Security and Privacy for Mobile Electronic Health Monitoring and Recording Systems (Draft)

Johannes Barnickel, Hakan Karahan, Ulrike Meyer
UMIC Research Center
RWTH Aachen
Email: http://itsec.rwth-aachen.de/people

September 13, 2012

Abstract

In this draft we detail the security and privacy architecture and implementation of the HealthNet mobile electronic health monitoring and data collection system. HealthNet consists of a body sensor network embedded in clothing that communicates wirelessly to the wearer's mobile phone. The mobile phone is used to manage, store and transfer the data in a secure way. Data may be transferred to other parties, such as medical experts, emergency care and private parties trusted by the wearer himself, e.g., his family. The patient controls who may access his data. Only emergency physicians nearby the patient may access vital data without the patient's individual consent. We describe the unique security and privacy features of our architecture which may also be used to improve other telemonitoring solutions.

1 Introduction

Automatic continuous surveillance of vital parameters enables patients with chronic diseases to leave their hospital ward and take part in everyday life. Most importantly, they are able to live in their own homes. With the ever increasing life expectancy this is a growing market. The concept of telemonitoring was envisioned before the technology was ready for it. A patent filed in 1974 [3] already describes a system that detects disconnected electrocardiography (ECG) electrodes and relays the alarm over radio. A patent filed in 1991 [4] describes a system that combines telemonitoring with geographical patient tracking. Due to the restrictions of the radio interfaces, the range of these systems was limited such that the systems allowed a patient to leave his bed, but not the hospital. In the 1990s, telemonitoring became a research focus for various research groups,

academic [11, 17] as well as industry [6, 7] and military [15] ones. Today, there are some systems available on the market, but none has gained an outstanding market penetration. This is in part due to constant advances in technology that quickly render systems obsolete but there are also legislative issues and concerns by patients. With the rapid development of radio technology culminating in the deployment of 3G cellular networks in the European and North American markets, the connectivity required for telemonitoring systems beyond ECG monitoring was established. With prices for data connections over 3G cellular networks dropping and affordable flat rates being available in many countries, the systems have become feasible.

Two academic telemonitoring systems based on 3G that have completed tests with patients are the Australian Personal Health Monitor [8] and the European MobiHealth [17] system. MobiHealth has a detailed security specification but no privacy features, Personal Health Monitor achieves some privacy features but does not have a detailed security specification. Some commercial systems [7] have no clear security and privacy specification at all and rely on security by obscurity by claiming diffuse security features without disclosing how they are achieved. To better cope with user concerns and legal requirements, a precise security and privacy specification is required.

In the following, we describe the novel design of a security architecture for HealthNet. The HealthNet project is a joint research project of several research groups of RWTH Aachen University based on a sensor network embedded in clothing [9]. The sensor network collects vital parameters and communicates wirelessly with the wearer's mobile phone. The mobile phone is used to manage, store and transfer the data in a secure way. Data may be transfered to other parties, such as medical experts, emergency care services and private parties trusted by the wearer himself, e.g., his family. The patient controls who may access his data. Only emergency physicians nearby the patient may access vital data without the patient's individual consent. The system is designed to support automated emergency calls when vital parameters match predefined patterns. The system is not aimed at creating an infrastructure among medical experts or health insurance companies. Cryptographic techniques are used to prevent security attacks on wireless data transmission and stolen devices. We show that our architecture is feasible on technologies currently available and large parts of the implementation are feasible with consumer equipment that is readily available. Only the wearable sensor shirt requires unique hardware.

In Section 2, we will explain our approach to automatic continuous surveillance of vital parameters and its security and privacy features. In Section 3, implementation details are provided. We show a performance evaluation in Section 4, and compare our approach to existing solutions and recommend changes to other telemonitoring solutions in Section 5. Finally, the conclusion is drawn and we provide an outlook on future work in Section 6.

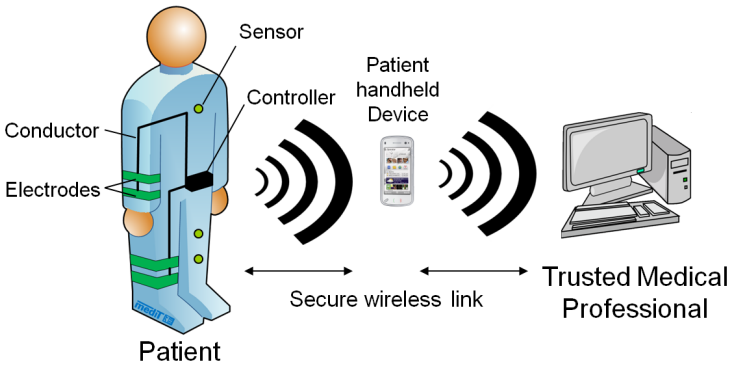

Figure 1: HealthNet scenario overview

2 HealthNet Architecture

2.1 System Outline and Security Requirements

The scenario underlying the HealthNet project [9] is illustrated in Figure 1. A patient will be prescribed a wearable sensor shirt by a medical expert. The data originates from sensors that are embedded in the shirt worn by the patient. The sensors are exchanging data via a wireless ZigBee link to the central hub node that is also embedded in the shirt. This central node is communicating to a handheld device, usually a mobile phone or PDA, via a Bluetooth link. While the sensor nodes and the central node on the shirt do not have a user interface, the handheld device is used by the patient to check his vital parameters and to modify the settings of the system. For privacy reasons there is no central data storage server that stores data of all system users in our architecture. The handheld device processes the sensor data to filter out meaningless sequences, which reduces the overall amount of data. Using data mining techniques, only summaries of non-critical sensor readings are stored and transfered in regular intervals. As there is no need to transmit, e.g., every single heart beat to a central data center in real time, the HealthNet project avoids draining the batteries of the mobile device and time synchronization issues that occur when the clocks of different devices are out of sync.

The handheld device is also used to manage trust, i.e., to add and delete trusted other devices. Trusted other devices may access the data on the patient's handheld device at any time without the patient's interaction. Trusted devices are owned either by a medical expert, by the patient himself, or by another person trusted by the patient, e.g., his spouse. Data transfers from the patient's device to other devices are achieved by wireless Bluetooth or WLAN 802.11 in ad hoc mode directly connected to the equipment of the medical experts. Cellular networks are currently not used, but may be added at any time.

Apart from the base scenario the HealthNet architecture supports several additional features:

1. In order to cope with situations where the patient is, e.g., unconscious, all emergency physicians within Bluetooth range may access the data on the patient's handheld device using their own special handheld devices at any time and without the patient's explicit consent.

2. When the patient's handheld device detects a critical condition, it will automatically contact an emergency dispatcher with the patient's standing data and the medical situation, sound an audible alarm, and establish a voice connection.

3. The patient may also run his own long term data collection on his desktop PC, to which the handheld device transfers data in regular intervals, especially before exceeding its local memory.

The measured data must be kept confidential at all times: during collection, in storage and during transmission within and between all components of the system. To reduce the risk of data extortion from stolen devices, secure authentication methods must be used both for wireless links as well as user interfaces on the devices themselves. Generally, data may only be read by persons authorized by the patient. However, data may be read without the patient's explicit consent during an emergency detected by the body sensors or when an emergency medical expert is close to the patient. The reading equipment of emergency medical experts must be remotely revocable. Finally, no more data than required for a given monitoring application shall be stored.

2.2 Security and Privacy Mechanisms

Confidentiality during data collection is achieved by using ZigBee AES-128 encryption between the sensor nodes and the hub and Bluetooth encryption E_0 between the hub and the handheld device. These are both single hop connections with fixed partners.

Confidentiality during data storage is achieved using AES-128 encryption on the devices, so that no data can be recovered wrongfully by someone who has physical access to a device. All devices that allow user interaction on medical data, such as the patients' handheld devices, the trusted parties' devices and the emergency physicians' handheld devices, require the user to authenticate to the device. This is implemented using a password scheme, where reauthentication is required after a short idle period. An authenticated session can also be terminated by the user by logging out manually. Upon logout, all measured data and the decryption key are erased from the systems' memory such that the data only remains on the device's storage medium in encrypted form.

For confidentiality and integrity protection during communication from the PDA to trusted devices we do not rely on the security mechanisms of the technologies used (Bluetooth, WLAN). Instead, all data transfers apply AES-128 encryption and message authentication codes on the application layer. The system does not rely on security mechanisms of the wireless technologies used because the data must not be revealed to the network operators and wireless

technologies like GSM, UMTS, and WLAN typically only encrypt the air interface. Also, a receiving station may not detect if an incoming connection uses an insecure link somewhere along the connection before the last hop to the receiver when relying on link layer mechanisms, e.g., a WPA2 protected WLAN network seen by the device could relay data over an unprotected WLAN network, which cannot be detected by the device.

Therefore, in our system no party may attempt or accept connections without HealthNet's own application layer security mechanisms.

In wireless connections to trusted parties and emergency physicians, all parties are identified using certificates for 2048 bit RSA keys, 256 bit ECC keys or a shared key of at least 112 bit strength. This is in accordance with current recommendations of the NIST [14]. Shared key authentication is used in our system for all use cases except emergencies. This is possible because connections are usually only made between the patient and one to four other parties (medical expert, long term storage and family), who will always personally meet the patient anyway. These parties do not change frequently. These parties are authenticated according to the patient's chosen settings. The patient adds and removes entitled parties at any time using his handheld device after authenticating to it. The handheld reading devices of emergency medical experts are equipped with certificates that enable them to read patients' devices in their proximity at any time without the patients consent. These certificates are issued by the operator of the system, who has deployed it. Certificate revocation is achieved through certificate revocation lists (CRLs) downloaded by the patients' handheld devices via the cellular network in regular intervals. A CRL consists of the serial numbers of revoked certificates, its validity period, and a signature by the CA. CRLs are automatically created by the CA when new certificates are revoked or before the validity period of the last CRL has expired. The CA is trusted by the patient's handheld device, i.e., its public key is preconfigured on the device. Thus, patients are at all times in control of their data, with the exception of emergency cases, where physicians within Bluetooth range may read data if they have been authorized by a CA.

As a trust anchor for bootstrapping, we assume that the sensor shirt will be given to the patient by a medical expert whom he trusts. Thus, when initially giving the sensor shirt to a patient, the medical expert will take care of a secure pairing process between his remote reading device and the patient's handheld device, i.e., authorizing himself as a trusted party on the patient's handheld device before issuing it to the patient. The medical expert who sets up the patient's handheld device will verify that the patient's device knows the correct public key of the CA used for emergency experts reading devices by comparing the CA certificate fingerprint on the patient's device to that on his own device. The patient will then setup the user authentication, possibly with the help of the medical expert or his staff, so that from then on, he controls who is able to read data from his handheld device.

We believe that these mechanisms can be adopted by other mobile health monitoring systems and that they would increase their security and privacy, thus reducing legal nuisances and user skepticism.

3 Implementation of the System

This section presents details of the implementation of our HealthNet architecture, including used hardware, software, and security mechanisms.

3.1 Hardware and Software

For our system, we use the Nokia N97 smartphone. It runs Symbian OS v9.4 with the S60 5th Edition software platform on an ARM 11 CPU with a clock rate of 434 MHz and 128 MB SDRAM. Bluetooth 2.0 as well as WLAN 802.11b/g, including WPA2 (AES/TKIP), are supported [1].

Our application is implemented as a MIDlet for the Java ME environment, which requires a number of Java Specification Requests (JSRs) provided by the N97. JSR 75 *FileConnection* is required to perform file system operations on the built-in telephone memory and the exchangeable Micro SD memory card. JSR 82 *Java API for Bluetooth* is used for Bluetooth connections to other devices. JSR 135 *Mobile Media API* provides means of sending SMS and calling telephone numbers.

JSR 177 *Security and Trust Services API* provides basic cryptographic operations like creating message digests with SHA1 or MD5, and symmetric encryption with DES/Triple DES, which do not meet our security requirements. There is neither certificate handling nor AES support. In addition, while asymmetric cryptography to encrypt data is supported, asymmetric data decryption is not supported. To address these problems we use the *BouncyCastle* Crypto API for Java [16]. It provides a collection of cryptographic APIs for Java and C#. The Java release is divided into different providers, i.e., JDK 1.2-1.6 and Java ME. Nearly every current cryptographic algorithm is supported by BouncyCastle, including RSA, AES and X.509 certificate handling.

The Mobile Information Device Profile is part of the Java ME framework and provides the Record Management System (RMS). RMS manages the record store, which is stored in binary files on the mobile phone's file system. A record store can be marked either as shared, so that any MIDlet on the phone can access the store, or as private, so that only the MIDlets in the same suite that created the store can access the store. We use a private record store for the storage of the login password and other settings.

3.2 Implementation of Security Mechanisms

3.2.1 User Authentication

After starting the MIDlet, the user is asked to enter a password to get access to the MIDlet functionalities. The password is stored on the smartphone as a SHA-1 message digest in a record store. Upon input of the password, the message digest is computed and compared to the stored value. If the hashes match, the user is successfully authenticated and gains access to the MIDlet. User interaction is monitored, and after an idle time of three minutes the user is

logged out automatically so that he needs to reauthenticate to use the MIDlet again.

3.2.2 Sensor Data Storage

Record stores are not a good fit for large amounts of data. Thus, we use the Micro SD card to store sensor data. The sensor data is cached for a minute before it is written to the file system. To achieve confidentiality, this data is encrypted with the symmetric AES-128 cipher. The AES key used for this encryption is generated with the help of a fixed salt and a passphrase which needs to be entered upon connection establishment to the sensors. When the connection to the sensors is lost or when the MIDlet is terminated the AES key will be deleted from the memory. For decryption of the data or further encryption upon reconnect to the sensors the passphrase must be reentered to generate the same AES key. Thus, data on a stolen device cannot be decrypted.

Data filtering on the device to reduce the amount of data and to protect the patient's privacy so far was only implemented exemplary by setting a lower pulse threshold. Data mining is the focus of another research group at RWTH Aachen [10].

3.2.3 Connecting to Trusted Third Parties

The patient device can be connected to trusted devices via Bluetooth. Therefore, it is always in Bluetooth discoverable mode. Requiring the patient to interact in the connection process would obstruct connections by emergency medical experts to devices of unconscious patients. Only outgoing connections to medical experts may use WLAN to avoid addressing issues. For both transmission technologies, mutual authentication between the patient's smartphone and trusted third parties, i.e., the patient's long term storage, medical experts or family members, is achieved through a password-authenticated key agreement. We use a share-password authenticated Diffie-Hellman key exchange for session key agreement and authentication to prevent eavesdropping and impersonation attacks, even under a man-in-the-middle scenario.

Forwarding stored sensor data to a trusted third party is implemented by directly transmitting the cipher blocks from the patient's Micro SD card to the trusted party's storage. The AES key that was used for the encryption by the patient device is also transmitted, but encrypted with the new session key. The trusted party stores the key and the indices of the respective blocks in order to access the data. This avoids a bulky re-encryption of the Micro SD card contents.

The implementation of the certificate handling, the certificate based authentication scheme, and certificate revocation lists for the emergency physicians is work in progress.

sensor type	frequency	precision	data rate
electrocardiography	5 Hz	848 bit	530 byte/s
accelerometer	10 Hz	96 bit	120 byte/s
body temperature	1 Hz	64 bit	8 byte/s
total			658 byte/s

Table 1: Sensor data rates

3.2.4 Emergency Dial

To automatically contact an ambulance in case of emergency, an SMS is sent to a regular land line emergency number. The SMS will be read out automatically by the telephone service provider. The smartphone will then create a voice connection to the emergency line. As there are currently no emergency dispatching services accepting data connections and because our current platform is unable to play voice messages to telephone contacts, this seems like the best workable solution. Sending SMS and initiating telephone calls always require user confirmation, which is a limitation of the Java ME platform. It is impossible to set these permissions beforehand, neither through setting MIDlet-Permissions in the JAD file during deployment, nor through signing.

4 Performance of the System

4.1 Connection Time

The MIDlet needs about 12 seconds to start up. After that it is running in the background. Switching back and forth between MIDlet and other phone functions happens immediately. To connect to the central sensor node a manual discover-and-connect operation needs to be started from within the MIDlet which takes about 15 seconds. The overall time before the MIDlet is fully initialized and starts gathering data from the sensor nodes is under 30 seconds. This value is rather negligible since the MIDlet only needs to be started once after the smartphone was turned on and we assume that the smartphone will run 24/7.

4.2 Battery Life

The Nokia N97 runs out of battery after 11 hours of data recording, which includes a constant Bluetooth connection to the body sensor network, data processing, and storing the data on the Micro SD memory card. When the battery can be charged twice a day, our implementation is already adequate for a patient's day-to-day use, but there is room for improvement.

4.3 Memory Requirements and Uploads

In the final prototype the gathered sensor data will consist of three different packages (see Table 1) and amount to 658 bytes per second = 759 MB per week. Data mining will be used to to filter uninteresting data, which will reduce the amount of data that will be stored on the patient's device. The 32 GB Micro SD card of the N97 provides abundant storage space. Even a much smaller Micro SD card would be sufficient. When the therapy does not require more frequent uploads, one upload every two to six weeks seems advisable. The time required for an upload depends on the length of the period, the reduction rate by the patient's device, and the technology used.

5 Related Work

5.1 Selected Mobile Health Monitoring Systems

In the following, we provide a brief overview over some examples of systems developed so far. It is by no means an exhaustive list. The most notable academic systems are the Australian Personal Health Monitor [11] and the European MobiHealth [17] system. Both feature working prototypes that have completed field tests on a number of actual patients.

Personal Health Monitor uses Bluetooth sensors to monitor the wellbeing of high risk cardiac patients around the clock. The sensors are connected to a Windows mobile smartphone, which will process the data. There is no permanent connection to a health care center during regular operation. Personal Health Monitor uses data processing on the mobile device to reduce the amount of data. The information stored on the mobile device can be transferred to the central patient personal health record via an Internet connection. In case of emergency the mobile device displays a warning, asks whether to call an ambulance and defaults to "yes" after a timeout, plays a voice message for bystanders with first help instructions, and sends SMS to pre-assigned numbers. Communication to emergency services is realized via 3G or any Internet connection available on the phone.

The European MobiHealth project is a real-time remote health monitoring system centered on a Java enabled mobile phone with a detailed backend system. All measurements are transmitted in real time to medical experts, who review the data, partly automated, in their offices. No filtering or processing is done on the mobile device.

A direct comparison of MobiHealth and Personal Health Monitor can be found in [8]. In the following, we will compare the HealthNet features to the features offered by these systems.

5.2 Differences in Architectures

Architectures of telemonitoring systems differ in the distribution of data storage, distribution of data processing, security and privacy mechanisms, and in

whether they are real-time or store-and-forward systems. Many systems assume a centralized infrastructure where all data of all patients is being uploaded to by the mobile devices and accessed by medical experts. Other systems do not require a centralized infrastructure. Instead, they either require a backend in the patient's control, such as a desktop computer in his home, or use direct transmission of data to a single trusted medical expert's device.

Data mining for critical or otherwise significant data can be conducted in a decentralized way on the devices in the patient's domain, on a centralized infrastructure, at the medical expert's device, or (if there is no data mining in the system) by the medical expert himself. The closer to the sensors the data is processed, the less data needs to be transmitted, stored and protected on systems out of the patient's control. [5] identifies two groups of telemonitoring systems:

Real-time telehealth systems constantly transfer health data in real time. These systems allow immediate response in case of emergency, but have high communication and energy costs. The constant surveillance may feel intrusive to some patients.

Store-and-forward telehealth systems record health data and will only transfer it at regular intervals. These are more efficient for data collecting but are limited in terms of emergency handling. Privacy is still an issue, as still complete data is transferred. Some store-and-forward systems process the data on a home PC to reduce the amount of data sent, which makes the systems less intrusive, as only data relevant for the affliction is transmitted. Still, emergencies cannot be detected promptly. Other store-and-forward systems process the data on a mobile device instead of a fixed PC. As the mobile device can always be connected to the body health sensors, this enables real time emergency detection. This approach may retain privacy if the data is reduced sufficiently. As on mobile devices communication is usually more expensive than calculation in terms of energy, better energy efficiency is achieved if the data is filtered before it is sent over a long-range radio interface.

The Personal Health Monitor and MobiHealth projects are prominent examples of these two types of architectures. Like Personal Health Monitor, HealthNet is a store-and-forward telehealth system.

5.3 Security and Privacy Features and Risks

Centralized vs. Decentralized: The centralized infrastructures in many systems enable easy sharing of data among medical experts but take control over the data away from the patient. As such data is also interesting for parties not trusted by the user (insurance companies, employers, etc.) this may result in privacy concerns for some users. In a centralized storage architecture, an intruder who is able to bypass the access control of a medical data storage system infrastructure gains access to everyone's data. In a decentralized storage architecture, such an attacker gains access only to the data of a single user. Even if the attacker is able to bypass the security mechanisms of all decentralized storage systems, he still would have to identify their communication ports, e.g., scan IP ranges,

steal mobile phones, etc, which makes an attack to recover data of a large part of the users infeasible. Decentralized health data storage also leaves the user in full control of his data. He may chose to delete parts of his data and can rely on the fact the there are no other copies.

Personal Health Monitor is a centralized system designed around a single website. HealthNet uses a decentralized infrastructure with one system at each physician and data storage centered at the patient. MobiHealth has many physicians able to access patient data on a single server, e.g., at a hospital, so it is none of the extremes.

Data minimization: Reducing the data volume using data mining techniques instead of storing raw sensor data is also a privacy feature, as it will only store data variations that are interesting for the purpose of the therapy. Otherwise, sensor data could be used to reconstruct a patient's habits, e.g., sleeping times or sporting activities. While this may be useful for certain types of therapy, in many others it is a threat to privacy. When these datasets are required for the therapy, the system may be configured not to filter them.

Personal Health Monitor and HealthNet apply data minimization, while MobiHealth does not.

Use of cryptography: There is no explicit specification for communication or storage security in Personal Health Monitor. Secure web access is mentioned for remotely accessing the data [5]. However, the website[1] where the data is to be uploaded uses an insecure login mechanism, thus exposing transmitted health data and user credentials to eavesdropping attackers. The user credentials may be used by attackers to impersonate users and access their data. The authors are aware that the Australian personal privacy protection in health care information systems guidelines apply [2], but do not detail how the system helps fulfilling them.

MobiHealth is one of the few systems with an expressive description of security requirements and at least some implementation details [12, 13]. MobiHealth relies on Bluetooth and ZigBee link layer security for communication to the sensors and uses HTTPS mutual authentication and encryption for connections to the backend. HTTPS and Java MRI (TLS/IPsec) is used for connections from the backend to physicians. While authentication and confidentiality are achieved, there are no mechanisms to support privacy. All sensor data is transmitted to the backend, where it is out of the patients' control and physicians may access it at any time. The authentication allows identification as well as non-repudiation. The wealth of data allows reconstruction of personal habits.

Personal Health Monitor does not use cryptographic techniques [11, 5, 2], while MobiHealth and HealthNet do.

5.4 Summary

MobiHealth is a secure real-time telemonitoring system and Personal Health Monitor is a privacy preserving store-and-forward telehealth system. Mobi-

[1] `http://personalheartmonitor.com/members/Login.aspx`

Health achieves a security level comparable to HealthNet, but does not achieve privacy at all. Personal Health Monitor reduces the data volume by local processing like HealthNet, but it stores all remaining measurements on a single server that all medical experts may access. No details are given about the access restriction mechanisms on the server. Also, it does not use specific cryptographic security techniques. Instead, it relies on the security mechanisms provided by the transport technologies used by the system, even if there are none.

Our approach unifies the advantages of both systems, as it is a secure and privacy-preserving store-and-forward telehealth system with real time emergency handling ability and data minimization on the user's device.

5.5 Transferability of our Results

The contribution to security and privacy in telemonitoring lies in HealthNet's preprocessing of sensor data on the mobile device [10], decentralized data storage, requiring an existing trust relationship between the patient and a single medical expert that prescribed the monitoring device, and in encryption, authentication and integrity protection through standard cryptographic techniques on the application layer for communication and storage. These mechanisms can be adopted by any telemonitoring system with more or less effort.

The changes to individual devices are: Wireless sensors need to use encryption and authentication for the communication to the personal device. Handheld devices and reading devices need to add user authentication and remote authentication as well as encryption and integrity protection for data storage and communication.

The handheld devices also need to establish a trust relationship with the reading device of the physician that prescribed it. If emergency physician readers with special privileges are required, a certification authority that must be trusted by the patients' devices and a quick certificate revocation mechanism is required.

6 Conclusion and Future Work

Our new architecture offers security and privacy features other future systems may leverage on. Privacy and security is achieved through data avoidance, data minimization, decentralized storage, and the use of cryptography. These mechanisms can be adopted by other mobile health monitoring systems to increase their security and privacy features, thus reducing legal objections and increasing user acceptance. This will help bringing more systems of this type to patients.

In the future, we would like to conduct field tests with our prototype equipment. In addition, adding biometric user authentication to the devices may help avoiding password nuisances.

Acknowledgments

This work has been supported by the UMIC Research Centre, RWTH Aachen University.

References

[1] Nokia N97 details. http://www.forum.nokia.com/devices/N97/.

[2] J. Brakel, V. Gay, and P. Leijdekkers. From the hippocratic oath to electronic data storage: Ethical aspects for m-health projects in australia. eHealth09: Proceedings of the IADIS International Conference On eHealth.

[3] R. Dillman, J. Larsen, and A. Nardizzi. Electrocardiograph telemetry system including method and means for indicating inoperative conditions, 1976.

[4] R. Engira. Miniature multilead biotelemetry and patient location system, us patent no. 5,153,584, filed 1991, 1992.

[5] Valérie Gay, Peter Leijdekkers, and Edward Barin. A mobile rehabilitation application for the remote monitoring of cardiac patients after a heart attack or a coronary bypass surgery. Proceedings of the 2nd International Conference on Pervasive Technologies Related to Assistive Environments, 2009.

[6] HealthFrontier Inc. `http://www.healthfrontier.com/`, last checked july 16th, 2012, archived at `http://www.webcitation.org/69CBRHoIm`.

[7] iMetrikus, Inc., now listed as Numera Inc. `http://numera.com/`, last checked july 16th, 2012, archived at `http://www.webcitation.org/69CBqCLwQ`.

[8] Val Jones, Valerie Gay, and Peter Leijdekkers. Body sensor networks for mobile health monitoring: Experience in europe and australia. ICDS: Proceedings of the 2010 Fourth International Conference on Digital Society, 2009, pp. 204–209.

[9] Saim Kim, Lisa Beckmann, Moritz Pistor, Linda Cousin, Marian Walter, and Steffen Leonhardt. A versatile body sensor network for health care applications. ISSNIP: 5th International Conference on Intelligent Sensors, Sensor Networks and Information Processing, 2009, pp. 175–180.

[10] Philipp Kranen, David Kensche, Saim Kim, Nadine Zimmermann, Emmanuel Müller, Christoph Quix, Xiang Li, Thomas Gries, Thomas Seidl, Matthias Jarke, and Steffen Leonhardt. Mobile mining and information management in healthnet scenarios. MDM: 9th International Conference on Mobile Data Management, 2008, pp. 215–216.

[11] Peter Leijdekkers and Valerie Gay. Personal heart monitoring system using smart phones to detect life threatening arrhythmias. CBMS: Proceedings of the 19th IEEE Symposium on Computer-Based Medical Systems, 2006, pp. 157–164.

[12] R. Martí, J. Delgado, and X. Perramon. Security specification and implementation for mobile e-health services. IEEE International Conference on e-Technology, e-Commerce and e-Service, 2004.

[13] Ramon Martí and Jaime Delgado. Security in a wireless mobile health care system. WWW2003: International World Wide Web Conference, Workshop on Emerging applications for wireless and mobile access, May 2003.

[14] W. Timothy Polk, Donna F. Dodson, and William. E. Burr. DRAFT: Cryptographic algorithms and key sizes for personal identification verification (PIV). In *NIST Special Publication 800-78-2*, 2009.

[15] M. Scanlon. Acoustic sensor for health status. online, `http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA398960`, retrieved September 10, 2012, archived at `http://www.webcitation.org/6AZgmPLeV`, 1998.

[16] The Legion of the Bouncy Castle. http://www.bouncycastle.org/.

[17] K. E. Wac, R. G. A. Bults, D. Konstantas, A. T. van Halteren, V. M. Jones, I. A. Widya, and R. Herzog. Mobile health care over 3G networks: the MobiHealth pilot system and service. `http://eprints.eemcs.utwente.nl/7526/`, last checked July 16th, 2012, archived at `http://www.webcitation.org/69CDhFDP5`, 2004.