

Security, Privacy and Legal Issues in Pervasive eHealth Monitoring Systems

Frank Kargl,
Institute of Media Informatics,
Ulm University
89069 Ulm, Germany
frank.kargl@uni-ulm.de

Elaine Lawrence, Martin Fischer,
Yen Yang Lim
University of Technology Sydney
Broadway 2007 NSW, Australia
elaine|fischer@it.uts.edu.au
brian.lim@uts.edu.au

Abstract

In this paper we analyze the security and privacy requirements of eHealth monitoring systems which use wireless sensor networks. Based on our experience developing our eHealth system, ReMoteCare, we have devised a model of such systems which we use to discuss threats and attacks, address security requirements and give guidelines for security mechanisms. The contentious issues of privacy of medical data are canvassed – especially as there are legal ramifications if personal health information is compromised.

1. Introduction

In this paper the authors analyze the security and privacy implications of *Pervasive eHealth Monitoring Systems* (PEMS). Under this term we subsume all kinds of IT systems that constantly monitor human bio-signals for the purpose of medical analysis or diagnostics in a mobile and everyday environment. This is a contrast to traditional monitoring where patients are usually only subjected to short term monitoring (e.g. by a doctor) or are attached to large monitoring devices which restrict patient mobility significantly (e.g. being in the intensive care unit at a hospital).

PEMS need components that monitor human bio-signals like pulse, oxygen saturation level, or ECG. In order to be pervasive these devices must be small enough to be carried around without too much disturbance to the person's regular activities. This implies size and weight limits which restrict the kind of sensors you can use, and also prevents usage of cabling for power supply or data transmission.

When looking at existing PEMS, there are two kinds of major applications: The first concerns systems

that perform pure *local data collection, storage, and analysis*. The collected data stays in the mobile device and can either be used to trigger an alarm based on some local data analysis to detect critical situations or it can be stored and downloaded e.g. whenever the patient consults his doctor for later offline analysis. Note however that at the moment of data collection, there is no data transmission of any kind.

In contrast, the second application category uses *online transmission of data for remote alarm or for remote data collection and data analysis*. In this case, data is not only collected and analyzed locally, but is also sent to some remote entity with better capabilities for data storage and analysis. The data can, for example, be stored in a data warehouse, be analyzed by resource-intensive algorithms or even be monitored by medical staff.

All these options are not available in a pure local system. Given these clear advantages, the analysis presented here is exclusively focusing on the second approach which can be regarded as a superset of the pure local approach.

There are a variety of PEMS, some of which are even already commercially available, whereas others are still at the stage of early research. Many of the existing systems rely on some mobile computer, smart phone, or PDA that queries the sensors, pre-analyzes the data and might then trigger a remote alarm or send some of the data to a specialist. Projects or products include the Personal Health Monitor system **Error! Reference source not found.** and the products of eHit from Finland [2].

Another approach that recently gained attention in the scientific community is the use of Wireless Sensor Network (WSN) technology for PEMS. WSNs are made up of miniaturized computers, called motes, that contain elements of computation, storage, wireless communication and sensing. The big advantage is the

extremely small size of the motes (in the order of 2 AA batteries or smaller) and the fact that they have a very low energy consumption, so the monitoring devices may run days or weeks without maintenance or recharge. That way they become really ubiquitous, because integration in everyday objects like clothes, rings, or eyeglasses can be envisioned. People will be carrying and using the devices almost without noticing. The WSN nodes will virtually disappear.

A drawback is that these devices usually have very limited user-interface capabilities and no displays, so local interaction with the device is restricted to simple alarms or button-presses. Furthermore, local computing resources are very limited. The purpose here is clearly to rely on remote systems for analysis and reaction. Given that only trained personnel should interpret medical data, this might even be a reasonable approach.

Examples of this class of PEMS include CodeBlue [3], BigNurse [4], MoteCare [5] and our latest prototype 'ReMoteCare' [9].

Although the presented systems open up significant opportunities for future health-care, they also collect and process very sensitive personal information. This includes not only the medical data itself, but also location data that is collected during wireless communication, and other data derived from medical data. For example, having access to constant monitoring of heart-rate and oxygen saturation, may allow unscrupulous persons to deduce the time, whereabouts and amount of sports activities of a person. A possible scenario could be a rival sporting team spying on an opponent's team to gain a competitive advantage.

Furthermore, large scale data collection also opens the door for abuse of this data. Unauthorized collection and use of this data (e.g. by insurances) represent significant privacy breaches. Modification of the data may lead to false alerts of paramedics. Nobody wants his location to be traceable around the clock. So when designing PEMS, security and privacy risks definitely need to be considered.

It is the purpose of this paper to analyze and classify possible misuse of different system components and to derive guidelines for secure and privacy-friendly design of PEMS. Section 2 outlines the system model we have developed and give a brief overview of ReMoteCare. Threats and attacks on such systems are outlined in Section 3. Security and privacy issues for eHealth monitoring systems are discussed in Section 4. Section 5 highlights related work whilst the conclusions and future directions for developing secure and privacy-friendly solutions are found in Section 6.

2. System Model

Before discussing security and privacy we initially suggest a comprehensive model of WSN-based PEMS to substantiate the system under discussion. As shown in Figure 1 the system consists of some or all of the following components:

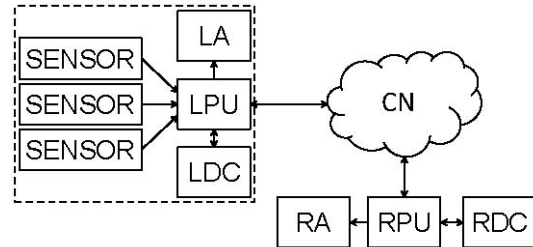


Figure 1. System Model for WSN-based Pervasive eHealth Monitoring Systems

Sensor: captures the medical data and transfers it to the local processing unit.

Local Processing Unit (LPU) processes data from this and other units, sends it to RPU.

Local Data Collection (LDC): stores the data for later retrieval and analysis.

Local Actuator (LA): provides the possibility of triggering a local action, e.g. ringing an alarm.

Communication Network (CN): allows the communication between motes and between motes and the RPU.

Remote Processing Unit (RPU): receives data from motes and processes/analyzes this data.

Remote Data Collection (RDC): stores data for analysis and later reference.

Remote Actuator (RA): provides the possibility for triggering an action, e.g. sending an email to a doctor.

Note that the capabilities of the remote components usually exceed that of the motes by magnitudes, allowing for example, more complex analysis algorithms, storage of huge amounts of data, or communication via the Internet for triggering alarms. From a security point of view, securing the remote components is much easier, as traditional and heavy-weight security mechanisms like SSL can be applied and the components can be placed in physically protected environments. Motes, on the other hand, can only apply light-weight security mechanisms such as TinySec and are subject to tampering or even being stolen.

Another important issue when discussing the security and privacy of PEMS is the scale of their

deployment. We consider three different scenarios here:

Individual home monitoring: One person (or a small group of persons like a family) uses PEMS to monitor personal health levels. Both local and remote components belong to this person. Data is only made available to other persons under certain conditions, for example when visiting a doctor or in case of alarms and only to a predetermined audience, such as the personal doctor or an emergency unit.

Hospital monitoring: A larger group of people, such as patients in a hospital, is monitored by a PEMS. Data is gathered centrally and constantly accessible to a limited range of persons for example doctors and nurses.

Large-scale monitoring: This can mean that a whole population (e.g. of a state or country) uses PEMS and the data is collected centrally, for example by the medical authority. Although this scenario sounds unlikely, there are a number of arguments why it might be implemented in the future. Assessing the public health on a large scale base allows detailed predictions of future medical therapy requirements and costs. This might also save costly screenings. Instead only people showing certain early symptoms of a specific disease would be requested to undergo an examination. Other scenarios for large-scale monitoring include potential pandemics like bird flu. A population wide monitoring facility could provide vital information and lessen the effects dramatically. Therefore having medical data available on a large-scale offers opportunities but also poses severe security and privacy risks.

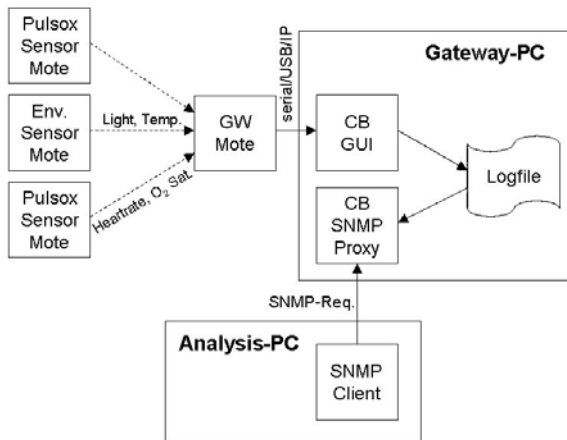
2.1 RemoteCare:

The model of our PEMS prototype called ReMoteCare is illustrated in Fig. 2 below. Full details on the architecture and analysis of ReMoteCare are given in [9] and [10].

As can be seen, ReMoteCare represents a typical PEMS in the sense of the definition given above. The sensors, LPU, and LDC are all combined into motes. There are currently no LAs. The sensor nodes gather data and communicate over a communication network (CN) either directly or via multi-hop ad-hoc networking (not shown) with a gateway, which then collects data and presents it for local or remote analysis (using SNMP protocol in case of ReMoteCare). The RPU/RDC/RA components are split over the gateway- and analysis-PC. Using SNMPv3 supports both

encryption and provides end-to-end point security [3, 7] in the RPU/RDC/RA subsystem.

Figure 2: Architecture of ReMoteCare.



3. Threats and Attacks

In this section, we discuss threats and attacks in respect to different types, different attacker models, and based on the components attacked. Finally we discuss the impact of deployment scale on the gravity of attacks.

3.1. Types of Attacks

A list of different attacks is by nature incomplete as constantly new types of attacks are developed and some cannot be envisioned before the system is implemented and deployed. However, it is likely that some of the attacks that are found in today's systems or that are considered for future ubiquitous computing systems will also appear in PEMS:

Eavesdropping on medical data: As medical data is collected, transmitted and stored throughout the system, attackers can try to access that data. One example is the unauthorized snooping on radio communication between motes and subsequent recording of data. As medical data is personal and very sensitive to abuse, this needs to be prevented.

Modification of medical data: When attackers are able to modify medical data while it is being collected, transmitted, or during storage, incorrect patient records and false system reactions may be the result. This can create either false positives like triggering false alarms and lead e.g. to unnecessary rescue missions. Even worse, false negatives (i.e. modifying alarming data into regular result) can hide abnormal or emergency situations.

Forging of alarms on medical data: Similar to the previous point, attackers can simply create fake messages instead of modifying regular ones. This can again lead to wrong data records or false system

reaction like rescue teams being sent to help a non-existent person.

Denial of Service: Jamming or overloading the system can render the system unusable. In a worse case scenario sick or injured people are not given the assistance required.

Location tracking of users: As a user of a PEMS leaves a constant trace of messages sent out and, as the system might even explicitly support localization of persons, this data could be collected, aggregated, and analyzed to gain very detailed location profiles. This is clearly a privacy infringement that needs to be prevented. Yet as reported by [6] staff movement monitoring via tokens is a common form of staff control today. If staff do not wear or carry the device they may be denied access to certain areas. Indeed such schemes that log transactions "also support movement tracking, retrospective analysis of movements and potentially even real-time predictive capabilities relating to the person's likely destination". Such location tracking of persons, be they ordinary citizens or parolees being tracked by legal authorities is causing disquiet among privacy advocates. The term "dataveillance" (a contraction of data and surveillance) has recently been overtaken by the term "Uberveillance"[7]. Uberveillance takes "that which was static and discrete in the data veillance world and makes it constant and embedded." In [7], Uberveillance is defined as the sum total of all types of surveillance (CCTV, national identity card, biometrics, ePassports, microchip implants) and the deliberate integration of personal data for continuous tracking and monitoring of identity and location in real time. PEMS enable and simplify exactly this kind of surveillance.

Activity tracking of users: This kind of attack is very special to eHealth systems. Based on the recorded data, it might be possible to actually analyze the activities of persons. As an example, it might be possible to analyze the amount of sport a person is performing by simply looking at heart rate and oxygen saturation data when a person is being constantly monitored. Such medical monitoring is a feature of ReMoteCare as is video monitoring as described in [10]. Insurance companies might abuse this information to restrict access to benefits for people with an unhealthy lifestyle. Again this affects a user's privacy. As well, mobile phones with GPS chipsets make it possible for service providers to perform a position fix within minutes of receiving a police request [8]. According to [8] "Beyond statistical data, location intelligence reveals a great deal about one's preferences, friends, associations and habits"

Physical tampering: As access to the motes is quite straightforward, attackers might steal equipment or tamper with motes to modify sensor values, simply throw the motes away or vandalize them.

3.2. Attackers and Motivations

Depending on the capabilities of an attacker, the feasibility and potential impact of the attacks listed above varies. We distinguish the following types of attackers:

External passive attacker: Is not part of the system and does not control any of its components. An external passive attacker is mostly restricted to eavesdropping on the communication in the CN. Simple encryption using a shared key may already be sufficient to defeat this kind of attacker in the communication network. In ReMoteCare, at least parts of the communication system are protected by SNMPv3s built-in encryption capabilities. However, some forms of location or activity tracking might still be possible, if the attacker can for example record communication events and read address information in the packets.

External active attacker: This attacker is also not part of the system, but can try to modify or forge packets or mount jamming attacks. The primary goal of any security solution against external active attackers is usually creating a closed user group where messages from external entities are rejected and certain measures against Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are introduced.

Internal passive attacker: Internal attackers are part of the system or control some of its components. An internal passive attacker is again mostly restricted to eavesdropping or tracking, however, he may e.g. circumvent certain encryption mechanisms, because of knowledge of key material. The attacker could be anyone from a disgruntled employee to simply a user of the PEMS.

Internal active attacker: The internal active attacker is the most powerful attacker variant. He controls parts of the system and is able to actively modify or forge data in those parts he controls.

3.3. Attacked Components

Attackers may target different components of the system depending on where they are located and what components they eventually control. Here we discuss the impact of attacks on different parts of the system.

Sensor: Attacking the sensors can mean capturing the data directly from the sensor or even replacing the sensor and injecting false data. However, attacking the sensor usually means the attacker has to have direct

access to the mote hardware. Therefore only internal attackers (especially the user) can do this. Motivation for such an action can be to hide certain medical conditions from doctors or insurance companies. In ReMoteCare, removal of sensors from the environment is a distinct possibility as the patient or anyone in the patient's room can easily remove the pulse oximeter (or indeed the entire mote) from the mote.

Local Processing Unit (LPU): Similar reasoning holds true for the LPU. However, some systems envision remote software updates to the LPU. If attackers manage to manipulate this software update, they may be able to remotely manipulate the LPU for eavesdropping or manipulation of data. Being very resource constrained, complex and resource intensive security mechanisms cannot be implemented here.

Local Data Collection (LDC): Again, attacks on the LDC are similar to sensor and LPU attacks. However, reading out LDC can provide a lot of information at one time. Similarly, altering information stored in the LDC can modify the patients' long-term medical record very quickly. Thus, ensuring the integrity of data stored in LDC becomes a primary concern. In ReMoteCare, data is not stored persistently in the motes but instead directly communicated to the gateway.

Local Actuator (LA): Focusing on the LA basically allows attackers to trigger inappropriate actions like emergency calls directly. Note however, that this usually can also be achieved by feeding manipulated data to the system assuming that the analysis procedures are known.

Communication Network (CN): Whereas the previous attacks need to manipulate any individual mote and therefore have a scalability problem, attacking the CN is the first place that may allow eavesdropping or manipulating the system as a whole as all data passes the CN on its way to the remote components. Therefore data collection or manipulation become much more effective when carried out in the CN rather than attacks on individual motes.

Remote Processing Unit (RPU): The remote processing unit is responsible for collecting and analyzing all data sent from the sensor network. Therefore it is again a very attractive target for attacks, as the enemy is again not limited to individual motes but can damage the whole system. At the same time, the RPU might be connected to the Internet, allowing also remote attacks, whereas there is usually no direct connectivity to the sensor network. Offering rich resources, the RPU can implement also comparatively complex security mechanisms. In ReMoteCare the RPU functionality is split between the gateway and the

analysis systems and therefore, security mechanisms must be distributed, too.

Remote Data Collection (RDC): As the RDC will collect the information from all motes in the system, eavesdropping on or even modification of data in the RDC can have devastating effects, e.g. altering the medical records of whole populations.

Remote Actuator (RA): Like with the LA, attackers addressing the RA can trigger inappropriate actions. Again, the scale of the attack is different, as they now can trigger alarms for each mote and for many motes in the system at once.

3.4. Impact of Scale

Attacks on a PEMS will have very different goals and effects, depending on the scale on which they are deployed.

Individual home monitoring: If an attack addresses a system that monitors only single individuals, it makes no big difference in terms of impact whether the attacker addresses the local or remote systems as the data available and the effects that can be triggered are almost identical. In such a scenario, attacking a larger population becomes very difficult, as a lot of individual systems have to be targeted. This can only be done if attacks can be automated to high degree.

Hospital monitoring: Located in between the other two options, targeting remote components in a hospital system allows the attackers to affect a number of motes and persons in parallel. At the same time, the users and operators of the PEMS are restricted in number, enhancing the probability that an attacker will have to act as an external attacker without immediate access to the system. This gives opportunities to isolate the system from the outside world as a measure of protection.

Large-scale monitoring: In large scale monitoring, almost everybody is at least a user of the system, owning some components that participate in the system. So every potential attacker is an internal attacker to some extent. At the same time, successfully attacking the remote components can be disastrous, as medical records for whole populations can be accessed/alterd there or RAs can be used to overload a whole medical emergency system by creating large amounts of false alarms.

4. Securing eHealth Monitoring Systems

In this section the authors discuss security requirements for PEMS and give initial guidelines for security solutions addressing the various threats

outlined in the previous section. We will structure our discussion according to the classic security goals *integrity*, *confidentiality*, and *availability* and add a special discussion of privacy.

4.1 Integrity Protection

Preventing unauthorized modifications of data while at the same time ensuring that only legitimate motes can create and inject data to the network prevents many of the previously discussed attacks. The components in the sensor nodes (*sensors/LPU/LDC/LA*) are vulnerable to physical tampering which cannot easily be prevented on a pure logical level. Using tamper-resistant devices is a viable but costly alternative. In the communication network (CN) lightweight authentication and integrity check methods (e.g. using MAC) can provide integrity protection during transit. In the backend system (*RPU/RDC/RA*) standard security mechanisms as well as privacy enhancing mechanisms should be deployed. This can include: server-based security mechanisms to prevent attacks on the server; access control mechanisms in the medical applications; physical security against access to the hardware, and many more).

4.2 Confidentiality

Eavesdropping on data in the sensor nodes (*sensor/LPU/LDC/LA*) can again be ensured using tamper-resistant devices. Availability of public key cryptography in the sensor nodes should allow for data encryption¹.

In the communication network (CN), data should be encrypted using either shared keys or public key cryptography. Regarding the backend system (*RPU/RDC/RA*) the same mechanisms as discussed in the previous paragraph should be considered. In addition, encryption of data in the RDC can increase the protection level.

In the ReMoteCare system, SNMPv3 is used to ensure confidentiality in the RPU. Securing the communication network is still challenging due to resource constraints in the motes [13].

4.3 Availability

Availability in the sensor nodes (*sensor/LPU/LDC/LA*) cannot be ensured reliably, as users controlling individual nodes can easily bring them down by switching them off, removing the sensors or physically destroying them. However, nodes

¹ There are very different opinions on the viability of public-key cryptography in sensor nodes.

should be protected from remote denial of service attacks like power drain attacks. Denial of Service in the communication network (*CN*) should be prevented by allowing enough redundancy so that failure of individual nodes will not affect the overall system. Single point of failures – such as the Stargate gateway in the ReMoteCare prototype – are especially vulnerable to DOS attacks. Overload attacks on the network might be addressed by rate limits for example. Ensuring the availability of the backend system *RPU/RDC/RA* does not differ from traditional systems.

4.4 Privacy

Given that data confidentiality is already ensured and only authorized people can actually access the medical data, the major privacy issue is localization. In order to prevent location profiling, sensor nodes (*sensor/LPU/LDC/LA*) should be traceable only in case of emergencies and only by authorized medical staff. One way to achieve this is by doing the localization inside the sensor node and deliver the location data to external entities only in case of alarm situations. As the communication network (*CN*) may also be used for tracking node positions, this has also to be taken into consideration. Regarding the backend system (*RPU/RDC/RA*), privacy might be enhanced by storing the data using pseudonyms and having a separate mechanism for pseudonym resolution, for example.

4.5 Legal ramifications

In the United States there are a several agencies, including the FBI, working in the area of cyber crime, often with overlapping jurisdictions. The National Information Infrastructure Act, 1996 provides a framework for dealing with computer crimes at the federal level. The Electronic Communications Privacy Act (ECPA) 1986 is also relevant. In particular, s2511 prohibits “interception and disclosure of wire, oral or electronic communication. However, s2511 (2) g (i) provides that it shall not be unlawful for any person “to intercept or access an electronic communication made through an electronic communication system that is configured so that electronic communication is accessible to the general public”.

Sec. 33A.04. “Theft of Telecommunications Service” states:

(a) A person commits an offense if the person knowingly obtains or attempts to obtain telecommunications service to avoid or cause another person to avoid a lawful charge for that service by using: (1) a telecommunications access device without the authority or consent of the subscriber or lawful holder of the device or pursuant to an agreement for an

exchange of value with the subscriber or lawful holder of the device to allow another person to use the device [11].

However, in Bill 495 being considered by the New Hampshire legislature, the onus will be placed on operators of wireless networks to secure them or lose some of their ability to prosecute anyone who gains access to the networks [12].

In Australia, under the Cybercrime Act 2001 “Serious Computer Offences”, punishable by lengthy jail sentences are established for unauthorized access to, or modification of, data held in a computer or impairment of electronic communication to or from a computer [17].

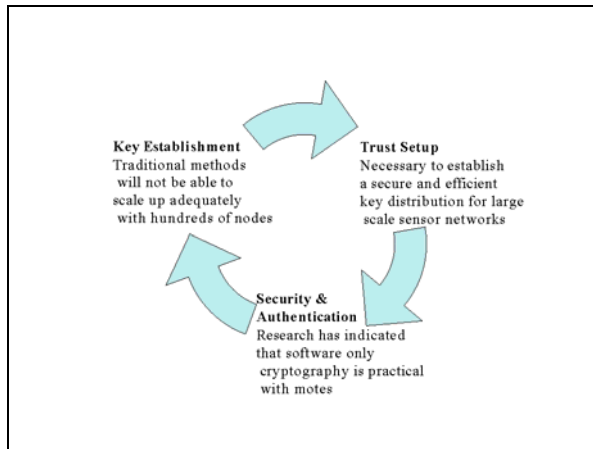
Also in Australia, under the Telecommunications (Interception Act) 1979, criminal penalties apply to a person who “authorizes, suffers or permits another person to intercept a communication passing over a telecommunication system” [17].

5. Related Work

The work of [8] gives a generic survey on WSN security. Many of the presented mechanisms may also be used in PEMS but need to be analyzed considering the specific requirements. Although looking at the sensor network alone is not enough, as the backend systems need to be taken into consideration, too. An initial discussion of PEMS security is found in [5].

The following figure illustrates some of the current thinking on how to secure wireless sensor networks. The issue is especially relevant in the case of healthcare data. Researchers from Berkeley believe that security for motes must be integrated into every component as components designed without security are the vulnerable points where attacks start [16]. The accuracy and security of vital medical information received from motes must be maintained and is an area for further exploration. If motes move into critical healthcare applications they may be subject to regulation as medical devices [14]. Of course, performance issues also need to be taken into account as the application should exhibit real-time characteristics.

Figure 3 Security and Motes [14] [15]



Another issue that needs to be addressed is to ensure that the huge data stream of information regarding the patients does not overwhelm the medical personnel and does not clutter the information system with unnecessary detail. However sensors are capable of sending vast streams of personal, private, medical information wirelessly where it could be intercepted by unauthorized people or perhaps mishandled by medical/office personnel who could be unused to handling such large streams of information and who may be unable to work out which data should be kept and which discarded in a safe fashion. The huge data stream of information regarding the patients must not overwhelm the medical personnel and clutter the information system with unnecessary detail. Healthcare providers or others who have access to health information and do not act on it may incur substantial liability.

For using PEMS in a limited scenario like Home Monitoring, it might be sufficient to ensure a trusted 1:n connection between a private monitoring system (e.g. a PDA) and a set of sensors. [18] suggests a process called imprinting for this and the European projects MAGNET and MAGNET-Beyond propose to establish trusted “personal networks” composed of trusted personal devices [19].

6. Summary and Outlook

As shown in this paper, security and privacy of personal eHealth monitoring systems need to address their specific characteristics and fulfill a whole set of security requirements. Our system ReMoteCare has started to address these issues. Initially, we rely SNMP v3 for securing the remote components. It is important to recognize that it is not sufficient to look only at the sensor network but that an integrated discussion of the whole system, including backends, is necessary. In addition to the topics raised in this paper, national laws

on privacy and data protection of medical data need to be considered. Our future plans include the discussion of such legal and organizational questions as well as the extension of our existing PEMS prototypes by security mechanisms.

7. References

- [1] P. Leijdekkers and V. Gay, “Personal heart monitoring and rehabilitation system using smart phones,” in ICMB. IEEE Computer Society, 2006, p. 29. [Online]. Available: <http://doi.ieeecomputersociety.org/10.1109/ICMB.2006.39>
- [2] Arto Holopainen, A (2006) Use Of Modern Mobile Technologies To Enhance Remote Healthcare Services, 6th Nordic Conference On Ehealth And Telemedicine, Helsinki, 31 August 2006
- [3] K. Lorincz, D. Malan, T. R. F. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnyder, G. Mainland, S. Moulton, and M. Welsh, “Sensor networks for emergency response: Challenges and opportunities,” *IEEE Pervasive Computing, Special Issue on Pervasive Computing for First Response*, 2004. Available: <http://www.eecs.harvard.edu/mdw/papers/codeblue-ieeeperc04.pdf>
- [4] R. Bader, M. Pinto, F. Spenrath, P. Wollmann, and F. Kargl, “Bignurse: A wireless ad hoc network for patient monitoring,” in *First Workshop on Location Based Services for Health Care, Locare’06*, Innsbruck, Austria, November 2006.
- [5] E. Lubrin, E. Lawrence, and K. F. Navarro, “An architecture for wearable, wireless, smart biosensors: The motecare prototype,” in *ICN/ICONS/MCL*. IEEE Computer Society, 2006, p. 202. Available: <http://doi.ieeecomputersociety.org/10.1109/ICN/ICONS/MCL.2006.48>
- [6] Clarke, R. (2007) Appendix to what “uberveillance” is and what to do about it: Surveillance vignettes, The Second Workshop on the Social Implications of National Security – From Dataveillance to Uberveillance and the Realpolitik of the Transparent Society” Ed by K Michael and M.G. Michael, 29 October 2007, Wollongong.
- [7] Michael, K. and Rose, G. (2007) Human tracking technology in mutual legal assistance and police interstate operation in international crimes. The Second Workshop on the Social Implications of National Security – From Dataveillance to Uberveillance and the Realpolitik of the Transparent Society” Ed by K Michael and M.G. Michael, 29 October 2007, Wollongong.
- [8] E. Shi and A. Perrig, “Designing secure sensor networks,” *IEEE Wireless Communications*, vol. 11, no. 6, Dec. 2004. Available: <http://sparrow.ece.cmu.edu/~elaine/docs/secsensornet.pdf>

- [9] M. Messina, Y. Lim, E. Lawrence, D. Martin: Implementing and Validating an Environmental and Health Monitoring System, 5th International Conference on Information Technology: New Generations (ITNG 2008), April 2008
- [10] Y. Lim, M. Messina, F. Kargl, L. Ganguli, M. Fischer, T. Tsang: SNMP-proxy for wireless sensor network, 5th International Conference on Information Technology: New Generations (ITNG 2008), April 2008
- [11] Texas Penal Code, Sec. 33A.04., Theft of Telecommunications Service
- [12] New Hampshire House Bill 495, <http://www.gencourt.state.nh.us/legislation/2003/HB0495.html>
- [13] Martin Fischer: Enhancing the ReMoteCare prototype by adding an SNMPproxy and video surveillance, diploma theses, University of Koblenz, 2008
- [14] D. Culler and W. Hong, "Wireless Sensor Networks " ed. Communications of the ACM, June 2004 From: <http://www.pbol.org/projects/genie/publications/infomanager.pdf>, 47:6 (2004).
- [15] E. Lawrence, K. Felix Navarro, J. Riudavets, M. Messina, "Macroscopic Sensor Networks: Application Issues in the Healthcare Industry," Proc. Third International ISCA Conference on Computer Science, Software Engineering, Information Technology and eBusiness and Applications (CSITeA 2004), December 27-29 2004.
- [16] Shnyder, V., Chen, B., Lorincz, K., Fulford Jones, T. and Welsh M., "Sensor Networks for Medical Care," Technical Report TR-08-05, Division of Engineering and Applied Sciences, Harvard University. Available: <ftp://ftp.deas.harvard.edu/techreports/tr-2005.html> (2005).
- [17] Lawrence, E., Lawrence, J. & Zmijewska, A. (2006) Legal Remedies for Securing the Mobile Enterprise. IADIS International Journal of WWW/Internet (ISSN: 1645-7641)
- [18] F. Stajano, R. Anderson, The Resurrecting Duckling: Security Issues for Ubiquitous Computing, first Security & Privacy supplement to IEEE Computer, April 2002.
- [19] ICT Projects MAGNET and MAGNET Beyond: <http://www.telecom.ece.ntua.gr/magnet/index.html>