Security for Medical Sensor Networks in Mobile Health Systems

Ilya Nikolaevskiy*, Dmitry Korzun†, Andrei Gurtov*‡
{firstname.lastname}@hiit.fi
*Helsinki Institute for Information Technology HIIT and Department of Computer Science and Engineering, Aalto University, Finland
†Department of Computer Science, Petrozavodsk State University, Russia
‡University ITMO, St.-Petersburg, Russia

Abstract—Emerging Internet of Things (IoT) technologies and mobile health scenarios provide opportunities for enhancing traditional healthcare systems. Yet current development meets the challenge of sensing patient's health data with strong security guarantees in mobile and resource-constrained settings as well as in emergency situations. This paper presents a generic IoT-aware system architecture that enables security of personal mobile data and their transfer to healthcare services. Our security solutions apply the Host Identity Protocol. We validate the efficiency using a prototype implementation.

Keywords: Medical sensor network, Mobile healthcare, Security, Host Identity Protocol

I. INTRODUCTION

The recent advances in bioengineering and the proliferation of wireless sensor platforms have allowed the realization of pervasive and mobile health (m-Health) systems. Sensors, wearable by a patient or implantable within her/his body, form a medical sensor network (MSN) accessible to medical personnel and the patient himself. The mobile terminal centric view states that end-user device (such as smartphone) becomes a personalized access point and a service hub from the patient’s MSN to larger healthcare system.

Being mobile and using open network environments, data collection and transfer must be kept private as well as strict secure access must be applied [10], [5]. Many medical devices on the recent market are vulnerable to attacks, see examples in [16], [6]. We consider a generic system architecture where selected technologies are integrated to support security on the patient side, i.e., in patient’s MSN-based m-Health system.

Our security approach is based on the standardized protocol for Internet—Host Identity Protocol, HIP [4]. Recently, HIP has induced several promising security mechanisms for mobile networks and IoT-devices [17], [19], [7], [13]. In this paper, we contribute an MSN security solution for m-Health systems. It provides confidentiality of data transmission over insecure network, access control, fallback mechanism, revocation procedure, and certificate-based user authorization including temporary role delegation and authenticity of communications of patients with healthcare services and medical personnel. We have implemented a prototype system that demonstrates the feasibility of proposed security solutions for such specific and constrained IoT-devices as medical sensors.

The rest of the paper is organized as follows. Section II introduces the system architecture to attach a personal m-Health system with healthcare services. Section III describes scenarios when and what security is needed. In section IV we propose a lightweight key exchange scheme and in section V we make security analysis for different types of attacks. Section VI reports experimental study of our solution. Section VII contrasts our results with related work. Section VIII summarizes the paper.

II. SYSTEM ARCHITECTURE

The proposed system architecture aims at a wide class of healthcare systems (Fig. 1). We employ the known approach of personal mobile gateways [21], [11], which is widely accepted in emerging m-Health scenarios. Patient’s m-Health system is organized over the MSN and attached to a healthcare backend system via the patient’s gateway. The healthcare system collects all data and provides services. Medical facilities (e.g., in hospital) becomes accessible by remote participants (i.e., patients and medical personnel on behalf of them) and additional network data flow appear.

All MSN devices form a private information space of the patient. In general, the space covers Body Area Network (BAN) and Personal Area Network (PAN). The BAN subsystem consists of wearable and implantable devices. ECG or glucose sensors, RFID tags, insulin pumps and accelerometers

Fig. 1. Generic architecture of healthcare system: each personal m-Health system is attached to healthcare services.
are examples of such components. The PAN subsystem is composed of environmental sensors deployed around as well as of portable and mobile devices that belong to the patient. Temperature and humidity sensors, RFID readers, PDAs, and smartphones are rich sources of personal and environmental data important for healthcare services.

Each patient’s m-Health system includes a gateway, which is responsible for communication between MSN devices and all the outside world. The gateway aggregates, processes, and transfers information to the healthcare system. The gateway is a control point for making decisions on which data from the private MSN space to transfer to the system.

Transmission distance in MSN does not exceed 1-2 m. The IEEE 802.15.6 and 802.15.4/ZigBee standards suit well for this short range radio communication; they also become available on medical sensors recently appearing on the market.

Digital healthcare services run on backend servers physically located in medical facility or in clouds. Services need input data from the MSN and surrounding patient’s environment. They can also use information about status/outcome of other services. For instance, remote monitoring of patient’s well-being is a rich family of possible healthcare services.

Instant access to the real-time data on the patient side is an important requirement. One example is an emergency treatment outside of medical facilities. Occasionally there may be no Internet connection for the gateway. To ensure dependability the architecture introduces Portable Medical Terminal (PMT) for medical personnel on the patient side. PMT is very similar to the gateway and allows medical personnel to directly access patient’s MSN. In the normal operation mode, PMT communicates with the gateway. In the fallback mode, when the gateway is unavailable, PMT directly communicates with any MSN device. To preserve constrained resources of the sensors, the fallback mode is activated only if the gateway is unavailable. For instance it happens when the patient cannot function himself, the gateway device is lost, broken, stolen, or its battery is empty.

In such MSN-based IoT-oriented systems, enabling security and its smartness on the mobile patient side is one the most crucial problems [10], [20]. We distinguish the following person-related communication channels (Fig. 2). They are key targets for m-Health system security in our architecture.

**CH1 Sensors to gateway communication:** A sensor regularly transmits data to the gateway for processing, aggregation, and feed of healthcare services. Short range radio is used.

**CH2 Gateway to healthcare system:** The gateway forwards personal MSN data (possibly filtered and aggregated) to make them available for healthcare services. Wireless Internet connection is used.

**CH3 Sensors to PMT (fallback mode):** The channel is activated in emergency cases, when communication via the gateway is impossible. It is used also for configuring a new sensor or gateway in the MSN. Short range radio is used.

**CH4 Gateway to PMT (normal operation mode):** Medical personnel access instant data from the MSN and issue commands to medical devices. Short range radio is used, so not imposing additional demands for PMT hardware.

The architecture makes resource-constrained sensors pure data providers; they almost always communicate with the gateway only. The latter is relatively powerful and able to perform non-trivial logic for communicating with services and making rational decisions. All intensive processing is delegated to the backend infrastructure, which has enough computational capacity and ensures stability.

All the channels are subject to “smart security” when security solutions adapt to dynamic situations [9]. For healthcare systems, it is especially important in emergency and other critical scenarios since network connectivity or its participants are changing unpredictably at run-time.

### III. Security solutions

We aim at protection of sensitive medical data and patient’s well-being as well as at prevention of malicious adversary from gaining the control over devices in MSN. All network communications in the system are encrypted and data integrity is protected. Communication parties must be mutually authenticated using secure key exchange.

Secure key exchange is one of the most resource demanding operations. Due to this reason we apply different key exchange schemes depending on the communication channel.

**CH1 Sensors to gateway communication:** Since this channel is established in a secure environment, preshared keys are used. They are installed at the time of device configuration by medical personnel or manufacturer.

**CH2 Gateway to healthcare system:** Since gateway is a powerful enough device and has an Internet access, the standard HIP key exchange is utilized.

**CH3 Sensors to PMT:** Since very constrained devices are involved, a lightweight key exchange scheme is used for mutual authentication in access control. We apply own custom key exchange scheme described in Section IV.

---

**Fig. 2. Communications channels in a m-Health system**
CH4 Gateway to PMT: To keep simplicity and light hardware requirements at PMT we employ the same key exchange scheme as for CH3.

After the key exchange procedure both parties will have a shared secret key. Then the key is used to encrypt and to protect integrity of all subsequent communications. Although concrete cryptographic primitives depend on the implementation, we expect the sufficiency of the AES-CTR algorithm for encryption and AES-CMAC algorithm for protecting the integrity of messages.

To prevent an abuse of the fallback mode the gateway blocks fallback communications while it is operational. One way to implement it is to transmit periodic signals—beacons. Each sensor keeps a track of received beacons and if there are no beacons received for some time interval (detection interval) then the sensor switches to accepting pairing with PMT. Any received valid gateway beacon will immediately switch the sensor to not accepting any pairing request. To prevent DoS attacks any beacon packet is MAC protected. To prevent replay attacks a packet includes an unique nonce. Sensors do not remove shared keys whenever the gateway is lost; they continue to use the keys after gateway restoration. Values of detection interval and period between beacon transmissions depend on a duty cycle; this issue is beyond the scope of this paper. The proposed solution secures sensors from the unauthorized access and conserves sensor’s energy still providing accessibility of sensors in case of gateway malfunction.

To tackle the issue of stolen PMTs each PMT is equipped with a time-limited certificate. It is validated during the key exchange procedure. Certificates also contain an access control related information: access rights and device identity. Examples of possible access rights are: an access to non-private data (vital parameters), an access to the patient identity, a non-dangerous parameters configuration, a life-critical parameters configuration, issuing commands for implantable actuators (pacemakers, defibrillators, and other devices). Configuration with certificates is made before taken out on a shift. A PMT also requires a personal PIN code or a password from medical staff to operate. Finally, patient’s gateway device warns her/him about incoming communications from a PMT and allows prevention of them. The gateway can also check if the certificate was revoked using the global list of revoked certificates for lost/stolen devices if Internet connection is available. Since certificate lifetime is limited sensors store revoked certificates only until expiration. These measures together render improbable serious damage from a stolen PMT.

Smart security mechanisms can be further constructed to simplify access control and user experience. Depending on the surrounding environment, medical sensors readings, and the policy, the gateway makes decisions to omit warning of the patient about incoming communications from PMT or cease to send beacons to enable fallback mode. That can be done if an emergency situation is detected.

IV. LIGHTWEIGHT KEY EXCHANGE

We propose HIP DEX [13] based key exchange scheme to secure communications between the PMT and patient’s devices (short range radio). We apply the same scheme between gateway and PMT to not overcomplicate system architecture. Our symbol notation is summarized in Table I.

HIP DEX is a lightweight key exchange protocol. It provides DoS attack protection due to a cryptographic puzzle mechanism. HIP DEX uses no hash function, has fixed cryptographic primitives, and requires less than 450 bytes transmitted for handshake. Other known lightweight key exchange schemes either require an additional infrastructure for distributed computing (e.g., DHIP [17]), have an insufficient security level (e.g., LHIP [7]), or are too complicated for resource-constrained device (e.g., IKE [8]).

Conventional certificates require much computational power and memory. We utilize Elliptic Curve Qu-Vanstone (ECQV) implicit certificates [18] to reduce computation load. The ECQV implicit certificate needs only one EC multiplication, one EC addition, and one hash function calculation to verify the certificate. An implicit certificate is used to derive a public key of certificate holder. If the certificate is valid (i.e., issued by the authority), then the certificate holder will possess the corresponding private key. We propose transmitting implicit certificates instead of Host Identities (ECC public keys) like it is done in HIP DEX. The ECQV certificate is only slightly larger than the public key it is replacing.

The public key of host $U$ can be derived from $Cert_U$ as

$$Q_U = \text{Hash}(Cert_U) \ast P_U + Q_{CA},$$

where $Q_{CA}$ is Certificate Authority (CA) public key, and $P_U$ is EC point stored in the implicit certificate. Details of certificate issuing can be found in [18].

Our key exchange scheme differs from HIP DEX because of the inclusion of certificate verification. Second difference from the standard HIP is that our scheme does not establish IPSEC associations after key exchange: there may be no IP stack in the sensor nodes. Our scheme uses derived keys to encrypt and MAC-protect all subsequent packets using the AES-CTR and AES-CMAC algorithms.

Our key exchange scheme is presented in Fig. 3. Initiator $I$ of key exchange is always a PMT. Its responder $R$ is a sensor or gateway. The key exchange is composed from the four packets.

### TABLE I: SYMBOL NOTATIONS

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Q_{CA}$</td>
<td>Public key of Certificate Authority</td>
</tr>
<tr>
<td>$D_{CA}$</td>
<td>Private key of Certificate Authority</td>
</tr>
<tr>
<td>$Q_I$, $Q_R$</td>
<td>Public keys of initiator $I$ and responder $R$</td>
</tr>
<tr>
<td>$D_I$, $D_R$</td>
<td>Private keys of initiator $I$ and responder $R$</td>
</tr>
<tr>
<td>$Cert_I$, $Cert_R$</td>
<td>Certificates of initiator $I$ and responder $R$</td>
</tr>
<tr>
<td>$SK$</td>
<td>Shared key derived using DH algorithm</td>
</tr>
<tr>
<td>$G$</td>
<td>Generator of the cyclic subgroup on the elliptic curve</td>
</tr>
<tr>
<td>$[X]_k$</td>
<td>Least $k$ significant bits of $X$</td>
</tr>
<tr>
<td>CMAC($K$, $X$)</td>
<td>MAC function of $X$ with key $K$</td>
</tr>
</tbody>
</table>
I1: The packet is a trigger for the key exchange. It contains only the initiator’s Host Identity Tag (HIT) [13]. The processing of the packet requires no cryptography or state.

R1: The packet is a response to the I1 packet. It contains a cryptographic Puzzle, which is easy to check and hard to solve. The packet also contains responder’s certificate CertR. Processing of this packet includes solving the cryptographic puzzle. The initiator also processes the ECQV certificate to obtain a public key of the responder, which is then used in Diffie-Hellman algorithm to derive a shared secret. That shared secret allows encrypting a random value SecretX and MAC protect a response packet.

I2: The packet contains a solution to the puzzle from the packet R1. It also contains the initiator’s ECQV certificate CertI. The responder checks the puzzle solution before performing any other heavy operations: computing an ECC public key from the certificate, deriving the Diffie-Hellman shared secret, and checking MAC. The responder also checks that the certificate is valid (i.e., it is issued to the gateway or the PMT), is not expired, and has necessary access rights.

R2: The packet contains a MAC protected and encrypted random value SecretY used to calculate the shared keys.

After the successful key exchange both parties have keys for symmetrical cryptography, which are then used to encrypt and MAC-protect all subsequent communications.

Note that responders in our scheme (i.e., sensors and gateways) have certificates too. They are not limited in validity time and cannot be used to initiate key exchange. They are used to mitigate impersonation attacks and are configured once devices are installed.

V. SECURITY ANALYSIS

Let us review security properties of the proposed solutions. We consider that an adversary can intercept all packets, send forged packets to any entity in the network, and can gain control over a PMT. However, we assume that a certificate authority private key is not compromised.

Security of key exchanges: Since there is no key exchange on communication channel CH1, there are no attack vectors there. For discussion on standard HIP key exchange security used on channel CH2 refer to [14].

The custom lightweight key exchange used on CH3 and CH4 relies on the EC scalar-point multiplication and therefore is provably secured under the random oracle model, assuming that the discrete logarithm problem over the subgroup is intractable. Security properties of proposed scheme are similar to the HIP key exchange.

The eavesdropping is ineffective as the proposed key exchange extends the security strength of the standard ECDH key agreement. The proposed key exchange also mutually authenticates all parties because it requires them to possess a corresponding private key, thus preventing Impersonate and Masquerade attacks. To prevent replay attacks key exchange relies on a random nonce generated by the responder each time. DoS attacks on the responder are mitigated with the cryptographic puzzle mechanism.

Attacks using data packets: The eavesdropping is useless as all sensitive data is encrypted at all communication channels. Since all data packets after a key establishment are supposed to include an always increasing nonce and be MAC protected, packet replay attacks are impossible. Without a correct shared key the attacker also can’t forge packets.

Attacks using stolen PMT: If the adversary could acquire a PMT it may present a threat for all patients in the system. That problem is mitigated by limiting the lifetime of certificates issued to medical terminals. Medical terminals should also require entering a PIN code or a password which will greatly increase the difficulty of performing such attack. Lastly, a personal gateway warns a patient about an incoming pairing request and provides possibility to block it. Therefore unauthorized access with a stolen gateway is not a threat.

DoS attacks: DoS attacks using data packets are not efficient on all communication channels as packets will be discarded right after the MAC check. There may be other vectors of DoS attack like jamming but it is impossible to cope with that attacks without special hardware. DoS attacks using key exchange packets are inefficient as responder requires a proof of work before doing heavy computations. It is impossible to mount a DoS attack on a sensor’s battery if a gateway is present since sensors do not process any external packets in that case.
**Gateway jamming:** The proposed architecture relies on a gateway sending beacon packets to sensors. There may be an attack preventing sensors from receiving such packets. In that case they still are protected by key exchange scheme but there may be an energy drain attack. It is not an issue because the gateway will be able to detect such attacks and therefore warn the user about communication problems immediately.

VI. Evaluation

The proposed design is evaluated in terms of performance and resource demands. We focus on the feasibility of our architecture for resource constrained devices. Since a gateway is powerful enough, we do not evaluate the performance for CH2 (between gateway and healthcare services).

Real medical devices on the market are proprietary, and they are hard to experimental programming. To simulate such devices we used common WSN motes in our experiments. TelosB\(^1\) has capabilities similar to recent medical devices. Table II provides a comparison of capabilities between TelosB and MAXIM MAXQ2010 based insulin pump\(^2\). Prior work [11] evaluated the feasibility of HIP-based solutions for Imote2\(^3\). However, Imote2 is essentially more powerful than real medical devices we focus on.

TelosB motes have IEEE 802.15.4 compliant CC2420 RF transceivers. The hardware includes 8 MHz, 16-bit MCU with 10 Kbyte RAM and 48 Kbyte ROM. CC2420 RF transceiver has maximum data rate of 250 kbps and frequency band of 2400 MHz. Our implementation uses NesC on TinyOS\(^4\) 2.1.2. ECC (for EC arithmetic operations) and natural number (NN, for large natural number operations) interfaces are adopted from TinyECC configurable library \[12\]. TinyECC was configured to operate with the secp160r1 elliptic curve because the latter has a reasonable security level and allows fast EC operations (due to special nature of a parameters). TinyECC with Barrett Reduction is used to speed up modulo operations, Hybrid multiplication and squaring for the integer multiplication, and Projective Coordinate Systems for the point addition.

Our testbed setup consists of three TelosB nodes to simulate a medical sensor, a wireless interface for the gateway, and a wireless interface for the PMT. Two latter are connected to laptops via USB cables for forwarding packets from the wireless network to the application on the laptop and backwards. The reason is our assumption that both gateway and PMT are rather powerful devices that support two network interfaces (for low range PAN and for access to the Internet). We evaluated the following scenarios.

1) Authentication between PMT and gateway.
2) Authentication between PMT and sensor.
3) Gateway forwards data to the backend system.

---

**Table II**

<table>
<thead>
<tr>
<th>Resource</th>
<th>TelosB</th>
<th>MAXQ2010</th>
<th>Imote2</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>10kB</td>
<td>2kB</td>
<td>256kB</td>
</tr>
<tr>
<td>ROM</td>
<td>48kB</td>
<td>64kB</td>
<td>32MB</td>
</tr>
<tr>
<td>CPU</td>
<td>16-bit</td>
<td>16-bit</td>
<td>32-bit</td>
</tr>
<tr>
<td>Freq</td>
<td>8MHz</td>
<td>1MHz</td>
<td>13-416MHz</td>
</tr>
</tbody>
</table>

**Table III**

<table>
<thead>
<tr>
<th>Operation</th>
<th>Duration</th>
<th>Current</th>
<th>Energy</th>
</tr>
</thead>
<tbody>
<tr>
<td>I1 proc. (sensor)</td>
<td>3.91 ms</td>
<td>2.2 mA</td>
<td>0.03 mJ</td>
</tr>
<tr>
<td>R1 proc. (PMT)</td>
<td>50.13 ms</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>I2 proc. (sensor)</td>
<td>10.89 s</td>
<td>2.2 mA</td>
<td>79.1 mJ</td>
</tr>
<tr>
<td>R2 proc. (PMT)</td>
<td>0.23 ms</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Data transmission</td>
<td>13.8 ms</td>
<td>19.4 mA</td>
<td>0.9 mJ</td>
</tr>
<tr>
<td>Total handshake</td>
<td>10.95 s</td>
<td>—</td>
<td>80.03 mJ</td>
</tr>
<tr>
<td>ECDH key gen.</td>
<td>5.41 s</td>
<td>2.2 mA</td>
<td>39.3 mJ</td>
</tr>
<tr>
<td>ECQV key proc.</td>
<td>5.35 s</td>
<td>2.2 mA</td>
<td>38.8 mJ</td>
</tr>
</tbody>
</table>

The measurements are taken in terms of execution time, memory, and energy consumption. We use Ironside IMT6000 digital multimeter in ammeter mode to measure immediate electric current with 0.1 mA precision. These values are converted to energy drain using known voltage (3.3V) and measured time. The execution times are measured directly on the sensor node using internal 32kHz counter and on the laptops using system time. We measure time and energy needed to process each handshake packet. We also measure resources needed for most costly operations on sensor (ECDH, ECQV certificate processing). We run each scenario 20 times and calculate an average for each measurement.

Our implementation required total of 4572 bytes of RAM and 27341 bytes of ROM to be installed on a device.

Results of measurements are provided in Table III. Most of the delay is introduced by extremely costly EC operations calculated during I2 packet processing. These operations can’t be omitted because at least one EC multiplication is needed for DH and at least one another for ECQV certificate processing. For the best of our knowledge there are no methods for ECDH and certificate verification faster than that. Total energy consumption is about 80 mJ per handshake. Typical LR44 battery capacity of 150 mAh will be enough for more than 20,000 handshakes.

Note that a key establishment with several sensors does not require much more time than a handshake with a single sensor, as most of the delay is introduced by the sensor processing I2 packet. Since all sensors work in parallel, then pairing with several sensors only PMT’s part of handshakes processing will be sequential. Thus we estimate a total handshake time with \( k \) sensors as \( 10.89 + 0.064 \times k \) seconds. It is a reasonable delay as pairing with sensors directly is supposed to be very rare operation. The handshake between the PMT and the gateway is much faster and takes only 228ms.

The beacon broadcasting mechanism efficiently protected sensor from unauthorized access in our prototype as the sensor ignored all incoming I1 and I2 packets when the gateway was functioning. Since the gateway was removed the sensor
successfully established association with the PMT.

Our experiments show that the proposed system can be implemented on devices capacity-equivalent to real medical devices on the market. The proposed key exchange scheme introduces reasonable delay and requires small energy resources.

VII. RELATED WORK

Denning et al. [1] secure Implantable Medical Devices (IMDs) using Communication Cloaker. In presence of such a device an IMD ignores all incoming communications from all other parties. Gollakota et al. [3] proposed physical protection of IMDs with a jammer-cum-receiver device that causes IMD to ignore communications as well as actively to jam all possible external communications. Garcia-Morchon et al. [2] proposed a general security framework for MSNs. It does not tackle constraint nature of IMDs, does not focus on dependability, and does not use standardized protocols. Explicit certificates are employed, which is a costly solution for IMDs. Recent work [15] considered ECQV implicit certificates in WSN key exchange protocol. That proposal, however, does not provide DoS protection.

Our solution considers realistic communication modes for IoT settings and proposes a general solution that covers practical aspects of security for m-Health applications and benefits from standardized components.

VIII. CONCLUSION

This paper has presented a generic architecture for secure function and attachment of MSN-based m-Health systems as mobile components of a healthcare backend system. Our architecture utilizes a standardized HIP security base and extends it for mobile healthcare scenarios in the IoT context. We provided security solutions for protecting private data on the mobile patient side and their transfer outside the m-Health system. We introduced implicit certificates in HIP DEX handshakes for supporting portable terminals of medical personnel on the mobile patient side. The feasibility and performance of the designed solutions were evaluated using an experimental implementation and testbed. Medical devices are simulated with easy-programmable devices of similar computational and network capabilities. The results enable implementation of ubiquitous access to the life treating medical devices while ensuring a high security level.

IX. ACKNOWLEDGEMENT

This work was supported by Academy of Finland project SEMOHealth and grant #14-07-00252 of the Russian Foundation for Basic Research.

REFERENCES


