SAMPOS (Strategies for Seamless Deployment of Mobile Patient Monitoring Systems)
Project number 176875

Threat Assessment of Wireless Patient Monitoring Systems

Wolfgang Leister, *Chief Research Scientist, Norsk Regnesentral (NR), wolfgang.leister@nr.no*

Co-authors: Habtamu Abie (Senior Research Scientist, NR), Arne-Kristian Groven (Senior Research Scientist, NR), and Ilangko Balasingham (Professor, Interventional Centre, Rikshospitalet).

Mobile patient monitoring systems use biomedical sensor networks, and communication to hand-held devices which communicate over wireless channels with the databases at hospitals. Despite many advantages, their use could compromise patient safety, patient privacy, and availability of health care systems. We identified threats for 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 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.

Threat Identification for Biomedical Sensor Networks

A biomedical sensor network consists of several sensor nodes. These measure biomedical signals, process them and transmit the results to a sink node, which is connected to the hospital infrastructure. Biomedical sensor nodes work autonomously, and have limited capabilities due to size, cost, memory, and battery lifetime constraints. Therefore resource-intensive algorithms cannot be used, security capabilities might be limited, and communication patterns might be restricted.

Since biomedical sensor networks use wireless communication, an adversary can, without additional measures being in place, eavesdrop on traffic, inject new messages, replay or change previous messages. Threats are categorized into the sensor node level, the routing level, and the forwarding level. A variety of attacks mentioned in the literature can apply. Note that threats at the sensor node level could potentially harm patients (e.g., overheating of a sensor node).

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, and specifically to biomedical sensor networks. These requirements 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 in, e.g., hospitals, at accident sites, and home care monitoring situations. Currently, we are investigating whether the use of the MPEG-21 multimedia framework standard would be suitable as such a technical measure.

Project web page: http://www.iet.ntnu.no/projects/sampos/