Security for Pervasive Healthcare

Oscar Garcia-Morchon, Thomas Falck, Tobias Heer, Klaus Wehrle

***Abstract*— Wireless sensor networks are going to allow for ubiquitous health monitoring, improving users' well-being, making the healthcare system more efficient, and helping to quickly react on emergency situations. Meeting the strict security needs of ubiquitous medical applications is a big challenge: safety and privacy of patient data has to be guaranteed all the way from the sensor nodes to the back-end services, the system has to fulfill latency needs, and lots of mobility is expected.**

In this paper, we introduce a deployment model for wireless sensor networks for pervasive healthcare based on the concepts of patient area and medical sensor networks. We propose a complete and efficient security framework organized into three layers, addressing the operational requirements and security needs at the patient area network, medical sensor network, and back-end levels. We specify how these layers are interconnected with each other as well as the needed security and privacy mechanisms that allow for the efficient and practical deployment of secure pervasive healthcare systems based on wireless sensor networks.

***Index Terms*— Medical Information Systems, Medical Sensor Network, Patient Area Network, Security.**

I. Introduction

NOWADAYS, sensor and wireless communication technologies are rapidly evolving and conquering new application areas in the healthcare domain. Wireless medical sensors ($WMSs$) are becoming smaller and more powerful, allowing for ubiquitous usage of a wide range of medical applications, such as chronic disease management. In the simplest healthcare setting, a fixed set of $WMSs$ forms the user's patient area network (PAN) allowing for health monitoring and measuring the user's vital signs. A gateway can allow the user or medical staff to access, gather, or process her medical data directly, or transmit it to a remote healthcare service. The ubiquitous use of $PANs$ enables pervasive health monitoring of users in their daily life, improving their well-being and quality of medical care, yet allowing for cost reduction in the healthcare sector [1]. Pervasive health monitoring in these diverse situations and locations is carried out by different organizations, such as surgeries, fitness centers, hospitals, or retirement homes by means of a medical sensor network (MSN) allowing authorized parties, such as medical staff, family, or sport trainers to access to the sensed health information. Thus, $PANs$ will not be isolated but will interact, coexist, and become a part of a world of professional $MSNs$, each comprising thousands of sensors, accommodating hundreds of users's $PANs$ (see Fig. 1 and related example). The exchange of users' medical data leads to privacy and security concerns, hence basic security services are required to fulfill legal regulations such as $HIPAA$ in the US [2] or the European Directive [3]. These concerns become especially challenging due to the resource-constrained nature of the wireless medical sensors, the strict latency requirements [9], and the mobility and scalability requirements of systems involving a multitude of parties [6].

II. Security for Pervasive Medical Sensor networks

We propose a flexible and extensible security framework [6] addressing both the hospital-centric approach predominant today, in which each healthcare institution has complete control on the medical data, and a patient-centric vision [5], where the patient controls her electronic health information (EHI). Our security framework comprises three

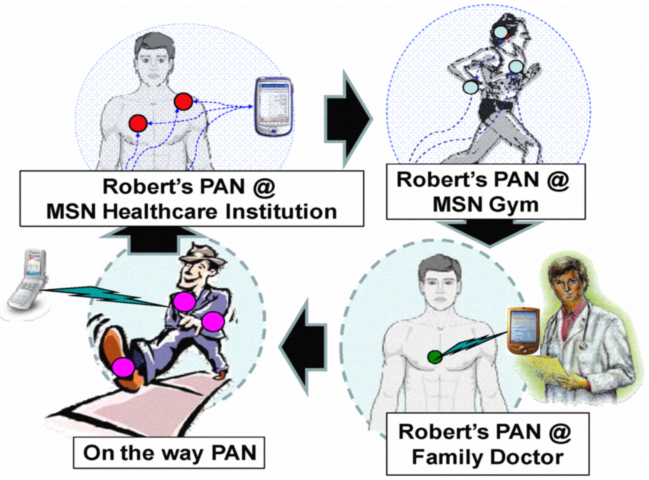

Fig. 1. Application Scenario of pervasive $PANs$ and $MSNs$: The health state of a user, Robert, is monitored in a multitude of medical sensor networks managed by a surgery, a healthcare institution, or a gym. Robert moves between those $MSNs$, and different wireless sensors such as ECG can be used in each MSN to form Robert's PAN and monitor his health state 24/7. Robert's identity should be linked to his health data independently of his location, time or medical equipment, while ensuring the privacy and security of his health data when different MSNs and back-end services interact with each other. Here, secure interaction should guarantee that medical data measured in different environments is securely transferred without endangering Robert's privacy. This work describes our security framework and discusses the elements that enable efficient security in this context.

Manuscript received on June 9th, 2009.

O. Garcia-Morchon (oscar.garcia@philips.com) and T. Falck (thomas.falck@philips.com) are with Distributed Sensor Systems at Philips Research Europe, the Netherlands.

T. Heer (tobias.heer@rwth-aachen.de) and K. Wehrle (Klaus.wehrle@rwth-aachen.de) are with Distributed Systems at RWTH Aachen University, Germany.

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2009.6962
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2009.6962

complementary security layers addressing the management of *MSN*s, *PANs*, and overall secure interoperation by means of a back-end security layer.

The security framework focuses on mechanisms for the distribution and establishment of secret keys that allow bootstrapping secure links, access control to the sensed information, and privacy-aware management of the medical data and user's identities. We combine centralized and distributed security solutions in order to provide an adequate balance between performance and security requirements. Each layer provides specific security algorithms as well as the physical elements and technologies needed for our framework to fulfill the specific operational requirements and ensure for seamless interaction between layers.

The *MSN security layer* allows each healthcare organization, e.g. a hospital, to manage the security in its *MSN* security domain. It allows any pair of devices or users in the same *MSN* to bootstrap a secure communication link and identify each other. For this layer, we focus on lightweight and distributed cryptographic methods based on polynomials for key establishment, identification, and information verification. These mechanisms are (i) lightweight to fulfill the delay requirements and save the scarce node resources, and (ii) distributed to fit the medical workflow in *MSNs*: medical staff can communicate with any *PAN* they encounter in a direct way, although both *PANs* and clinicians are continuously moving.

The *PAN security layer* allows a user to manage the security in her own patient area network and ensures the secure disclosure of her measured medical data when interacting with *MSNs* (e.g., clinicians in an *MSN*) and back-end services. The security management of this layer is centralized and it relies on a trusted device linked to and controlled by the patient, the *PAN* security manager (*PSM*), that allows transforming a *PAN* into a security domain where *WMSs* can securely join and leave at any time according to access control methods running on the *PAN*. The reason for this is that the *WMSs* forming a *PAN* belong to the *MSN* security domain, but the measured medical data belongs to the user. The application of a tamper resistant healthcare card [8], which forms a part of a user's *PSM*, simplifies the *PAN* management and ensures the *PAN* interoperability across the whole system of *MSNs*. The *PAN* layer further incorporates lightweight security mechanisms and protocols to configure a *PAN* when a user joins an *MSN*, enable distributed access control to the *PAN* and the sensed electronic health information, and identify a *PAN* in a privacy-aware way by means of pseudonyms.

The *back-end security layer* relies on public-key cryptography and ensures the secure interaction of users' *PANs* moving between *MSNs* controlled by different healthcare organizations. We assume a simplified centralized model for this layer based on public-key infrastructure and a single certification authority managing the healthcare system. Thus, *MSNs* and *PANs* just have to enroll at the certification authority to become part of the healthcare system owning some secrets such as a pair of public/private keys or a unique *PAN* identifier.

This overall arrangement aims at ensuring the easy, autonomous, and transparent management of the whole system in professional environments where users without technical background must be able to intuitively handle the (security) appliances given to them. We move all the set up procedures for *PAN* security to the moment when a user joins an *MSN*. The low resource requirements of the symmetric-cryptographic primitives [7] used during normal system operation guarantee the transparent but secure system operation without disturbing the medical workflow. The use of body-coupled communication at the *PAN* layer makes handling with a *PAN* extremely intuitive [4], as sensors only need to be attached to the patient's body and the *PSM* automatically and securely configures them as members of the *PAN* security domain.

III. Conclusions

Medical sensor networks allows for pervasive health monitoring. Security and privacy are key requirements for the successful deployment of those systems in which the sensed medical data must be protected all the way from the sensors to back-end systems. This paper provides a comprehensive view on our efficient and practicable security framework, including security algorithms, technologies, and procedures. Our solution provides an adequate balance between security and performance matching the expected system workflow. Thus, we allow for the feasible and secure deployment of the envisioned pervasive healthcare systems.

References

[1] U. Varshney, "Pervasive Healthcare" Computer, vol. 36, no. 12, pp. 138-140, Dec., 2003.

[2] The US Congress, Health Insurance Portability and Accountability Act. Washington D.C., 1996. (online available at http://www.hhs.gov/ocr/hipaa/).

[3] The European Parliament and the Council of the European Union, Directive 95/46/EC (online available at http://www.cdt.org/privacy/eudirective/EU_Directive_.html)

[4] T. Falck, H. Baldus, J. Espina, and K. Klabunde, "Plug'n Play Simplicity for Wireless Medical Body Sensors," in proc. of Pervasive Health Conference and Workshops, 2006 , vol., no., pp.1-5, 2006

[5] "Patient-centric: the 21st century prescription for healthcare" Healthcare and life science, July 2006.

[6] O. Garcia-Morchon, T. Falck, T. Heer, and K. Wehrle, "Security for Pervasive Medical Sensor Networks," in proc. of the Sixth Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (MobiQuitous 2009)

[7] O. Garcia-Morchon and H. Baldus, "Efficient and Distributed Security for Medical Sensor Networks," in proc. of ISSNIP 2008.

[8] Smart Card Alliance – White Paper, "HIPAA Compliance and Smart Cards: Solutions to Privacy and Security Requirements" September 2003 (www.smartcardalliance.org/pages/publications-hipaa-report)

[9] C. Cordeiro and M. Patel, "Body Area Network Stardardization: Present and Future Directions," in proc. Of 2nd International Conference on Body Area Networks (BodyNets 2007), June 2007.

Digital Object Identifier: 10.4108/ICST.MOBIQUITOUS2009.6962
http://dx.doi.org/10.4108/ICST.MOBIQUITOUS2009.6962