Threat Assessment of Wireless Patient Monitoring Systems

Wolfgang Leister, Habtamu Abie,
Arne-Kristian Groven, Truls Fretland
Norsk Regnesentral
Oslo, Norway
{wolfgang.leister, habtamu.abie,
arne-kristian.groven, truls.fretland}@nr.no

Ilangko Balasingham
Interventional Center
Rikshospitalet University Hospital
Oslo, Norway
ilangkob@klinmed.uio.no

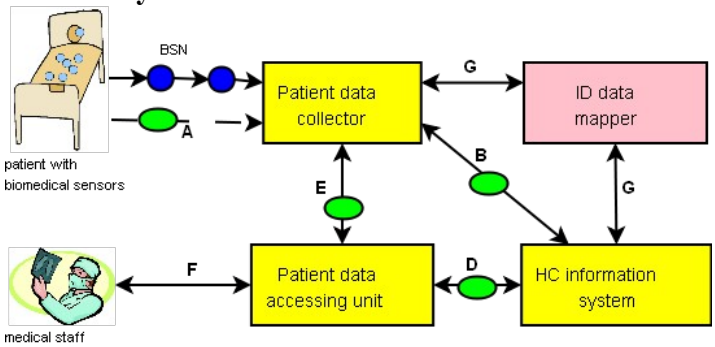
Introduction

Mobile patient monitoring systems may consist of wireless biomedical sensor networks, handheld devices, and database systems connected to the hospital information system. Such a monitoring system exhibit many advantages; however, there should be careful considerations on patient data security, patient privacy, and availability and reliability of the system. We identified threats for some selected parts of mobile patient monitoring systems based on a security architecture developed in previous projects.

The threat assessment is performed with regard to the security objectives confidentiality, privacy, integrity, availability, and non-repudiation. The underlying security architecture is based on a generic system model consisting of components and channels. This generic system model is adapted to scenarios using wireless communication based on public networks, short range networks, and wireless body area biomedical sensor networks.

We focused on the communication level, where wireless communication is based on broadcast principles, and hence cannot be trusted without extra technical measures. Threats on other levels include compromised or fake components, destroyed, malfunctioning, lost or stolen components, software errors, misuse of emergency access, denial-of-service attacks, compromised or fake communication infrastructure, and eavesdropping.

Generic System Model



Generic System Model with components (boxes) and channels (arrows). The green markers denote channels that must be protected.

The generic system model used for the threat assessment is shown in the above sketch. It consists of biomedical sensors, the patient data collector, the healthcare information system, and patient data accessing units used by healthcare personnel. The channels in between these components must be protected by technical and administrative security measures. In many cases information can be broadcast on a wired or wireless medium.

The generic system model is applicable to most of the patient monitoring systems. Using the generic model for a specific case study we identify the channels that need additional protection. The channels include data transmission using wireless short range communication (e.g., biomedical sensor networks, wireless replacement for cables) or long range wireless systems provided by other parties (e.g., GPRS, UMTS).

Special attention must be given to the channel between the biomedical sensors and the patient data collector, which is denoted as the biomedical sensor network. Since wireless communication is preferred in order to reduce the use of cables, this channel could be subject to different threats.

For the components of the generic system model the threats and associated factors identified include (1) compromised or fake components, (2) destroyed, malfunctioning, lost, or stolen component, (3) software errors, (4) misuse of emergency access, and (5) denial of service attacks. For the channels threats and associated factors include: (6) compromised or fake components of the communication infrastructure, (7) unstable communication infrastructure, and (8) eavesdropping of communication. These threats and vulnerabilities identified may lead to the unwanted consequences that information or equipment might be unavailable, incorrect information is received (medical data, patient identity, sensor type, etc.), sensitive information is leaked, or damage to the patient, operators or equipment.

Threat Identification for Biomedical Sensor Networks

A biomedical sensor network consists of several sensor nodes. The sensor nodes measure biomedical signals, process them and transmit the results to a sink node, which is connected to the hospital infrastructure. Typical biomedical data measured by biomedical sensors can be electrocardiogram (ECG), electroencephalography (EEG), blood oxygen saturation, blood pressure, and temperature. Biomedical sensor nodes work autonomously and have limited processing and transmission capabilities due to limited size, cost, memory, and battery. Therefore resource-intensive algorithms cannot be used, which implies that security capabilities can be limited and communication patterns can be restricted. This means that public key encryption schemes may become too expensive in terms of required resources such that alternative protection techniques may be considered. The wireless aspect of sensor network may become easy to eavesdrop on traffic, inject new messages, replay, or change previous messages. Threats have been categorized into the sensor node level, the routing level, and the forwarding level. A variety of attacks mentioned in the literature are also applicable. Some of the threats at the sensor node level could potentially lead to harm patients due to overheating in sensor nodes.

Threat Assessment in the Deployment of Biomedical Sensor Networks

Identification of threats leads to the definition of security requirements for the deployment of patient monitoring systems using biomedical sensor networks. These requirements will address infrastructural, administrative, and technical measures. Especially, identities, authentication, roles, and assets are important. Technical and infrastructural measures will be applied to the different medical scenarios so that wireless monitoring systems can be securely used for instance in hospitals, at accident sites, and home-care monitoring situations.

Threats at different levels have been scrutinized for mobile patient monitoring systems using long range wireless communication using third-party providers (e.g., GPRS) and short range wireless sensor networks. Based on threat assessments a set of security requirements has been identified, and recommendations have been suggested for the overall patient monitoring system.

The medical data can be considered as multimedia data, where the data are aggregated over a period of time and bundled with patient identity and communication system configuration information. This means that multimedia standards such as the MPEG-21 multimedia framework (ISO/IEC 21000) could be used for data security. Due to resource constraint in sensor networks, the usability and adaptability of MPEG-21 in sensor networks remains to be seen.