Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Wireless Health and Care

Security architecture

The Wireless instrumentation demonstrator - WiSMoS

Note

Note no	DART/07/05
Authors	Per Røe, Jon Ølnes, André Larsen, Ilangko Balasingham, Karl Øyri
Date	September 2005

Norsk Regnesentral

Norsk Regnesentral (Norwegian Computing Center, NR) is a private, independent, non-profit foundation established in 1952. NR carries out contract research and development projects in the areas of information and communication technology and applied statistical modeling. The clients are a broad range of industrial, commercial and public service organizations in the national as well as the international market. Our scientific and technical capabilities are further developed in co-operation with The Research Council of Norway and key customers. The results of our projects may take the form of reports, software, prototypes, and short courses. A proof of the confidence and appreciation our clients have for us is given by the fact that most of our new contracts are signed with previous customers.

Memscap

Memscap as was established in February 2002, after the MEMSCAP SA acquisition of the Norwegian company Capto AS from the Norwegian MEMS Company SensoNor ASA.

The history of Memscap goes back to the early sixties when the basic silicon technology platform was developed at the Norwegian Research Laboratory SINTEF. This technology platform was also the main reason for the foundation of SensoNor ASA back in 1985.

Today's main focus areas in Memscap are divided between the (Bio-) Medical and Aerospace segments (flow and pressure measurements), where the goal is to obtain growth through the company's strong application knowledge after years of experience in these market areas.

The Memscap 844 blood pressure transducer has been in the market since 1972 and was the first blood pressure transducer with a disposable dome. Today, the 844 transducer is the only one real reusable transducer on the market with the very best performance. Memscap supply the 844 transducer to the global market through partners like Philips Medical, Siemens / Dräger, GE-Medical etc. where it is promoted as the preferred blood pressure transducer.

The Interventional Centre, Rikshospitalet

The Interventional Centre (IVC) is a Research and Development (R&D) Centre at Rikshospitalet University Hospital. IVS was established in 1996 to conduct research and development on minimally invasive and image guided therapy. IVC conducts basic and applied research on technology, anesthesiology, radiology and clinical procedures. In 2004, 650 humane procedures and 70 animal procedures were performed at the centre. IVC is funded by the Rikshospitalet University Hospital. In addition some of the research activities have external funding from the Research Council of Norway, European Union and various organizations and industrial partners. The outcomes of IVS's research activities are PhD's, peer reviewed papers published in international journals, industrialization of commercial ideas and patents. So far two spinoffs have been created.

Title	**Wireless Health and Care - Security architecture** **The Wireless instrumentation demonstrator – WiSMoS**
Authors	**Per Røe, Jon Ølnes, André Larsen, Ilangko Balasingham, Karl Øyri,**
Date	September
Year	2005

Abstract

This document describes given an analysis of the computer security aspects of the demonstrator developed in work package 12 of the Wireless Health and Care (WsHC) project. A risk analysis is performed and requirements for the system are established. The implementation of security measurements implemented in the demonstrator is discussed. Finally the risk analysis is revised according to the proposed security enhancements.

Keywords	Security architecture, wireless sensors, Bluetooth.
Target group	Participants in the WsHC project.
Availability	Public
Project number	320302
Research field	Computer security
Number of pages	20
© Copyright	Norsk Regnesentral

Contents

List of figures

1 Introduction

This document discusses the security in the demonstrator of work package 12 (WP12) of the Wireless Health and Care (WsHC) project. The document is built upon the general security requirement [2] and security architecture [1] documents for the project. WP12 studies use of wireless communication for sensors in a hospital environment.

This document focuses on the security aspects of the demonstrator. While availability is an important security property, safety aspects like battery lifetime, hardware reliability, etc. are not discussed. Also, general PC security is out of the scope. The PC used is assumed to be "secure" according to the policy applied by the hospital in question.

2 Description of the demonstrator

Today, a patient (e.g., before, during and after surgery) is usually monitored by a set of sensors, each with separate, wired communication towards the equipment (e.g., a PC or a monitor) receiving the sensor signals. Establishment and maintenance of the cabling is time-consuming, and moving the patient is rather cumbersome.

Memscap AS develops equipment that can collect signals from several sensors in one box close to the patient (e.g. attached to the bed), with wireless communication from the box to a PC with monitor. The box, WiSMoS (Wireless Sensor Monitoring System), is battery powered and highly modular. Individual modules interface various sensors, essentially digitalizing the sensor signals. Additionally, WiSMoS needs a communication module, which today is preferably Bluetooth wireless, alternatively RS232 wired. Modules can be plugged, unplugged and exchanged freely, according to the requirements for the patient in question.

WiSMoS communicates with a PC with Memscap's software, hereafter called MC-software, for receiving and processing of digitalized sensor data. The communication channel (even for Bluetooth) is always point-to-point between a WiSMoS and one PC. However, it is easy to change from one PC to another, e.g. when the patient is moved after surgery.

When the connection between the PC and the WiSMoS is set up, a registration form is filled out specifying the identity of the patient, operators, location, etc. At present the identity of the patient is inputted manually but in future versions the identity should be retrieved from a central patient database to ensure that the patient is identified correctly.

The function of the MC-software is to display the sensor data on a bedside monitor. Alarms are displayed on the same monitor, according to threshold values set by default for the sensor in question, or specified on the PC by medical personnel. The MC-software may perform logging of sensor data but this functionality is usually turned off (considered not needed since the monitor is usually under continuous observation by medical personnel).

The data that is retrieved from the sensors can be stored on a central database server. These data can then later be retrieved through a Reader Server, and then be viewed on other PC's running the MC-software, or on PDAs that are running a portable version of the same software.

2.1 Security in the present WiSMoS setup

Each WiSMoS has a unique serial number (resembles a MAC address) embedded in the software in the WiSMoS. In the data sent from the WiSMoS to the PC the patient is only indirectly identified through the serial number. The ID of the patient is stored together with the data on the PC, before the data is stored in the central database, or showed on another device.

Each WiSMos has an individual, alphanumeric, four-character password hard-coded in the Bluetooth software. The password must be input to the MC-software in order to establish the Bluetooth channel. The password is shown together with the serial number on a sticker placed on the WiSMoS. The idea is that all personnel present will anyway be authorized to set up the channel, and a displayed password will make the process a bit easier.

Once a Bluetooth channel is established, the WiSMoS will refuse further connection attempts. If one needs to switch to another PC (e.g. moving the patient), the original PC must terminate the Bluetooth channel before the new PC can connect. Similarly, the MC-software ensures that a PC can connect to only one WiSMoS at a time.

A WiSMoS is a “visible” Bluetooth device. It is automatically detected by PCs and other equipment within reach. It is possible to configure a Bluetooth device as “invisible” except for specified equipment (in this case a PC). However, this is not desirable as it would imply that the WiSMoS would depend on one particular PC to be present, and moving the responsibility for communicating with the WiSMoS from one PC to another would imply a more complex configuration procedure. While turning on “invisibility” in itself may add to security, it actually entails a higher risk due to the high probability of (manual) failure in the resulting configuration routines. It should also be noted that even an “invisible” Bluetooth device could be detected by advanced cracking tools [3], [4].

A “status button” (radio button on PC screen) is implemented. When this button is clicked, LEDs on the connected WiSMoS will flash.

Bluetooth encryption (link level) is always on for the channel between the WiSMoS and the PC. This encryption scheme has some theoretical weaknesses, but none that were deemed exploitable [4]. The pin-code is however the initial shared secret, and if the attacker is able to guess this code, the attacker can decipher the whole communication.

It should be noted that it is not possible to program or configure a WiSMoS over a Bluetooth channel. Such functionality is only present when a serial link is used.

2.2 Possible extensions for the demonstrator

Extended alarm functionality is a desired extension. For example, medical personnel may be alerted when an alarm goes off. The functionality may be implemented directly in the MC-software; however, interfacing to the Central System and taking advantage of the already existing alarm functionality in the Central System seems more appropriate. Note that that in many cases “false alarms” are common, e.g., during a surgery there is often a need to move sensors on the patient, resulting in a temporal loss of measurements and hence alarms. In the MC-software, the alarm functionality may be implemented as a “generic” alarm function, which can be configured to use one or more of the alarm channels available (display on monitor, send message to Central System, or even send a message directly from MC-software to intended receiver of the alarm).

3 System model

The general system model for WsHC is shown in Figure 1.

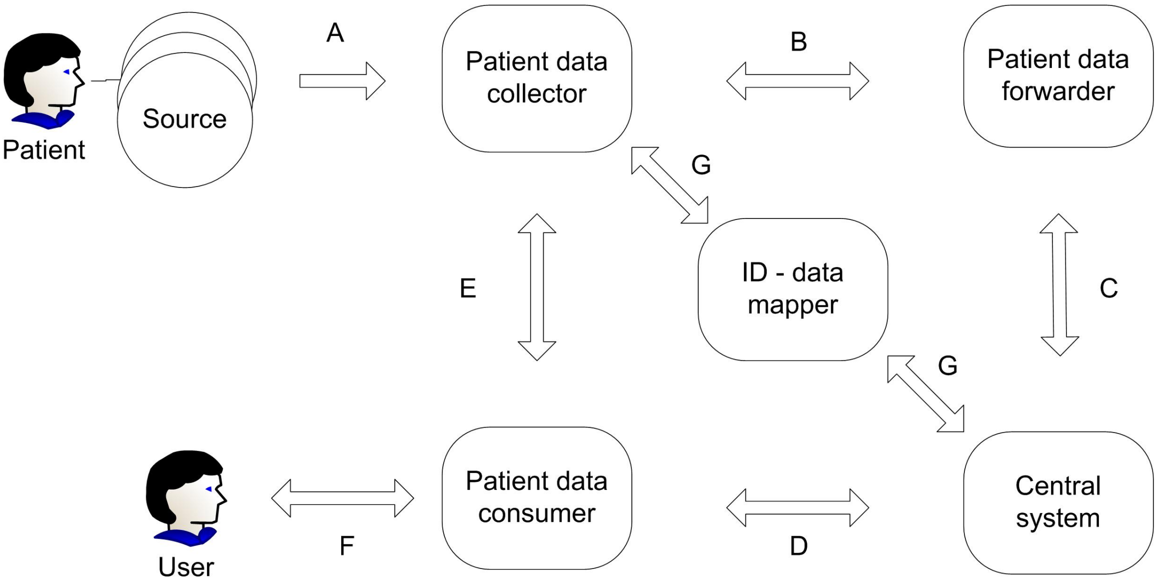

Figure 1: System model for WsHC

The wireless instrumentation demonstrator consists of the following actors:

- Sensors (at present invasive blood pressure and ECG electrodes)
- A WiSMoS with modules for digitalizing data from the sensors, and with Bluetooth connector. In our model WiSMoS functions as a source.
- PC, acting as Patient data collector.
- Monitors (visual display of results) connected to the PC, acting as Patient data consumers.
- Central system for aggregation and storage of data, alarm triggering, etc.

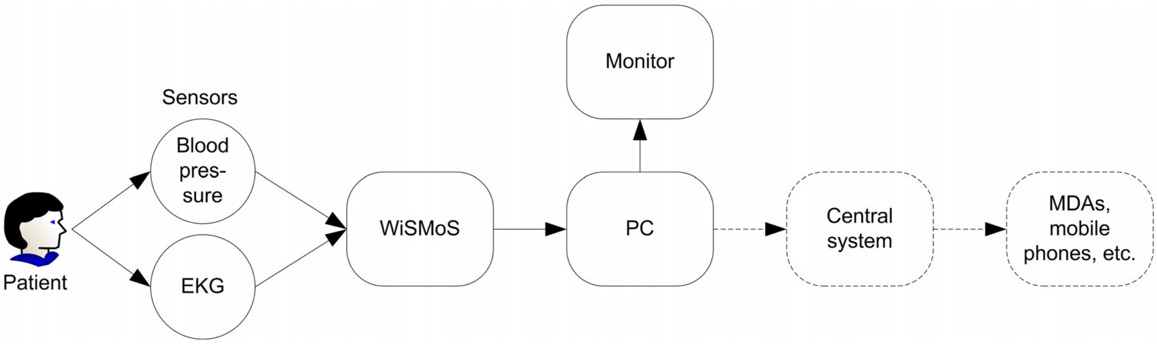

Figure 2: Physical architecture of the demonstrator

Use case:

1. The sensors are attached to a patient in the emergency room.
2. The sensors are connected with a cable to the WiSMoS.

3. The WiSMoS sends data to a PC. In the current version Bluetooth or serial cable is used, but other wireless technologies may be used in the future. Medical personnel can see the data on bedside monitors connected to this PC.
4. Samples of the data can be sent to the central system, where it can be retrieved by remote medical personnel.
5. The PC can monitor the signals, and send alarms if some predefined criteria are met.
6. Patient data may be entered on the PC by medical personnel, and sent to the central system.
7. Patient is moved to other locations (operation room, post-op) with sensors on.
8. A new connection is set up between another PC and the WiSMoS.
9. Patient data is sent to new bedside monitors at the new location (and continue to be sent to the central system and possibly remote medical personnel).

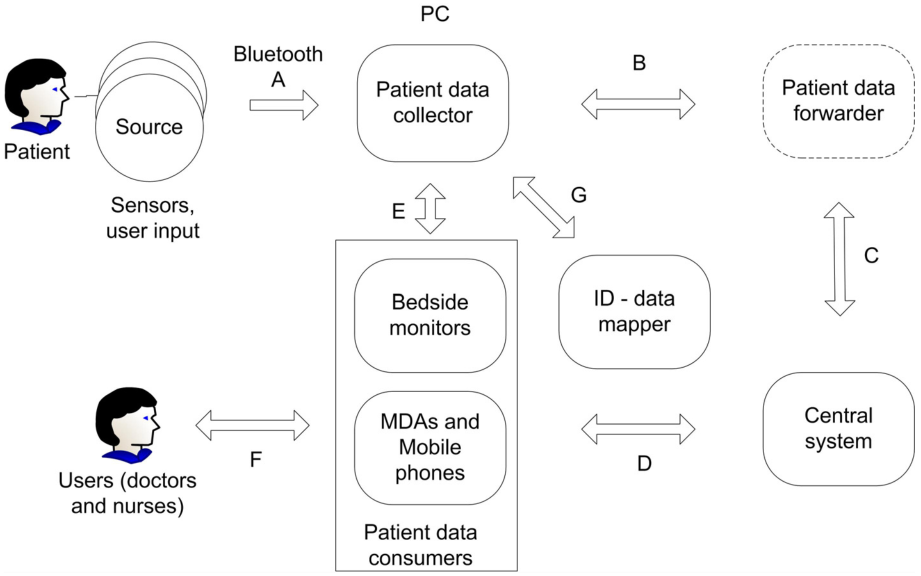

Figure 3: Architecture of the demonstrator mapped to the logical security architecture

In this document we are mainly interested in the subsystem consisting of the sensors, the WiSMoS and the PC, with the MC-software installed. We assume that channel C goes over standard hospital infrastructure, either a LAN with restricted access, or through a secure WLAN. The PC and the Central system should authenticate each other, and the data must be mapped to a patient before they are sent to the central system. The communication with the MDAs and mobile phones is covered by a separate work package in the WsHC project, and the security for this channel will not be discussed in this document.

4 Risk analysis

In the following section we analyze the risk in the system where the security measures listed in section 2.1 are implemented.

The data system that is treated in this document handles measurements from a range of sensors, mainly various forms of blood pressure and ECG. The data sent over the

Bluetooth link only contains the measurements and they are not directly linked to the patient. The data can however be linked indirectly to the patient through location and WiSMoS serial number. When the data is stored in the central database and viewed later the patient identification is stored together with the data.

Since the data can be used to show whether the patient is alive or dead and also can be used to diagnose some diseases the collected data are deemed to be highly sensitive. It is also important that the collected data are correct and that the data stream is not interrupted, since the data are important for monitoring and treating the patient.

In the following some risks are listed, and for each risk a probability level and a consequence level is given.

The consequence levels are defined as following:

Consequence level	**Description**
Catastrophic	Loss of lives.
Large	Danger for patients' life and health. Privacy breach for a large number of patients. Serious economic losses. Serious loss of reputation.
Moderate	No danger for patients' health. Privacy breach for a small number of patients. Moderate economic losses. Moderate loss of reputation.
Small	No danger for patients' health. No privacy breach. Inconsequential economic losses. No loss of reputation.

Table 1: Consequence levels

We use the following probability levels:

Probability level	**Description**
High	The event must be expected to occur several times per year. No security measures or security measures that can be accidentally breached, both by internal personnel and outsiders.
Medium	The event must be expected to occur at least once per year. Security measures can be easily breached by internal personnel, both accidentally or on purpose. Outsiders can't breach the security measures accidentally, and need some knowledge about the system and implemented security measures to attack the system on purpose.
Low	The event must be expected to occur once every 2-3 years. Security can be breached by internals on purpose and with knowledge of the system. Outsiders need detailed knowledge about the system and routines and special equipment to be able to attack the system.

Very low	There is a slight possibility for the event but it is not expected to occur. Security can only be breached by internal personnel with special competence. Outsiders can normally not attack the system.

Table 2: Probability levels

4.1 Unauthorized personnel gaining access to the data for one patient

An attacker can gain access to patient data using different kinds of attacks:

- Eavesdropping on the communication between the WiSMoS and the PC.
- Someone is able to set up a communication channel with either the WiSMoS or the receiving PC and gain access to patient information from there.
- Eavesdropping on the communication between the PC and the central database.
- An attacker gaining physical access to the PC or the WiSMoS.

The consequence of such an attack is considered to be moderate since it is a privacy breach for one patient.

The probability of eavesdropping on the communication between the WiSMoS and the PC is considered to be medium, since the confidentiality and authentication on this channel is protected using weak encryption, which is easy to break.

The probability of eavesdropping on the communication between the PC and the central database is considered to be low, since an attacker would have to have access to the hospital network to perform such an attack.

The probability of an attacker gaining physical access to the PC or is considered to be low, since the sensors in question are used in a controlled environment, i.e., the hospital and especially in the operation theatres.

4.2 Unauthorized personnel gaining access to the data for a large number of patients

An attacker can gain access to the patient data for a large number of patients by gaining access to the central database, either physically or by being able to download data.

The consequences of such an attack would be large, since it would entail a privacy breach for a large number of patients.

The probability of an attacker gaining physical access to central database is considered to be very low, provided that a sufficient level of access control, both physically and through user authentication, is implemented on the server.

4.3 Incorrect data stored or viewed for an patient

Incorrect data can be stored for a patient in the following cases:

- An attacker that manages to set up a communication channel with either the WiSMoS or the receiving PC, and injects false/harmful data that way.
- Software and hardware errors.

We deem the consequences of such an incident to be large since incorrect data or data that is mapped to the wrong patient can lead to mistreatment or delayed reaction to a serious situation.

The probability of software errors and hardware errors should be very low, provided that the system is sufficiently tested. The probability of injection of false data by hijacking the communication channel between the WiSMoS and the PC is set to low since the channel is protected by encryption using a small key, but special equipment and determination is still needed to perform such an attack.

4.4 Data mapped to the wrong patient

The following scenarios can lead to data mapped to the wrong patient:

- Error when inputting patient data.
- PC receiving data from wrong WiSMoS.

The consequences of data mapped to the wrong patient are deemed to be large, since this could lead to mistreatment or delayed reaction to a serious situation.

The probability of inputting wrong patient data is deemed to be medium, since this at present is done manually and without any check against central registers. The probability of receiving data from the wrong WiSMoS is deemed to be very low, given all the security measures that are implemented to prevent this.

4.5 Jamming of the Bluetooth channel

A denial of service attack can be performed against the equipment, either by jamming of the Bluetooth frequency specter, or by a denial of service attack aimed at the Bluetooth protocol. This can both be result of an attack or by accident if there are too many Bluetooth devices in the same area.

The consequences of such an incident are deemed to be small, since if the Bluetooth channel is jammed no data, or very little data comes through to the PC, and because of this, such an incident should be easy to spot, and measures, for example changing to another sensor, could easily be implemented.

The probability of an attacker jamming the Bluetooth channel on purpose is deemed to be low, since this would require sophisticated equipment, and since an attacker would not gain much from performing such an attack. The probability of accidental jamming is deemed to be low, since this would require a rather large number of Bluetooth devices, each transmitting large amounts of data.

4.6 Reprogramming of the WiSMoS

It is possible to reprogram the WiSMoS through the serial interface. To be able to do this the attacker needs to know the communication protocol and memory layout of the WiSMoS. The attacker also needs to be able to set up a serial connection with the WiSMoS since it is not possible to reprogram the WiSMoS using a wireless connection.

The consequences of such an attack are deemed to be large, since this could lead to malfunction of the WiSMoS, and thereby give wrong data.

The probability of such an attack is deemed to be very low, since physical contact with the WiSMoS is needed, and we assume that the WiSMoS is kept in a protected area. The attacker also needs detailed knowledge about the WiSMoS, the memory layout of the WiSMoS and the communication protocol.

4.7 Loss of data

Data can be lost in the following cases:

- Software, hardware or configuration failure or errors.

The consequences of such an incident are deemed to be small, since such an incident would be easy to spot, and measures, for example changing to another sensor, could easily be implemented. Procedures for handling failures and configuration errors should be implemented.

The probability of loss of data is deemed to be medium, since configuration errors and hardware failures often can happen in normal use.

4.8 Summary

Risk ID	Description	Probability	Consequence
R1	Unauthorized personnel gaining access to the data for one patient.	Medium	Moderate
R2	Unauthorized personnel gaining access to the data for a large number of patients.	Very low	Large
R3	Incorrect data stored or viewed for a patient.	Low	Large
R4	Data mapped to the wrong patient.	Medium	Large
R5	Jamming of the Bluetooth channel.	Low	Small
R6	Reprogramming of the WiSMoS.	Very low	Large
R7	Loss of data.	Medium	Small

Table 3: Summary of risks

In the risk matrix we have the following risk levels:

Low risk	Medium risk	High risk

Low risk – Acceptable risk level, however risk reducing measures that are easy to implement should be considered.

Medium risk – Risk reducing measures should be considered from a cost/benefit point of view.

High risk – Not acceptable risk level. Risk reducing measure **must** be implemented.

Consequence: **Probability:**	**Small**	**Moderate**	**Large**	**Catastrophic**
Very low			R2, R6	
Low	R5		R3	
Medium	R7	R1	R4	
High				

Table 4: Risk matrix

5 Requirements

5.1 Security requirements

The requirement numbers correspond to those of the logical system model given in the general requirements document [2]. Requirements that are not applicable for the demonstrator are left blank.

The requirement fulfillment column gives a short explanation of how this requirement is met in the demonstrator.

No.	Actor(s)	Requirement	Requirement fulfillment
S1	Source	**Limited storage**. Source shall not store sent data longer than necessary (confidentiality)	Neither the sensors nor the WiSMoS stores any data.
S2	Channel A	**Short-range communication.** Source and Patient data collector shall only communicate with each other short range (confidentiality and integrity)	The Bluetooth chip is a class II chip and is able to communicate up to 10 meters. (Note however that it is possible to eavesdrop on the communication from longer distances using special equipment [4].)
S3	Channel A	**Confidentiality protection.** Patient data should be protected from eavesdropping when transmitted to PC. (Note: communication is short range, which reduces the need for strong communication encryption)	The communication is encrypted using standard Bluetooth encryption, however a short key length is used, and it may therefore be possible to break the encryption (See 6.1
S4	Channel A	**Integrity protection**. Patient data should be integrity protected when transmitted to PC. (Note: this includes protection from interference)	The integrity is secured by using a reliable protocol, and by calculating CRC checksums.
S5	Channel A	**No automatic roaming**. The connection between Source and PC shall be manually initiated, i.e. a human actor determines (at some point in time and through a defined procedure) which Sources and PCs that shall talk to each other (integrity)	When the WiSMoS is connected to a new PC the connection process has to be done manually.

No.	Actor(s)	Requirement	Requirement fulfillment
S6	Patient data collector	**Verify Source identity**. PC shall verify correct identity of the Source (integrity and accountability)	The identity of the source is ensured by requiring that the operator inputs the serial number and password for the WiSMoS on the PC.
S7	Patient data collector	**Data integrity verification**. PC shall verify the integrity[1] of patient data (integrity)	The integrity is verified using the CRC checksums.
S8	Patient data collector	**No data modification.** PC shall not modify patient data, except possibly for aggregation or other defined transformations (integrity)	The data are not modified on the PC, but derived values are computed, and the PC can transform the data.
S9	Patient data collector	**No unauthorised data access.** PC shall not give unauthorised actors access to patient data (confidentiality and integrity)	This is done by password-protection and use of keyboard locks.
S10	Patient data collector	**Limited storage.** PC shall not store data longer than necessary to ensure successful transmission of patient data (confidentiality)	The system should not be used in such a way that data is stored locally on the PC. All data should be stored in the central system.
S11	Channels B, C, D and E	**Confidentiality protection.** Personally identifiable patient data shall be protected from eavesdropping when transmitted across open networks.	Handled by standard hospital IT infrastructure.
S12	Channels B, C, D and E	**Integrity protection.** Patient data shall be integrity protected when transmitted across open networks.	Handled by standard hospital IT infrastructure.
S13	Central system	**Data integrity verification.** Central system shall verify the integrity of patient data.	Handled by standard hospital IT infrastructure.

[1] "Integrity verification" refers to the verification that data has not been altered during transmission from the Source; it does not imply a "sanity check" on the data. Such a sanity check should be implemented somewhere in the system; at least in the Central system before storage of the data.

No.	Actor(s)	Requirement	Requirement fulfillment
S14	Central system	**Data origin authentication.** Central system shall authenticate the PC (integrity and accountability)	Handled by standard hospital IT infrastructure.
S15	Central system		
S16	Central system	**Patient identity.** Central system shall know the identity of the patient to whom the patient data pertains (integrity)	The data is linked to the patient in the MC-software at the PC, and the patient identity is sent together with the data to the central system.
S17	Central system	**Source type.** Central system shall know the type of Source used to produce the patient data (integrity)	The sensor type is stored together with the data.
S18	Channel D		
S19	Channel D		
S20	Channel E	**Authenticate User.** PC shall authenticate the User (confidentiality and accountability)	Handled by other work package
S21	Channel E		
S22	Patient data consumer	**Data integrity verification.** Monitor should (if possible) verify the integrity of patient data	Handled by other work package.
S23	Patient data consumer		
S24	All components	**Emergency access.** Where emergency access functionality is available, invocation of emergency access shall override any restriction on read access (availability)	No emergency access implemented. Personnel will always be able to watch the monitor.
S25	All components except Source	**Emergency access monitoring**. Emergency access shall trigger extended monitoring of relevant events to enable detection of unnecessary access (confidentiality and accountability)	No emergency access implemented.

Table 5: Security requirements

6 Security recommendations

6.1 Communication between WiSMoS and the PC

The pin-codes used in the project have a length of 4 alphanumeric characters, which gives a total of around 2.5 million different keys. It is therefore easy to break the pin-code using a brute force attack. The pin-code is the initial shared secret that is used to initiate the encryption, which is used both for authentication and for confidentiality protection of the communication. Breaking the pin-code would allow both eavesdropping, hijacking of the communication channel, injection of false data and spoofing, i.e. that another device claims to be the WiSMoS.

The Norwegian Data Inspectorate recommends the use of 128 bits encryption for communication of sensitive information like health information, and the Bluetooth standard supports pin-codes of up to 128 bits length. An API that allows the use of a 128 bits buffer as a pin-code for Bluetooth communication exists, however this API is at present not supported by almost all of the producers of Bluetooth equipment. Instead the only way to input the pin-code is through a dialog, something that effectively reduces the key length, and makes it complicated to handle long pin-codes.

The short length of the used pin-code can also be exploited to circumvent the authentication, by an attacker trying to set up a connection to the WiSMoS trying all possible pin-codes. This attack is difficult to perform, since such an attack will take some time, and the WiSMoS only is vulnerable if it is not already connected to another PC. However, an attacker can first break the pin-code using brute force on communication information from an earlier session. Since the pin-code does not change, the attacker can then later use the pin-code to gain access to the WiSMoS.

6.2 Mapping of data to patient

At present mapping of data to patient is done by manually inputting the patient's name and ID. This is error-prone. Instead name and patient ID should be looked up in the central patient database connected to Folkeregisteret (National Registry Office).

6.3 Security for communication with central database

The communication with the central database should be protected. This can be done either by implementing encryption on the used communication protocol, or by using a virtual private network (VPN). Access control should also be implemented in the central database to prevent unauthorized access to the data and unauthorized modification and injection of data. The communication between the central database and terminals accessing the stored data should be protected in a similar fashion.

7 Revised risk analysis

The following section gives a risk analysis where in addition to the security measures mentioned in 2.1 the following security measures are implemented:

- Use of 128 bit key for communication between the WiSMoS and the PC.
- Encryption and access control for communication with the central database.
- Patient data is checked against the patient database.

7.1 Unauthorized personnel gaining access to the data for one patient

The probability of eavesdropping on the communication between the WiSMoS and the PC is revised to very low, since it will not be feasible to break the encryption, and the attacker hence would need access to the pin-code.

The probability of eavesdropping on the communication between the PC and the central database is considered to be very low, since an attacker would have to have access to the hospital network to perform such an attack, and since all the communication is encrypted.

The probability of an attacker gaining physical access to the PC or is considered to be low, since the sensors in question are used in a controlled environment, i.e., the hospital and especially in the operation theatres.

7.2 Unauthorized personnel gaining access to the data for a large number of patients

The probability of an attacker gaining physical access to central database or being able to eavesdrop on the communication with the central database is considered to be very low, provided that a sufficient level of access control, both physically and through user authentication, is implemented on the server.

7.3 Incorrect data stored or viewed for an patient

The probability of injection of false data by hijacking the communication channel between the WiSMoS and the PC is revised to very low since the channel is protected by encryption using strong encryption and a long key.

7.4 Data mapped to the wrong patient

The probability of inputting wrong patient data is revised to low provided that patient data is checked against central databases.

7.5 Jamming of the Bluetooth channel

The probability for this incident is unchanged.

7.6 Reprogramming of the WiSMoS

The probability for this incident is unchanged.

7.7 Loss of data

The probability for this incident is unchanged.

7.8 Summary

Risk ID	Description	Probability	Consequence
R1	Unauthorized personnel gaining access to the data for one patient.	Very low	Moderate
R2	Unauthorized personnel gaining access to the data for a large number of patients.	Very low	Large
R3	Incorrect data stored or viewed for a patient.	Very low	Large
R4	Data mapped to the wrong patient.	Low	Large
R5	Jamming of the Bluetooth channel.	Low	Small

R6	Reprogramming of the WiSMoS.	Very low	Large
R7	Loss of data.	Medium	Small

Table 6: Revised summary of risks

Consequence: **Probability:**	**Small**	**Moderate**	**Large**	**Catastrophic**
Very low			R2, R3, R6	
Low	R5	R1	R4	
Medium	R7			
High				

Table 7: Revised risk matrix

8 References

[1] R. Arnesen, J. Danielsson, J. Ølnes and J. I. Vestgården. *WsHC Security Architecture*. NR Technical Report 1006, January 2005.

[2] R. Arnesen, J. Danielsson, J. Ølnes and J. I. Vestgården. *WsHC Security Requirements*. NR Technical Note DART/01/05, January 2005.

[3] O. Whitehouse. *War Nibbling: Bluetooth insecurity*. @-stake Research Report, October 2003.

[4] H. J. Rivertz, *Bluetooth Security*. NR Technical Note DART/05/05, March 2005.

[5] “The Norwegian Data Inspectorate”. http://www.datatilsynet.no/.