

[46] Romero-Zurita, N.; Ghogho, M.; McLernon, D. Physical layer security of MIMO–OFDM systems by beamforming and artificial noise generation. Physical Communication 2011, 4, 313.

[47] ISO/IEC 15408-1:2009 Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, International Organization of Standardization 2009.

[48] Stoneburner, G.; Goguen, A.; Feringa, A. Risk management guide for information technology systems. Special publication 800-30 **2002,** 1-41.

[49] ISO 31000:2009. Risk Managament – Principles and Guidelines. International Organization for Standardization.

Copyright © 2014, Infonomics Society 