# Secure Lightweight Protocols for Medical Device Monitoring

Andrei Gurtov
Helsinki Institute for Information Technology HIIT, Finland and ITMO University, Russia
gurtov@hiit.fi

Pawani Porambage
Centre for Wireless Communications
University of Oulu, Finland
pporamba@ee.oulu.fi

Ilya Nikolaevskiy
Department of Computer Science and Engineering
Aalto University, Finland,
Ilya.nikolaevskiy@aalto.fi

***Abstract*—In the present days, the health care costs are sky-rocketing and most developed nations, including EU and US, are struggling to keep the costs under control. One of the areas is related to monitoring and control of medical appliances embedded to human bodies, such as insulin pumps as heart pacers. Fortunately, recent technology advances make it possible to monitor the medical appliances remotely, greatly decreasing the need for personal doctor visits. Naturally, remote wireless monitoring of such crucial appliances poses several formidable technological challenges including security of data communication, device authentication, attack resistance, and seamless connectivity. A remote monitoring protocol must be executed in a resource-constrained environment with energy efficiency. The recently proposed Diet Exchange for Host Identity Protocol (HIP) could solve most of security issues of remote appliance monitoring. However, it has to be developed to run in an embedded device environment; its security properties must be triple-checked against the stringent requirements; potential privacy issues must be addressed; protocol messages and cryptographic mechanisms must be adopted to wireless sensor standards. Although bearing high risks of provable security and patient faith, remote monitoring of health appliances could create breakthroughs in healthcare cost reduction and bring great benefits of individuals and the society.**

## I. INTRODUCTION

Implantable Medical Devices (IMDs) such as pacemakers, drug pumps, implantable cardioverter defibrillators (ICDs), and neurostimulators are becoming commonplace. In USA alone, millions people live with such devices; only the cost of diabetes care are estimated to increase from $156 000 000 000 in 2010 to $192 000 000 000 in 2020 with about 20 million sick people [3]. Periodic tune up of commercial IMDs require a patient to spend several days in the hospital where the physicians can use special device programmers to monitor and control the IMD. A cost of a hospital stay in USA reaches 1000-2000 $ per day and presents a high burden on the national healthcare system. With secure remote monitoring capabilities, patients could be checked without a need to interrupt their daily activities and saving the costs of the hospital stays.

Currently, some of the IMDs use plain-text protocols to communicate using wireless over short-range ranges. A recent study revealed several successful attacks on one of the IMD models available on the market [1]. By reverse-engineering the communication protocol, researchers were able to compromise patient privacy (determine whether the patient has IMD, determine its particular model, serial ID, retrieve patient history and personal data, obtain telemetry information). Even worse, they were able to make active attacks directly threatening the patient's life (change of device settings, change therapy, or cause electric shock on the heart).

The study [1] made several proposals how to improve the security situation. The first measure they propose is to notify the patient of potential malicious activity with their IMD. For notification they suggest using a wireless activity detection circuitry together with a piezo-element that beeps when a proper radio signal is present. On the positive side, such a proposal could indeed make the patient aware of radio activity that would enable him or her to leave the dangerous area. It also operates based on external Radio Frequency (RF) energy and thus does not deplete the primary IMD battery. However, audible signals could be also used by attackers to detect people with IMDs by activating the RF transmitter among a group of people. Furthermore, the patient would might not be able to prevent malicious activity even being aware of it e.g., due to lack of time to react or less knowledge about prevention mechanisms.

As the next step, researchers were able to introduce simple cryptography support for communication between IMD and the programming device. The devices were able to encrypt communication using only RF energy thus avoiding the extra power overhead. The assumption was that the security key was somehow pre-recorded to IMD and the programming device. However, the mechanism to negotiate the key dynamically and securely was not developed. Latest proposals include the use of external shield to protect IMD [15].

IEEE standard 802.15.4 defined the protocol and compatible interconnection for data communication devices using low-data-rate, low-power, and low-complexity short-

ISSN 2305-7254

range RF transmissions in a wireless personal area network (WPAN) [7]. WPANs are used to convey information over relatively short distances. Unlike wireless local area networks (WLANs), connections effected via WPANs involve little or no infrastructure. This feature allows small, power-efficient, inexpensive solutions to be implemented for a wide range of devices. 802.15.4 is the basis for the ZigBee, WirelessHART, and MiWi specification, each of which further attempts to offer a complete networking solution by developing the upper layers which are not covered by the standard. Alternatively, it can be used with 6LoWPAN [9] and standard Internet protocols to build a Wireless Embedded Internet.

IEEE 802.15.6 is a task group for WBAN or BAN, short for (Wireless) Body Area Network. BAN consists of a set of mobile and compact intercommunicating sensors, either wearable or implanted into the human body, which monitor vital body parameters and movements. These devices, communicating through wireless technologies, transmit data from the body to a home base station, from where the data can be forwarded to a hospital, clinic or elsewhere, real-time. A new IEEE task group 802.15.9 targets to develop several Key Management Protocols (KMP) for the use with 802.15.4 and 802.15.6 short-range radio communication links. Light IKEv2, PANA, Diet Host Identity Protocol (HIP) are being considered as possible protocols for secure communication.

In this paper, we briefly explain the general requirements of an effective secure IMD monitoring architecture that provide pervasive and remote connectivity. Furthermore, we discuss a tentative security approach that can be integrated into IMD network architectures for trustworthy connectivity. The proposed security scheme includes lightweight key management and user authentication.

The rest of this paper is organized as follows. In Section II we give overall requirements for secure remote monitoring of medical devices. In Section III we outline the necessary components for the architecture and present its holistic view in Section IV. Section V describes the lightweight cryptographic protocols involved in the architecture. Section VI concludes the paper.

## II. General Requirements

Remote monitoring of IMDs is a new area in wireless networking that is likely to become one of the "hot" research areas in the near future. Leading largely to uncharted territory, the area offers low-hanging fruits and breakthroughs that can potentially have great impact on the society. The paper [4] only reveals the importance of the area and illuminates the need for a principled and deeper investigation into prevention mechanisms, detection mechanisms, audit mechanisms, deterrents, and methods that enhance patient awareness and ensure consent. Moreover, the fundamental challenge will be to develop methods that appropriately balance security and privacy with traditional goals such as safety and effectiveness. Following high-level objectives can be stated for secure remote IMD monitoring architecture:

### *A. High protection of the patient data*

The foremost goal of remote IMD monitoring architecture is to prevent unauthorized access to patient data and tampering with the device settings. An attacker should not be able to discover the presence of IMD nor trigger battery-depleting Denial-of-Service attacks. The patient data should be protected end-to-end, from the IMD up to physician's computer, to avoid being compromised by an attacker through Trojans in the relay devices and public networks.

### *B. Universal connectivity*

The patient's status should be available to physician regardless of the patient's present location. That mandates the use of public cellular and Wi-Fi networks to transmit the status data. Proper mobility and multihoming support is therefore required from the communication protocol. Transparent authentication architecture, such as [8], would facilitate access to such Wi-Fi communities as Wippies/FON since the patient may not have a capability to manually authenticate to network, e.g. using traditional captive DNS pages with login/password data. WBAN systems would have to ensure seamless data transfer across standards such as Bluetooth, ZigBee to promote information exchange, plug and play device interaction. Further, the systems would have to be scalable, ensure efficient migration across networks and offer uninterrupted connectivity.

### *C. Use of conventional mobile phones as a terminal*

The use of commercial smartphones or PDAs as a relay device between an IMD and the Internet has obvious benefits of cost savings compared to custom-made devices. Furthermore, through higher use volumes and open-source nature of software, higher reliability and security could be achieved, preventing potentially fatal software failures. Commercial phones can utilize public cellular network and hotspot connectivity.

### *D. Power efficiency*

Since IMDs have often non-rechargeable batteries, new communication protocols and cryptographic mechanisms should introduce as little as possible additional computational overhead. Solutions utilizing remote RF energy for communication instead of local battery are highly preferred. Furthermore, novel power source technologies for IMD e.g. utilizing patient's movements to generate electricity and recharge IMD batteries should be explored.

### *E. Accessibility in case of emergency*

While the foreseen communication architecture for IMDs would guarantee patient privacy and only authorized

access, sometimes the presence of "backdoors" is required to enable access in emergency situations. When the patient requires urgent treatment and could not give consent on IMD access, alternative mechanism to overcome access control might be needed. That may include consent given by the relatives that can reveal the encryption keys; close-body contact necessary to enable IMD access, or automatic state detection disabling security then more good than harm could be made by 3rd party interference.

### F. System Devices

The sensors used in WBAN would have to be low on complexity, small in form factor, light in weight, power efficient, easy to use and reconfigurable. Further, the storage devices need to facilitate remote storage and viewing of patient data as well as access to external processing and analysis tools via the Internet.

### G. Non-invasion of privacy

People might consider the WBAN technology as a potential threat to freedom, if the applications go beyond 'secure' medical usage. Social acceptance would be the key to this technology finding a wider application.

### H. Sensor validation

Pervasive sensing devices are subject to inherent communication and hardware constraints including unreliable wired/wireless network links, interference and limited power reserves. This may result in erroneous datasets being transmitted back to the end user. It is of the utmost importance especially within a healthcare domain that all sensor readings are validated. This helps to reduce false alarm generation and to identify possible weaknesses within the hardware and software design.

### I. Data consistency

Data residing on multiple mobile devices and wireless patient motes need to be collected and analyzed in a seamless fashion. Within Body Area Networks, vital patient datasets may be fragmented over a number of nodes and across a number of networked PCs or Laptops. If a medical practitioner's mobile device does not contain all known information then the quality of patient care may degrade.

## III. Universally available secure connectivity to IMDs

In order to realize the aforementioned vision we need to (1) develop a network architecture to link the IMD, the patient's gateway, the cloud infrastructure for data storage and to provide remote access by physician's PC; (2) develop lightweight key management protocols for securing communication between IMD and gateway; (3) develop efficient user authentication to access medical devices regularly and in case of emergency.

### 1) Medical network architecture

We would like to research a proper architecture combining several on-body medical devices on the patient, his gateway device, external devices provided by the hospital or paramedic team, outside connection to the cloud storage of patient data, and patient's own doctor providing treatment from a remote location.

When communicating with the rest of the Internet which requires IP, the wireless access point can serve as a conversion point, between an IP-less IMD link and the fixed IP-based network. A cryptographic delegation mechanism can be employed to provide the access point with necessary authority to act as a middleman for the IMD without introducing a possibility of the man-in-the-middle attacks (e.g. a false access point installed by an adversary). Patient's smartphone may also relay data from IMDs to the cloud directly via cellular network connection.

The use of communication protocols in infrastructureless environments, such as sensor, mesh or MANET networks, requires re-working of traditional networking services such as name resolution and rendezvous. Since there are no centralized entities being able to provide the function of the DNS or rendezvous server, the infrastructure functions must be decentralized in a P2P way so that other network nodes participate in message routing. A naïve approach can deploy broadcast to locate other nodes, while a more sophisticated way would integrate with existing routing protocols to reduce battery and computational overhead for other nodes.

### 2) Lightweight key management protocols

In order to achieve sufficiently secure and lightweight key exchange protocols for IMDs we propose following research approach with a novel combination of three cryptographic mechanisms: elliptic curves (EC), implicit certificates, and use of hardware symmetric cryptography in the place of outdated hash functions.

Elliptic Curve Cryptography (ECC) is a relatively new trend in Public key cryptography which provides encryption, digital signature and key agreement. Variables and coefficients are all in a predefined finite field. Curve domain parameters should be also predefined. Messages and keys are described as EC points. ECC provides an equal security to well known RSA with smaller key sizes with an adequate security. Due to the smaller key size, it reduces the processing overhead and memory utilization.

Elliptic Curve Qu-Vanstone (ECQV) is an implicit certificate scheme based on ECC. The certificate consists of user identity and public key re-construction data. Comparing to the traditional certificate schemes, this provides smaller certificate size, low computational complexity, and less processing time. Computations are performed on a predefined EC known by both requester and certificate authority (CA). Deriving a public key is faster than deriving a digital signature.

In order to fulfill the aforementioned objectives, a feasible two phase keying mechanism can be designed as follows: First step is to generate implicit certificates using ECQV certificate scheme, and distribute them among the sensor nodes. The certificate generation and distribution is performed by CA which can be taken as the cluster head node. When the sensor nodes posses their certificates, they can use certificates to compute their keying materials. In the second phase, sensor nodes can initiate key establishment process with the neighboring nodes using HIP-DEX and Diffie-Hillman key exchange protocols. In both phases, it is assumed that the EC domain parameters are common and known by all nodes.

As currently used hash functions such as SHA-1 become increasingly unreliable due to recent attacks, we plan to explore the possibility to use symmetric cryptographic mechanisms, such as certain AES modes available in hardware, as a way to replace hash functions necessary in a key generation process.

*3) User authentication*

The normal user access procedures to IMD should include encrypted communication using keys established using lightweight key management protocol. However, emergency access may need to turn off security when there is no time or possibility to perform normal access, e.g., in a case of accident in a remote location. Therefore, on-the-spot user authentication using a smart card and password is needed. Furthermore, reasonable mechanisms for disabling security altogether need to be studied.

Symmetric key cryptography is highly efficient. But the major drawback is to share the common secret which is the shared key between two communicating parties. Public key encryption is highly resource consuming. When there is a session key for each communication scenario, data can be encrypted using a symmetric key algorithm such as AES which is already supported in IEEE 802.15.4 standard. No need to keep the public keys of all the nodes in the network in the memory, because the keys are clarified in each communication scenario.

## IV. Medical Network Architecture

Our system for medical monitoring (see Figure 1) comprises several key components:

a. Personal Area Network (PAN) which includes multiple low-power medical sensors placed on a patient's body and performing long-term reading of vital health parameters (e.g. blood pressure, pulse, etc.) and a single on-body gateway which serves as a full-functional node for medical sensors and has two wireless interfaces (one short range wireless interface, e.g. 802.15.4 for maintaining connection with medical sensors or other devices in short range, and one long-range wireless interface, e.g. UMTS or 802.11, for maintaining Internet connection);

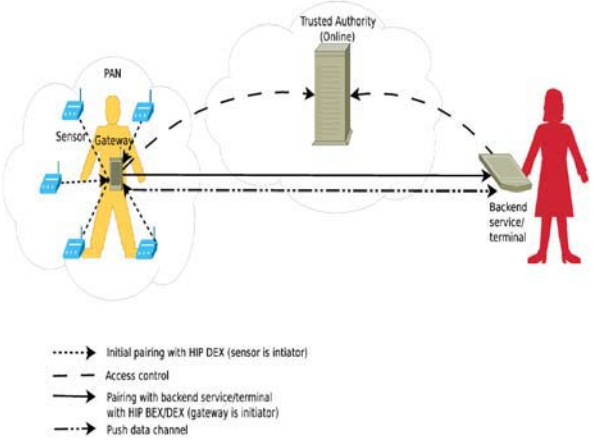


Fig. 1. Privacy-preserving communication architecture for IMDs.

b. A trusted authority (TA) which is a node trusted by all other parties belonging to the system and responsible for managing identities, revocation statuses, and access rights;

c. A backend server responsible for storing collected patient's sensor readings (a PAN gateway when connected to the Internet always establishes a secure channel to a backend server and uploads sensor readings to it periodically);

d. A portable terminal with a graphical interface used by accredited personnel (this does not necessarily need to be only patient's doctor, but may include any emergency services such as paramedics or police, having various access rights for reading patient's data). A portable terminal can retrieve patients' sensor readings from backend server, or accept readings directly from the gateway node after establishing a security association. The last is needed in emergency situations when no Internet connection is available. In exceptional cases when the gateway is not functioning or lost while the patient's life is in danger, the portable terminal may need to have access directly to the sensors.

Though if the nodes, especially gateways, due to absence of Internet connectivity do not have an ability to verify the status of the certificate, there is a chance that an intended attacker can receive access to confidential information.

To combat this, in our system medical personnel is granted two types of certificates: (i) Permanent membership certificate (PMC) which a node receives during pre-configuration (e.g. during initial pairing). (ii) On-demand short term certificates (OSTC) granted by TA for a short period of time (e.g. an hour or a day) based on the status of the PMC of the node.

For medical personnel both PMC and OSTC are stored on a personal smart card which is worn much like other physical keys, e.g. on a key chain. Moreover, these smart cards are required to be tamperproof to avoid cloning. This will prevent a stolen OSTC from being used to access multiple gateways simultaneously. When needed, the smart card is inserted into a portable terminal used by doctors to provide medical help to patients with a medical sensor network.

Gateways and back-end servers unlike portable terminals need only the PMC. It is this certificate that as we described earlier is used for establishing a secure pairing with the backend server. The HIP DEX handshake is interrupted if certificate is invalid. It is a responsibility of the medical personnel to request a valid fresh OSTC certificate in a timely manner. For instance, OSTCs can be requested and loaded into the smart card before an ambulance departs to the patient's premises. Note that the OSTCs are granted based on the status of the PMC: if the PMC was revoked no OSTC will be granted. Verification of PMC certificates on various devices is done using the TA's root public key. The PMC should be transmitted after successful HIP handshake on request. Upon receiving a certificate the device checks its digital signature to assure that the certificate is authentic. Note that PMC is only used to authenticate portable terminals by TA and gateways by portable terminals and backend servers. The OSTC is used to authenticate portable terminal by gateways and sensors. We suggest using implicit certificates as OSTC to decrease computations complexity on the sensors. Usage of ECQV implicit certificate scheme only requires a block cipher based hash function (AES Modification Detection Codes (AESMDC2)), which is rather easy to implement in hardware. It allows sensors to process OSTCs and enables the fallback mode Since OSTC certificates have relatively short-time life cycles, such hash function is considered secure. It is possible to piggy-back ECQV implicit certificates in HIP DEX. Then responder uses this certificate to derive initiator's public key which is used further in the handshake. The certificate validation is not needed in this scheme because initiator will be able to correctly decrypt data and achieve shared secret key only if it possess correct private key, which is possible only in case of a valid certificate.

Current IMDs easily reveal patient's personal information such as the name and birthday. Introducing a naïve security could still leave the privacy issue unsolved if, for example, IMD still reveals its permanent identifier to unauthenticated third party. That could enable tracking the patient location based on its IMD identifier. Therefore, straightforward use of public key as an IMD identity is undesirable. Instead, privacy-preserving protocols should be applied, such as BLIND [14].

## V. LIGHTWEIGHT KEY MANAGMENT

The Host Identity Protocol (HIP) [10] was proposed to overcome the problem of using IP addresses for host identification and routing. The idea behind HIP is based on decoupling the network layer from the higher layers in the protocol stack architecture. HIP defines a new global name space, the Host Identity name space, thereby splitting the double meaning of IP addresses. When HIP is used, upper layers do not any more rely on IP addresses as host names. Instead, Host Identities are used in the transport protocol headers for establishing connections. IP addresses at the same time act purely as locators for routing packets towards the destination. For compatibility with IPv6 legacy applications, Host Identity is represented by a 128-bit long hash, the Host Identity Tag (HIT). HIP offers several benefits including end-to-end security, resistance to CPU and memory exhausting denial-of-service (DoS) attacks, NAT traversal, mobility and multihoming support.

In our architecture HIP DEX [12, 13, 16] between medical sensors and a gateway is running directly on a MAC layer which allows to save space (indeed this can be implemented as a variant of 6lowpan to allow header compression and save space). Because HIP DEX does not use signature algorithms, and certificates are not suitable for medical sensors due to limited processing power, and 128 bytes frame size in 802.15.4 radio which is too small to fit a certificate, a two factor authentication process is required to guarantee secure sensor to gateway communication.

Duplicate encryption performed on the link layer and on network layer by IPsec is an issue, especially if both layers use the same CPU for cryptographic operations. With hardware support present, link layer encryption may not significantly affect bandwidth, although may still consume the battery power. In some scenarios, e.g. using 802.11 WPA and HIP together, double encryption might be actually desirable for certain applications, as WPA has known vulnerabilities permitting its breakdown but it does provide a basic protection over the air. Possibly, a per-packet granularity for encryption would be appropriate. One potential approach is to employ HIP-based encryption for link-level security.

In last-hop wireless link, removing the IP header can save 20-40 bytes of the overhead. Furthermore, in many networks the MTU size might be considerably lower, e.g. in sensor networks, on the level of 50-200 bytes. The HIP Base Exchange control packets typically take 40-800 bytes, causing fragmentation. Therefore, developing a smaller HIP control packet by adding more round trips and using ecliptic curve cryptography (ECC) appears a promising approach. ECC would also help to save bandwidth which is often an issue for long-distance or low-power wireless communication.

When running HIP over wireless link, additional initial delay can result to multiple RTTs needed to perform the link-layer operation that enables exchange of HIP control

packets. Integrating link-layer and HIP messages together, subject to MTU and other restrictions, can produce significant latency reductions especially on long-delay links such as 3G.

## VII. Conclusion

In this paper we stressed the importance of developing an architecture for secure remote monitoring of personal medical devices. We outlined a feasible approach and proposed several mechanisms for secure communication between medical personnel and wearable medical devices on a patient. Lightweight key management protocols based on HIP Diet Exchange are able to accomplish secure key exchange in a way that does not produce additional attacks e.g. on depleting a device battery. The protocols are currently under standardization in the IEEE 802.15.9 working group.

## Acknowledgment

This work was supported by Academy of Finland project SEMOHealth. We also thank Dmitry Kuptsov, Dmitry Korzun and other members of the Networking Research Group at HIIT.

## References

[1] Halperin, Daniel; Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel (May 2008). "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses". *IEEE Symposium on Security and Privacy.*

[2] Jim Tomcik. *Wireless Health Initiatives And Body Area Networks: Physical Layer and MAC Characteristics*. Qualcomm Corporate Research and Development, 2009.

[3] Darrell M. Wilson, BAN and Diabetes a template for medical device communication. *IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)*. May, 2009.

[4] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel. Security and privacy for implantable medical devices. *IEEE Pervasive Computing, Special Issue on Implantable Electronics*, January 2008.

[5] T. Aura, A. Nagarajan, A. Gurtov, Analysis of the HIP Base Exchange Protocol, in *Proc. of the 10th Australasian Conference on Information Security and Privacy (ACISP)*, July 2005.

[6] R. Moskowitz. Progress with HIP and Future efforts. Presentation at *HIP Research Group meeting*, July 2009.

[7] IEEE Standard for Information technology. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), 2006.

[8] D. Kuptsov, A. Khurri, A. Gurtov, Distributed authentication architecture in Wireless LANs, in *Proc. of the 10th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'09)*, June 2009.

[9] 6LoWPAN. http://en.wikipedia.org/wiki/6lowpan.

[10] A. Gurtov, *Host Identity Protocol (HIP): Towards the Secure Mobile Internet*, ISBN 978-0-470-99790-1, Wiley and Sons, June 2008. (Hardcover, 332 p).

[11] A. Gurtov, I. Nikolaevsky, A. Lukyanenko, Using HIP DEX For Key Management And Access Control In Smart Objects, in *Proc. of Workshop on Smart Object Security*, March 2012.

[12] D. Kuptsov, B. Nechaev, and A. Gurtov, Securing Medical Sensor Network with HIP, *in Proc. of the 2nd International ICST Conference on Wireless Mobile Communication and Healthcare (MobiHealth'11)*, October 2011.

[13] A. Khurri, E. Vorobyeva, A. Gurtov, Performance of Host Identity Protocol on Lightweight Hardware, *in Proceedings of ACM MobiArch*, August 2007.

[14] Ylitalo, J.; Nikander, P. 2004. BLIND: A complete identity protection framework for end-points. *In Proceedings of the twelfth international.*