Security aspects of ubiquitous computing in health care

E. Weippl, A. Holzinger, A. M. Tjoa

Today, ubiquitous devices lack many of the security features known in desktop computing, an industry that is known to have a plethora of security problems. As ubiquitous devices are increasingly applied in the health care industry, security aspects need to receive even more attention. Clearly, patient-related data is extremely sensitive and legal requirements (such as HIPAA) attempt to enforce strict privacy controls. While we cannot solve the overall problem, our proposal to use RFID tags to authenticate users with ubiquitous devices addresses one of the most fundamental requirements of all security mechanisms: to reliably establish the user's identity. In this paper we discuss some questions that raised during experiments with ubiquitous devices at Graz University Hospital. The main problems which could be identified included security and privacy issues (protection precautions, confidentiality, reliability, sociability). The experiments showed that new and emerging computer technologies such as mobile, ubiquitous and pervasive computing have an enormous potential for the improvement of manifold workflows in health care, however, psychological and technological research must be carried out together in order to bring clear benefits for the end-users and to optimize workflows in health care in the daily routine.

Keywords: mobile devices; security; health care; RFID

Sicherheitsaspekte von Ubiquitous Computing im Gesundheitsbereich.

Sicherheitsmechanismen, die in PCs heute als Standard vorausgesetzt werden, fehlen in vielen mobilen Geräten. Da mobile Geräte zunehmend im Gesundheitsbereich eingesetzt werden, gewinnen Sicherheitsaspekte an Bedeutung. Daten von Patienten und Krankenakten sind ganz offensichtlich sensible Daten, die sowohl durch technische als auch durch gesetzliche Maßnahmen geschützt werden müssen. Authentifikation ist eine Grundvoraussetzung für alle weiteren Sicherheitsmaßnahmen. Unser Vorschlag ist, RFID für die Authentifikation bei mobilen Geräten zu verwenden. In dieser Arbeit diskutieren die Autoren prototypische Entwicklungen, die am AKH Graz durchgeführt wurden. Der Fokus lag auf Aspekten der Sicherheit und Vertraulichkeit. Versuche haben gezeigt, dass neue Technologien das Arbeitsumfeld massiv verändern können und dass Vorteile nur durch eine enge Einbindung von Endbenutzern zum Tragen kommen. Täglich anfallende Arbeitsprozesse können dann effizienter und sicherer gestaltet werden.

Schlüsselwörter: mobile Geräte; Sicherheit; Gesundheitssystem; RFID

1. Introduction

Increased interoperability between systems and ever larger networks has leveraged the need for security. As networked devices shrink in size and use expands in industries such as health care, ubiquitous security has become a new and vitally important area of research (*Mazzola, 2003; Paul et al., 2004*) that encompasses both technical aspects as well as the human aspect (*Russell, Streitz, Winograd, 2005*).

Ignoring mobile devices, there are technical solutions to almost all security problems. However, there are obviously many security-related problems in non-mobile computing but the root cause is mostly of organizational nature – the weak point is nearly always the user as the many social engineering attacks (*Mitnick, Simon, 2002*) showed. For instance, LoveLetter was one of the most successful worms. It did, however, not propagate by itself. The user always had to open the attachment which then executed the unwanted code. Today, phishing is an extremely common problem that solely works because users trust emails and enter confidential data on a hacker's web site. As Mitnick (*Mitnick, Simon, 2002*) showed, social engineering is a very successful way of attacking any computer system. Wegner and Doyle realized that HCI and usability will be of major importance in mobile devices some years before mobile devices became so common (*Wegner, Doyle, 1996*).

With mobile computing the situation is different. Mobile devices are usually small and processing power is constrained by batteries. Slow processors, small displays and little or no keyboards render mobile devices a totally different platform as non-mobile computing. While security is certainly perceived as relevant requirement, devices such as PDAs still lack many security features that are well-known in desktop or laptop computers.

In this paper we

- highlight and summarize basic threats to security in mobile devices (Section 3),
- show how these threats influence the adoption of mobile devices in the health industry in which security and privacy of patient data is essential (Section 4).

Prior to looking at the specifics of mobile security, we will state the definitions of the key security requirements used (*Avizienis et al., 2001, 2004*) throughout this paper. Security requires confidentiality (aka secrecy), integrity and availability (CIA). All other requirements such as non-repudiation can be traced back to one of these three requirements. Non-repudiation, for instance, can be seen as a special case of integrity, i.e. the integrity of log data recording who has accessed which object.

Weippl, Edgar R., Univ.-Ass. Mag. Dipl.-Ing. Dr., Vienna University of Technology, Favoritenstraße 9-11, 1040 Wien, Austria; **Holzinger, Andreas, Univ.-Doz. Ing. MMag. Dr.**, Medical University of Graz, Auenbruggerplatz 2/4, 8036 Graz, Austria; **Tjoa, A Min, O. Univ.-Prof. Dipl.-Ing. Dr.**, Vienna University of Technology, Favoritenstraße 9-11, 1040 Wien, Austria (E-Mail: weippl@ifs.tuwien.ac.at, andreas.holzinger@meduni-graz.at, tjoa@ifs.tuwien.ac.at)

The perhaps most well known security requirement is *confidentiality*. It means that users may obtain access only to those objects for which they have received authorization, and will not get access to information they must not see.

The *integrity* of the data and programs is just as important as confidentiality but in daily life it is frequently neglected. Integrity means that only authorized people are permitted to modify data (or programs). Secrecy of data is closely connected to the integrity of programs of operating systems. If the integrity of the operating system is compromised, then the integrity of the data can no longer be guaranteed. The reason is that a part of the operating system (i.e. the reference monitor) checks for each access to a resource whether the subject is authorized to perform the requested operation. Since the operating system is compromised the reference monitor is no longer trustworthy. It is then obvious that secrecy of information cannot be guaranteed any longer if this mechanism is not working. For this reason it is important to protect the integrity of operating systems just as properly as the secrecy of information.

It is through the Internet that many users have become aware that *availability* is one of the major security requirements for computer systems. Availability is defined as the readiness of a system for correct service.

2. Why mobile devices are insecure

Some of the benefits that mobile computing offers are essential for the healthcare industry as the major part of nurses' and doctors' work requires them to go to patients. Their work style cannot be changed so that they work behind a desk using a stationary computer. Holzinger (*Holzinger, Nischelwitzer, Meisenberger, 2005; Holzinger, Schwaberger, Weitlaner, 2005*) reports on successfully using mobile and ubiquitous devices in e-learning and e-work, however, there is still much research to do in order to successfully using ubiquitous devices in clinical workflows. IT systems in health care that are located at the fixed terminal are inefficient because the necessary information will not be available at the time of query and that will interrupt the workflow (*Eisenstadt et al., 1998*). Healthcare providers would like to enter information in the patient record and process information at the point of care to save time and minimize entry errors (*Reuss et al., 2004*).

The inherent properties of mobile devices are the root cause of their security issues. As the term ''mobile devices'' indicates they are portable. Due to the form factor they have limited resources. Unfortunately, the current practice when addressing resource limitations is to ignore well-known security concepts. For instance, to empower WML scripts, implementations lack the established sandbox model; thus downloaded scripts can access all local resources without restriction (*Ghosh, 2001*).

Since mobile devices are mobile, they are used to being connected to various networks which are usually not trustworthy. In addition, mobile devices are usually connected to wireless networks that are often easier to compromise than their wired counterparts. Moreover, the devices are usually personal devices (personal digital assistant PDA) and therefore people store a lot of personal information on them, even though the operating systems usually offer little protection for the privacy of data (*Chou, Chang, Jiang, 2000*).

Their portability clearly makes mobile devices subject to loss or theft (*Halpert, 2004*). Once a mobile device has been stolen or lost, the thief or other unauthorized individuals are likely to gain direct access to the data stored on the device.

Another, completely different risk is caused by Trojan devices, which means that a stolen device is copied and a Trojan device is returned to the user. Thus attackers are able to access the recordings of all the actions performed by the user (*Weippl, 2005*).

One of the most important mechanisms to implement the basic CIA requirements is access control. For access control to work effectively, the identity of the user has to be established reliably. A common way of identification and authentication is the combination of a user name and a password. The user has to identify herself entering the password and prove her identity (i.e. authenticate herself) with a password. Other forms of authentication are either token-based or use biometrics.

Currently user authentication is one of the weakest points with mobile devices. Since the devices usually lack a keyboard, a screen saver that requires entering a password is too cumbersome to use. Several other forms of authentication have been proposed but are not widely used. For instance, users can unlock their PDA by tapping on a point on an image[1].

In this paper we propose a very simple and yet very effective solution to improve mobile security by using RFID tags. Since RFID tags are increasingly used for physical access control to and within buildings, we propose to implement user authentication for mobile devices with RFID. Compared to other approaches of wireless user authentication (e.g. using Bluetooth), RFID has several advantages. The most important one is that RFID tags can be externally powered and thus users do not yet have another device which needs to be recharged.

3. Threats to mobile devices

In this section we will elaborate on security threats to mobile devices. Since mobile devices are used to being connected to wireless networks the first subsection addresses communication security. The second subsection looks at the security of the device itself. More details can be found in (*Weippl, 2005*).

3.1 Communication security

Mobile devices are mostly used to communicate and thus securing this process is a first step. Mobile devices usually connect to wireless networks. Most security threats in this subsection are not limited to mobile devices; instead they pertain to wireless communication technologies where certain new aspects arise compared to wired networks (*Mahan; Rueckert et al., 2002*). Clearly, wireless communication technology is most relevant for mobile devices.

Denial of service (DoS) is the opposite of availability. A system or a network may become unavailable to legitimate users, or services offered are interrupted or delayed. In a wireless network a DoS attack can also be launched by jamming the wireless channel with a strong external signal.

One can distinguish between two meanings of *interception*. First, an external user can masquerade himself as a legitimate user and so gain access to confidential data. Second, the data stream itself can be intercepted during transmission. Therefore data encryption and authentication of communication partners is essential. WEP encryption is clearly not an option because of its inherent weaknesses. Even 128 bit WEP encryption can be broken in less than 30 minutes. Tools are widely available on the Internet.

Manipulation of data is a serious threat. When data is modified on a system or during transmission, a Trojan horse or a virus could be inserted. To avoid manipulation access to the network it needs to be protected.

The process when an unauthorized user or external source impersonates as legitimate user is referred to as *masquerading.* Strong authentication can be used to prevent masquerading attacks.

Repudiation is when a user can plausibly deny having performed an action on the network. Strong authentication of users, integrity assurance methods for data and log files and digital signatures are used to minimize this threat.

[1] http://picturepassword.com

3.1.1 Wireless LAN (IEEE 802.11)

Wireless LAN (WLAN) specifies two security services: (1) authentication and (2) privacy service, both handled by the wired equivalency privacy (WEP). Many papers on the weaknesses of the WEP standard have been published such as Borisov (*Rueckert et al., 2002*), but the 802.11 standardization committee responded (*Kelly, 2001*) that WEP was never intended to offer more protection than a physically protected (i.e. wired) LAN. WEP, however, is so weak that it can easily be decrypted by anyone who runs the widely available free software to intercept the traffic and decrypt the traffic such as Airsnort. A better choice is to use WPA or a Radius server (802.1x[2]). Unfortunately many mobile devices do not yet support these protocols.

3.1.2 Bluetooth

In the Bluetooth generic access profile (GAP[3]), the basis on which all other profiles build, three security modes are defined (*Gehrmann, 2002*).

In security mode 1, a device will not require any security mechanisms – this is the non-secure mode. In security mode 2, the Bluetooth device initiates security procedures after the channel is established (at the higher layers), while in security mode 3, the Bluetooth device initiates security procedures before the channel is established (at the lower layers). At the same time two possibilities exist for the device's access to services: ''trusted device'' and ''untrusted device''. Trusted devices have unrestricted access to all services. Untrusted devices do not have fixed relationships and their access to services is limited. There are three security levels for services are defined. (1) services that require authorization and authentication, (2) services that require authentication only and (3) services that are open to all devices. These levels of access are obviously based on the results of the security mechanisms themselves. Details on how security is handled on these levels can be found in (*Daid*). Although Bluetooth design has focused on security, implementations still suffer from vulnerabilities, such as bluebugging, bluesnarfing or car whispering[4]. Bluejacking, in contrast, is not a technical vulnerability but it uses the correct implementation of sending business cards for social engineering attacks.

3.1.3 GSM, GPRS, UMTS

The security of digital wireless wide-area networks (WAN) depends on the protocols used. Details on GSM, GPRS, HSCSD, etc. can be found in (*Gruber, Wolfmaier, 2001*).

User identification and authentication is first and foremost required to enable billing services to the correct user (*Hansmann, Nicklous, 2001; Walker, Myrick, 1985*). Secondly, the transmitted data must be protected for privacy reasons. Since GSM and GPRS are still widely used standards, we will look at these standards.

A unique device ID (IMEI international mobile equipment identity) is used to identify the hand set regardless of the SIM card used. A second unique ID is assigned to the SIM card. The SIM card is assigned a telephone number and, in addition, can usually store data such as short message service (SMS) or phone numbers.

As the cell phone connects to the network, the two unique IDs are transmitted. Based on these IDs a decision is made whether to permit the device access to the network. This decision is based on whether the device is white-listed, gray-listed or black-listed.

Once the phone has a connection, the user is authenticated. Each subscriber is issued a unique security key and a security algorithm. Both are stored in the operator's system and in the mobile device's SIM card. When accessing the network for the first time, the security system of the network sends a random number to the mobile device. The mobile device encrypts this random number with its security key and algorithm and returns it to the network. Subsequently, the security system of the network performs the same calculations and finally compares the result to the number transmitted by the mobile device. If both numbers match, the authentication process is completed successfully. Since random numbers are sent each time, replay attacks are not possible. In addition, the secret keys are never transmitted over the network (*Constantinos, Sotirios, Iakovos, 2003*).

Cryptography is not only used during the authentication process but the transmission of data may also be encrypted. Once a connection is established, a random session key is generated. Based on this session key and a security algorithm, a security key is generated. Using this security key and yet another security algorithm, all transmitted data are encrypted. Each connection is encrypted with a different session key. Even if this concept seems secure, there are various vulnerabilities as discussed, for instance, by Pesonen (*Pesonen, 1999*).

3.2 Device security

In this section we will look at the security of the device. Gollmann (*Gollmann, 1999*) defines computer security as dealing with ''*prevention and detection of unauthorized actions by users of a computer system*''.

3.2.1 Physical protection

Mobile devices are small and can be stolen easily. Various anti-theft devices such as steel cables and holsters can be used to secure the devices at the cost of making them less mobile.

3.2.2 Authentication

Authentication on the mobile device establishes the identity of the user to the particular mobile device. Most of the available mobile devices do not support any authentication mechanisms other than passwords and PINs. Some offer fingerprint sensors but they are not widely used and obvious drawbacks are that they cannot be operated with gloves.

Some products are already available that provide personal digital assistants (PDAs) with enhanced security features. For instance, PDASecure[5] and Password Safe[6] support password-based encryption for data. Some iPAQs such as the hx2700 come with built-in finger print sensor.

OneTouchPass[7] offers an image-based way of authentication. When the device is switched on, an image is displayed. The user authenticates by tapping on the previously specified places in the picture. The level of security offered by this program is similar to passwords; however, since the process of authentication is faster, more people are likely to use it. Hence, overall security may be improved.

3.2.3 Access control

As the name *personal* digital assistant suggests, a PDA is in most cases used by one person only. That said, access to data should still be restricted according to a policy for access control. In some cases, users may share devices or allow coworkers to access certain entries (business vs. personal). Most of the mobile devices do not provide sophisticated access control that goes beyond the distinction personal vs. business data.

[2] http://picturepassword.com

[3] https://www.bluetooth.org/spec/

[4] http://www.bluetooth.com/help/security.asp

[5] http://www.pcguardiantechnologies.com/PDASecure/

[6] http://www.schneier.com/passsafe.html

[7] http://www.onetouchpass.com

3.2.4 On-device encryption

Authentication and access control may not suffice to protect highly sensitive corporate or private data stored on a mobile device. A common attack is to circumvent the access control mechanisms provided by the device. It thus makes sense to encrypt sensitive data. The encrypted files are in most cases protected by a password. As mobile devices often have no or only a small keyboard, entering good passwords is cumbersome.

3.2.5 Anti-virus software

Installing anti-virus software is a standard security procedure for all corporate and most private computers and laptops. Anti-virus software is also available for mobile devices. It is expected that in the future more malicious software will be distributed that specifically targets handheld devices (*Leavitt, 2005*). Nonetheless, just as anti-virus software developers generally keep up with new virus developments within hours, we expect similar success for anti-virus software for mobile devices.

3.2.6 Application security

It is not sufficient to protect the mobile device itself and the wireless communication protocols. In addition, precautions are also required on an application level. There is extensive literature on how to improve software in order to avoid common security vulnerabilities (*Howard, LeBlanc, 2002; Swiderski, Snyder, 2004; Whittaker, 2003; Whittaker, Thompson, 2003*).

4. Mobile devices in health care

Increasing computerization and recent regulatory changes are putting new pressures on healthcare information management.

In today's hospital, IT is ubiquitous. At a medium-sized patient-care facility, visitors first encounter the admissions system, which not only tracks the admission of patients and their subsequent healthcare, but also monitors the availability of beds and care facilities. In the individual wards and clinics are arrays of terminals at nursing stations, where nurses and technicians monitor the patients' vital signs using data collected by biomedical equipment in each room. Physicians walk by entering notes and updates on personal digital assistants (PDAs). Pharmacists fill prescriptions, check for drug interactions, and maintain inventory control using online pharmacy systems. In some facilities, doctors use telemedicine to diagnose and treat patients in remote locations. Across facilities, the medical records and billing system tracks patients' progress and provides the data necessary for filing insurance claims.

Ironically, despite the current reliance on IT, healthcare was one of the last major industries to be computerized. The industry didn't accept the electronic medical record (EMR) until the mid-1990s, for example. Although it is tempting to blame computer-phobic physicians, the industry had many valid reasons for its resistance. The electronic patients record (EPR) integrates the patients' medical history, admissions information, diagnosis, and treatment plan, and it enables online billing transactions with insurers. It includes both written data and the medical images used for diagnosis. These characteristics call for stringent privacy, security, and verification requirements, which until recently, no fully automated system could meet. Moreover, the industry lacked standards for electronic documentation, which slowed the adoption of online insurance claims processing (*Jepsen, 2003*).

During experiments in various settings at Graz University Hospital (*Holzinger, Schwaberger, Weitlaner, 2005*) some problems have been identified, including immobility, inefficient user interfaces and navigation or misidentification, using the approach of ubiquitous computing (UC) – which, in the classical sense of Mark Weiser, enhances the use of computers by making many computers available throughout the physical environment, whilst making them effectively invisible to end-users (*Weiser, 1993*). Consequently, the research focused not only on technological, but on user-centered feasibility research and the development of ubiquitous computing demonstrators, taking *social issues* of real-work requirements and consequences into consideration. This combination of psychological and technological research enabled to assist enhancing applications with the idea of UC to reduce problems and generate new improvement potential in health care. Published research work describes improvements and existing infrastructure of ubiquitous computing in hospitals (*Bardram, Christensen, Olsen, 2002; Bardram, 2004*). However, most of this infrastructure has been extensively tested in the labs but is *not deployed in hospitals* (*Bardram, 2003*). One exception we found is the approach of Siemens in the Jacobi Medical Center in New York (see http://www.sbs-usa.siemens.com/press/docs/jacobimedical-casestudy.pdf). Similar to that approach, we performed customized and user-centered development within Graz University Hospital, which is amongst the largest hospitals in Europe.

4.1 Main issues

During our work three problem areas concerning security issues emerged:

1) protection precautions,
2) confidentiality,
3) integrity.

4.1.1 Protection precautions

We identified following problems. First, unprotected tags are clearly vulnerable to eavesdropping, traffic analysis, spoofing and denial of service. The properties making RFID attractive also make it vulnerable. The second and often discussed privacy concern is the tracking of individuals by RFID tags (Privacy and Customer Pushback), (*Weis et al., 2004; Want, 2004; Knospe, Pohl, 2004*). A possible solution is to read only a UID, and to lock all other data including uncritical information. ISO 15693 specifies these locks; in addition, all sensitive and security relevant data can be stored on secure server.

Fundamental information security objectives, such as confidentiality, integrity, availability, authentication, authorisation, nonrepudiation and anonymity are often not achieved unless special security mechanisms are integrated into the system.

4.1.2 Confidentiality

Usually, the communication between reader and tag is unprotected, with the exception of some high-end systems, such as ISO 14443. Consequently, eavesdroppers can listen in if they are in immediate vicinity. However, the forward channel from the reader to the tag has a longer range and is more at risk than the backward channel (*Weis et al., 2004*).

4.1.3 Integrity

With the exception of high-end ISO 14443 systems which use message authentication codes (MACs), the integrity of transmitted information cannot be assured. Checksums (cyclic redundancy checks, CRCs) are often used, however, they can protect only against random failures. The writable tag memory can be manipulated if access control is not implemented.

4.2 Additional security issues

4.2.1 Availability

Any RFID system can easily be disturbed by frequency jamming. Denial-of-service attacks are also feasible on higher communication layers.

4.2.2 Authenticity

The authenticity of a tag is at risk since the unique identifier (UID) of a tag can be spoofed or manipulated. The tags are in general not tamper resistant.

4.2.3 Anonymity

The unique identifier can be used to trace a person or an object carrying a tag in time and space. This may not even be noticed by the traced person. The collected information can be merged and linked in order to generate a person's profile.

4.3 Security mechanisms

Effective security mechanisms can provide protection against the described problems, however, we must take into account that the primary purpose of the RFID technology is the realization of cheap and automated identification. Thus, standard security mechanisms can hardly be implemented because of their relative complexity compared with the constrained tag computing resources (AES, SHA-1) and efficient public-key protocols like NTRU are too elaborate for low-cost tags (*Weis et al., 2004*)

4.3.1 Access control and authentication

Some tags implement access control mechanisms for their read/write memory. Access to the UID is mostly unrestricted, and the strength of memory access control procedures varies a lot (e.g. nothing, clear text password, challenge-response protocol). Current RFID tags do usually not protect the unique identifier which raises the above mentioned problems. Some tags (in particular ISO 14443) enforce authentication mechanisms before granting read or write access to specific memory blocks.

In practice a password authentication or a unilateral or bilateral challenge-response authentication (e.g. ISO 9798-2) with symmetric keys is realized. For part 4 of the ISO 15693 standard a challenge-response authentication protocol with DES or 3DES is proposed. High-end transponders which comply with ISO 14443-4 can also employ application level authentication like contact smart cards.

The security and privacy risks induced by the unprotected tag identifier gave reason to a number of contributions and protocol propositions.

One common option is to destroy (kill) the tag after it has been used (*Sarma, Brock, Engels, 2001*); a password protected 'destroy' command has also been integrated into the electronic product code (EPC) specifications.

There is an RFID blocker tag (*Juels, Rivest, Szydlo, 2003*) available, which exploits tag singulation (anti-collision) protocols in order to interrupt the communication with all tags or tags within a specific ID range. The blocker works for the most relevant anti-collision protocols (tree walking and ALOHA) and may be used for privacy protection but it can also be misused for mounting denial-of-service attacks.

(*Juels et al., 2003*) proposes also a system of multiple tag pseudonyms which renders tracking by external entities more difficult. Only authorized entities can link the different pseudonyms.

(*Ishikawa et al., 2003*) propose that the tag emits only an 'anonymous EPC'. A back-end security centre then delivers the clear text electronic product code (EPC) over a secure channel to authorized entities. In an extended version, the readers can send a reanonymising request to the security centre which generates a new 'anonymous EPC'. The tag is then updated with this ID.

(*Weis et al., 2004*) propose a 'hash-based access control protocol'. The tag is first in a 'locked' state and transmits only a 'Meta ID' which is the hash value of a key. An authorized reader looks up the corresponding key in a backend system and sends it to the tag. The tag verifies the key by hashing it, returns the clear text ID and remains only for a short time in an 'unlocked' state. This would provide reader authentication and a modest level of access security. Privacy would still be at risk when the 'meta ID' remains constant over time. Hence, (*Weis et al., 2004*) proposed a 'randomized access control' in another mode of operation where tags respond with a randomized hash value. Since the reader would have to compute hash values for all possible IDs, this mode would only be feasible with a small number of tags.

(*Engberg et al., 2004*) argue that privacy and security enhancements should be adapted to the RFID tag lifecycle; prior to being sold, an article can be tracked by supply chain management. As soon as the item is under the control of the customer, the customer should be able to decide how the tag is used. The tag should also be used for recycling and waste management once the product's life span is reached.

They propose a solution to the RFID privacy problem through zero knowledge (bilateral) authentication protocols which are based on a shared secret and use hash and XOR operations. At the point of sale, the tag changes from the ''ePC'' (electronic product code) mode to the privacy mode and a new authentication key – only known to the customer and the tag – is produced and stored. When returning the product for recycling, the privacy mode can be disabled and the tag returns to the original ''ePC'' mode. (*Avoine et al., 2004*) describe the multi-layer aspects of the privacy problem. It may not be sufficient to ensure privacy on the application layer. Lower layers also have to be considered. On the data link layer, a unique identifier is required for deterministic singulation (collision avoidance) protocols. Even on the physical layer the radio fingerprint can distinguish a single tag.

4.3.2 Tag authentication

There are also proposals for protocols which authenticate the tag to the reader and protect against tag counterfeiting. (*Vajda et al., 2003*) propose and analyse several lightweight tag authentication protocols. (*Feldhofer, 2004*) proposes the simple authentication and security layer (SASL) protocol with AES encryption and analyzes the hardware requirements.

4.3.3 Encryption and message authentication

Some high-end RFID systems (ISO 14443 and MIFARE® based) are able to encrypt and authenticate the data traffic with proprietary protocols. Since data exchange apart from identifiers does not play a major role for RFID systems, secure messaging is often not regarded as a key issue. Encryption of memory blocks may be realized on the application layer, which is transparent for the RFID tag. The unique identifier (UID) is usually read-only and many RFID-transponders (e.g. ISO 15693 or 18000-3 tags) permit a permanent write lock of memory blocks.

5. Conclusion

As some experiments with ubiquitous devices showed, security in ubiquitous computing in health care is of vital importance. The main security problems encompass three issues: 1) protection precautions, 2) confidentiality, 3) integrity.

Compared to active wireless technologies such as Bluetooth, RFID is much better suited for authentication purposes because it requires no separate power source. It is essential to have working prototypes at hand as early as possible to demonstrate the possibilities, to show these possibilities in experimental settings and in order to raise awareness amongst the end-users and amongst the executives, regarding the medical director and the executives of the hospital information system. Based on input from a various group of end-users, the prototype can then be subsequently adapted, iterated and reconfigured. Finally the prototype has to be tested in various real-life settings. However, most of the problems are not in technology – but in human issues, concerning awareness amongst both the end-users and the executives.

It is essential to take social issues of real work requirements and consequences into consideration. Only a combination of psychological and technological research enables to assist enhancing applications with the idea of ubiquitous computing to reduce problems and generate new improvement potential in health care. All our results show, that much research in the area of human-computer interaction (HCI) and usability engineering (UE) with pervasive and ubiquitous devices must be carried out and it will take a while to bring RFID solutions within the hospital into the daily routine.

References

Avizienis, A., Laprie, J.-C., Randell, B. (2001): Fundamental concepts of computer system dependability. Paper presented at the IARP/IEEE-RAS Workshop on Robot Dependability: Technological Challenge of Dependable Robots in Human Environments, Seoul, Korea.

Avizienis, A., Laprie, J.-C., Randell, B., Landwehr, C. (2004): Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions of Dependable and Secure Computing, 1 (1): 11–33.

Bardram, J. (2003): Hospitals of the future – ubiquitous computing support for medical work in hospitals. Paper presented at the 2nd Int. Workshop on Ubiquitous Computing for Pervasive Healthcare Applications.

Bardram, J. E. (2004): Applications of context-aware computing in hospital work: examples and design principles. Paper presented at the 2004 ACM Symposium on Applied Computing, Nicosia (Cyprus).

Bardram, J., Christensen, H., Olsen, A. (2002): Activity-driven computing infrastructure – pervasive computing in healthcare. Paper presented at the Pervasive 2002.

Chou, C., Chang, Y.-F., Jiang, Y.-Y. (2000): The development of an online adaptive questionnaire for health education in Taiwan. Computers & Education, 35 (3): 209–222.

Constantinos, F. G., Sotirios, I. M., Iakovos, S. V. (2003): Introduction of the asymmetric cryptography in GSM, GPRS, UMTS, and its public key infrastructure integration. Mob. Netw. Appl., 8 (2): 145–150.

Daid, M.: Bluetooth Security, Parts 1, 2, and 3. http://www.palowireless.com/bluearticles/cc1_security1.asp. Unpublished manuscript.

Eisenstadt, S. A., Wagner, M. M., Hogan, W. R., Pankaskie, M. C., Tsui, F.-C., Wilbright, W. (1998): Mobile workers in healthcare and their information needs: are 2-way pagers the answer? Paper presented at the 1998 AMIA Annual Symposium, Orlando (FL).

Gehrmann, C. (2002): Bluetooth security white paper. https://www.bluetooth.org/foundry/sitecontent/document/security_whitepaper_v1.

Ghosh, A. K., Swaminatha, T. M. (2001): Software security and privacy risks in mobile e-commerce. Communications of the ACM, 44 (2): 51–57.

Gollmann, D. (1999): Computer security. John Wiley & Sons.

Gruber, F., Wolfmaier, K. (2001): State of the art in wireless communication (SCCH-TR-0171). Software Competence Center Hagenberg.

Halpert, B. (2004): Mobile device security. Kennesaw: ACM Press.

Hansmann, M., Nicklous, S. (2001): Pervasive computing-handbook. Springer Verlag.

Holzinger, A., Nischelwitzer, A., Meisenberger, M. (2005): Mobile phones as a challenge for m-learning: examples for mobile interactive learning objects (MILOs). Paper presented at the Proc. of the 3rd Int. Conf. on Pervasive Computing and Communications Workshops (PerCom 2005 Workshops).

Holzinger, A., Schwaberger, K., Weitlaner, M. (2005): Ubiquitous computing for hospital applications RFID-applications to enable research in real-life environments. Paper presented at the UbiComp in HC, CompSAC.

Holzinger, A., Schwaberger, K., Weitlaner, M. (2005): Ubiquitous computing for hospital applications: RFID-applications to enable research in real-life environments. 29th Int. Computer Software & Applications Conference (IEEE COMPSAC): 19–20.

Howard, M., LeBlanc, D. (2002): Writing secure code (2nd ed.). Microsoft Press.

Jepsen, T. (2003): IT in healthcare: Progress Report. IT PROFESSIONAL, 5 (1): 8–14.

Juels, A., Rivest, R. L., Szydlo, M. (2003): The blocker tag: selective blocking of RFID tags for consumer privacy. Paper presented at the Proc. of the 10th ACM Conf. on Computer and Communications Security.

Kelly, S. (2001): Chair of IEEE 802.11 Responds to WEP Security Flaws.

Knospe, H., Pohl, H. (2004): RFID security. Information Security Technical Report, 9 (4), 39–50.

Leavitt, N. (2005): Mobile phones: the next frontier for hackers. IEEE Computer, 38 (4): 20–23.

Mahan, R. E. (2001): Security in wireless networks, SANS Institute. http://rr.sans.org/wireless/wireless_net3.php.

Mazzola, M. (2003): Interview. Queue, 1 (3): 12–16.

Mitnick, K. D., Simon, W. L. (2002): The art of deception. Controlling the human element of security. John Wiley & Sons.

Paul, D., Grinter, E., Delgado de la Flor, J., Joseph, M. (2004): Security in the wild: user strategies for managing security as an everyday, practical problem. Personal Ubiquitous Comput., 8 (6): 391–401.

Pesonen, L. (1999): GSM interception. Dpt. of Computer Science and Engineering: Helsinki University of Technology.

Reuss, E., Menozzi, M., Buchi, M., Koller, J., Krueger, H. (2004): Information access at the point of care: what can we learn for designing a mobile CPR system? Int. Journal of Medical Informatics, 73 (4): 363–369.

Rueckert, L., Deravanesian, A., Baboorian, D., Lacalamita, A., Repplinger, M. (2002): Pseudoneglect and the cross-over effect. Neuropsychologia, 40 (2): 162.

Russell, D. M., Streitz, N. A., Winograd, T. (2005): Building disappearing computers. Communications of the ACM, 48 (3): 42–48.

Sarma, S., Brock, D., Engels, D. (2001): Radio frequency identification and the electronic product code. IEEE MICRO, 21 (6): 50–54.

Swiderski, F., Snyder, W. (2004): Threat modelling. Microsoft Press.

Walker, N. W., Myrick, C. C. (1985): Ethical considerations in the use of computers in psychological testing and assessment. J. School Psychol. 23 (1): 51–57.

Want, R. (2004): The magic of RFID: just how do those little things work anyway? ACM Queue, 2 (7): 40–48.

Wegner, P., Doyle, J. (1996): Editorial: strategic directions in computing research. ACM Comput. Surv., 28 (4): 565–574.

Weippl, E. R. (2005): Security in e-Learning. Heidelberg: Springer.

Weis, S. A., Sarma, S. E., Rivest, R. L., Engels, D. W. (2004): Security and privacy aspects of low-cost radio frequency identification systems. In: Hutter, D. (ed.): Security in pervasive computing. Heidelberg. LNCS 2802: 201–212.

Weiser, M. (1993): Some computer science issues in ubiquitous computing. Communication of the ACM, 36 (7): 75–84.

Whittaker, J. (2003): Why secure applications are difficult to write. IEEE Security & Privacy (2): 81–83.

Whittaker, J. A., Thompson, H. H. (2003): How to break software security. Addison Wesley.