International Workshop on safety & security of (wireless) medical sensor networks

TU Delft - 21 January 2014

Summary report

Workshop Aims

The workshop aims were:

1. to explore safety and security threats of networked medical devices;
2. to assess the extent to which relevant standards are applicable and to identify the gaps that exist in the standards (e.g. 80001);
3. to identify gaps in the current research and to determine possible future research areas;
4. to foster collaboration and exchange of ideas through a community of practice beyond the workshop.

Participants

The workshop was attended by 26 people from 7 countries [Austria: 1, Switzerland: 1, Germany: 2, Denmark: 1, The Netherlands: 14, Norway: 3, United Kingdom: 4], see Annex B. Participants' domains were research (10), industry (6), Regulators/assessors (4), healthcare (3) and consultants (3).

Presentations

The presentations in the morning session paved the way for the discussions in the break-out sessions after lunch. In advance, the presenters had been asked to consider the questions, which would form the basis of the afternoon break-out sessions, in their presentations.

Overview of the presentations

1) Setting the Scene - EWICS Case Study: **Odd Nordland** [SINTEF, Norway]: "*A wireless medical sensor application and the problems it poses*".
   Odd presented a generic medical sensor network, addressed system error sources and scenarios, stated assurance requirements regarding suitability of use, safety and security, and identified problems to address.

2) **Oliver Christ** [PROSYSTEM AG, Germany]: "*Network Standard Session: Up-date on IEC 80001-1*".
   Oliver presented a comprehensive insight in the development of the IEC 80001 standard on application of risk management for IT-networks incorporating medical devices, its history, how it relates to other standards, an elaborated on the technical report series (80001-2-..) of which 80001-2-x (62A/915/NP) is close to the scope of the workshop.

3) Medical Sensor Developer Session: **Geoff Duke** [Johnson & Johnson, UK]: "*Wireless Connectivity of Medical Devices - Developer needs*".
   Geoff presented a kaleidoscopic overview of wireless networks, examples, issues of security from different perspectives, the relevance of the risk management rationale for different parties, and developer needs regarding risk management.

4) Network Security Session: **Karin Bernsmed** [SINTEF, Norway]: "*Security, privacy and accountability in cloud-based medical sensor networks*"
   Karin addressed the key issues in security of cloud-based medical networks from the perspective of the directive on protection of personal data (95/45/EC) and with focus on the roles and responsibilities of different actors.

5) Medical Network Vulnerability Session: **Reinout Hensbroek** [TNO, The Netherlands]: "*Vulnerability and patient safety (EMI: the single biggest obstacle ?)*"
   Reinout presented several practical issues of electromagnetic interference (EMI) on functioning of medical devices, field tests that reveal gaps in standards that have risk to patient safety consequences in health care practice.

6) Medical Profession Session: **Martin Janssen** [UMC St. Radboud, The Netherlands]: "*Medical IT - System Safety and Security in an OR: Safety First?*"
   Martin focussed on three cases of networked systems from a "safety first" in the operating room from a "safety first" perspective, concludes that security is often a safety issue, and also that balancing safety and security is a local prerogative.

The presentations can be found at http://www.ewics.org/docs/medical-sensor-networks-workshop

Some notes arising from the presentations:

- Patient with medical sensors should be considered in the same way as medical equipment (e.g. constraints in proximity to WiFi equipment).
  - Hospitals vs Patient wearing body sensors are different environments
- Need to consider effectiveness parameter in benefit analysis (e.g. beyond safety to treat whole population)
- Need to consider cloud storage in any case study
  - Control of cloud provider, who outsources services (Hospital data controller but cloud provider processes data)
  - Conflicts with Data Protection legislation
  - Who determines access control for different users of the system and information that can be accessed (e.g. patient location, personal)?
- Who manages the encryption over the network and when stored?
- Who is in overall charge of maintenance?

Break-out sessions

All participants including the speakers participated in the break-out sessions. The sessions were grouped in three rounds addressing eight questions in four sets of two questions. Thus, each pair of questions has been discussed at least twice by break-out groups. After the third round, the groups reported in plenary about issues discussed.

Q1a What are the conflicts between Safety and Security and how can they be resolved?
Q1b What are the Security Issues (e.g. privacy, legislation) and are these country dependent?

From the discussion, it is clear that security supports safety, and a security breach comes with safety problems. In health care organisations, there seems a conflict with privacy (e.g. access control of (electronic) patient files). Also, there is a difference between countries (e.g. UK people do bother less about privacy than German people). The responsibility for this should be on the heath care provider (e.g. the hospital). Patients must be empowered and be looked at as an individual in the societal system with the right to lie about his or her health condition.

Q2a How much reliance is placed on the patient (e.g. training, fault reporting)?
Q2b What are the issues of changing patient environment (e.g. home, hospital, trains, public areas)?

The discussion showed different perspectives. On the one hand, it was argued that there should be no reliance on the patient at all and, instead, that reliance effort should be on the system. On the other hand, it was advocated to put the patient in the centre of their own care, the patient being the only person who has a continuous awareness of their condition and data as they cross care boundaries. Reliable networks depend on criticality. This requires awareness about the devices by the doctor, a second opinion before decision making when impact on the patient might be high. Therefore, this is also a starting point for risk analysis leading to information for patients to decide whether the system will be "okay" for them, as well as information for doctors to decide whether the system will be "okay" for the patient. The notion of "intended use" should be accompanied by the notion of "intended patient".

Q3a What are the constraints on using of third party services (e.g. public wireless networks, roaming)?
Q3b How should responsibility and liability be distributed over the involved parties?

Regarding constraints on 3rd parties, the 'price' of a contract equates to willingness to pay money. Whoever takes the money, also takes the liability (i.e. should not hide behind the back of others). A health care provider needs waterproof service contracts, which will be the best guarantee. This requires thinking through scenarios, such as the doctor using a secure PC at work taking patient data home at an unsecure PC for the benefit of the patient.

Q4a What are the constraints on patient mobility (e.g. travelling abroad, using public transport, avoiding wireless dead zones in e.g. a cellar)?
Q4b What issues (e.g. ethical, technical, regulatory, country) need to be resolved in remote intervention through implanted sensors?

Consider the criticality levels in relation to the intended use of a medical device (network system). It is important that a doctor informs the patient about limitations of the system. Also, the patient needs an emergency protocol. A patient who accepts telemedicine should be informed and be knowledgeable about system limitations and emergency plans, and accept the related risks.

Issues to be resolved include clarity about "remote", as a doctor and patient are not in the same place and connections may involve different organisations. The system must be robust enough to increase trust. The different actors in the system include commercial systems outside health care that should assume liability for their services.

Panel session

Following the break-out sessions, the speakers from the morning session formed a panel and were invited to discuss the following questions:

1. What are the implications for clinical practice?
2. What are the implications for regulation/regulators?
3. What are the implications for research?

Each speaker gave his or her views, summarised below as notes.

- EU should coordinate the development of remote patient networks. In 20 years, technology has advanced much further than we can image. Research aspects are: better, smaller, more intelligent sensors, and new communication technologies.
- Framework for sensors can be used
- Health policies not coordinated
- Widespread use of sensors will reduce functionality of clinics
- Technology research in providing more sophisticated, reliable, smaller sensors.
- More security in networks

- Regulators need to look across industry into what is being done (e.g. ITU, workshops and seminars)
- Sensors need development
- Clinical studies to improve user experience, simulations for patients
- Diabetes increasing but funding decreasing

- Medical devices & IT seen as IT projects but should be clinical projects. Must be multi-discipline.
- Medical devices connected to IT have safety issues. 80001 was a good step but now needs to be brought into practice.
- Boundaries between health IT en medical devices are almost non-existent, so look at the combination to make the safety case.
- Many issues about availability, privacy, etc. also relate to safety, but how & why needs clarification to health care practitioners
- User is part of system. Regulators should work together.
- Research into regulation of defining safety, inter-domains.

- The 80001 standard is bringing together medical devices and IT, but telecom also needs to be included (ETSI).
- Regulator: More cooperation between different groups including telecoms, standardisation (missing where standards are going), more cooperation and harmonisation.
- The numbering of standards, sometime same number as IEC and ISO, but still with different content, is Incomprehensible for hospital engineers: help is needed here
- Clinical: All medical devices will have chips and be networked, which will change clinical practice dramatically
- Everything that is not going wrong now, will go wrong sooner or later, so there is opportunity for learning
- Research: WHO [World Health Organisation]: find out which medical devices are really needed: such research does not exist currently.

- Regulator: driver for regulation development about security comes from USA through FDA, who has recognised 25 standards on security and interoperability as relevant for medical devices.
- Research is needed about what kind of security standards are published in other domains that might be transferable to the domain of medical devices.
- Clinical: In Germany, number of hospitals is decreasing. 1/3 German hospitals are bankrupt, 1/3 in private hands, 1/3 religious hands. The number of owners of hospitals in decreasing, but the consortia of private hospitals become larger: this will influence the relationship between health care providers and industry.
- Research: use of social media such as Facebook.

- Regulator: privacy and processing of sensitive data in the EU fall under the Personal Data Protection Directive which has its shortcomings, e.g. different implementations in the different member states.
- Research: need to change behaviour in health care regarding maintaining privacy and access control to patient information. Understanding of work processes at hospital.
- Clinical: Medical devices at home over public networks. Something can be done. Practicality will drive hospitals to adopt the European health care regulation.

In the concluding discussion, the point has been made to make the clinical process more important: we have to work together.

Some overarching questions that emerged:

What is the role of the patient? The patient is in a unique position. They are the key stakeholder in their own care. They become experts in their condition if it is a chronic condition. They possess background information and are the only stakeholder that progresses along every step of the patient trajectory along with the information that is created throughout that trajectory. Caregivers often have only a partial view and require multiple and potentially error-prone handovers. Patients as users of health information technology and medical devices in their own environments are also useful and important partners in providing requirements.

To what extent can or should technology act autonomously? What kind of legal and ethical implications are there? Or should health information technology such as remote sensor networks only act as a data collection and data distribution service?

What are training and capability requirements for different stakeholders? What do patients need to know and be able to do? What do organisations and regulators need to know and what kind of capabilities do they require?

How should trade-offs between effectiveness and safety be made? Safety risks can be to an individual, but also to society on a larger scale. How do we trade-off the risk to the individual with the benefit to many patients from a risk management and from an ethical perspective?

Who has responsibility and accountability in distributed services? A remote monitoring scenario can involve many different stakeholders, such as device and network manufacturers, community health services, hospital services, GPs, ambulance services. It may be difficult to specify one "risk owner".

Thoughts about a proposed Scotland Health workshop:
The topic is around managing risk in networked and distributed health services.
The aim is to involve health professionals and also patients, because these have not been adequately considered thus far. Patients are unique stakeholders with a particular interest. Health professionals as service providers are owners of risk and liability.
The aims of the workshop include:
Raising awareness of standards; bringing in operational experience; enabling a more mature dialogue between healthcare professionals and industry providers; identifying gaps in the needs of healthcare professionals.
The workshop could involve external speakers like Chris Johnson.

Summary of future activities

On 22 January, the joint meeting of the Medical Devices and Security subgroups of EWICS, to which workshop delegates were invited, discussed the workshop outcomes.

From the workshop, the following goals where identified:

a) Follow-up events, such as workshops, especially one targeting health care practitioners
b) Writing and publishing
c) Research

Ad a) follow-up events

- A workshop like this one, but aimed at health care providers, i.e. mixed target groups with emphasis on health care practitioners and their views on medical devices and assurance of safety and security... within 1-2 years.
- An EWICS regional workshop seems feasible in Scotland with NHS participants and in the near future, possibly in July 2014. First steps have been undertaken already and Geoff Duke is leading the local preparations.
- Some activity in relation with MedCom.
- An event with suppliers of medical devices - this requires a *white paper* with questions to manufacturers in preparation of the event
- Safecomp 2015 in Delft will have a strong flavour on Medical Technology
- Participants of the workshop decided to exchange contact details to enable future communication and joint activities

Ad b) publications

- A publication about the workshop discussions in a professional journal for health care practitioners
- A rewrite and submission of a draft paper for Safecomp 2014 (due per 28-2-2014) with input from the workshop: work in progress
- A white paper with questions to manufacturers and health care practitioners

Ad c) research

- Elicit research questions from the workshop presentations + notes
- Explore possibilities for collaborative projects inside and outside Horizon 2020
- A pilot project directly derived from the workshop might be an inventory and comparison of networked medical technology systems in different EU countries, how they are regulated and what issues need to be addressed by different stakeholders (health care organisations, patients, manufacturers, regulators, etc.).

Conclusion

Through the presentations, break-out sessions and panel sessions, the workshop has achieved its aims set out at the start. Future work has been identified to progress these aims and build a community of practice.

ANNEX A: RESULTS FROM BREAK OUT SESSIONS

Break-out sessions						
		Issues	item 1	item 2	item 3	item 4
Qset1						
Q1a	What are the conflicts between Safety and Security and how can they be resolved?	**access controls**	conflicts with easy access	single sign-on (wish)		
		safety - security	definitions: safety is about harm from inside the system; security is from outside the system...	security = part of safety	safety and security measures need to be balnced	safety is in conflict with privacy: needs to be balanced
Q1b	What are the Security Issues (e.g. privacy, legislation) and are these country dependent?	**hospital staff**	wants easy access (single sign-on)			
		availability	main priority for hospital staff	confidentiality & integrity ignored		
		legislation	different around the world	health care systems in EU by agreement not harmonised	security requirements often stem from privacy laws	legislation needs to be harmonised...
		patients	will move around: their data need to follow	may become data controllers	have the right to lie!	
		privacy	notion of privacy is country-dependent (cultural differences)			
		data integrity	is a security issue			

		Issues	item 1	item 2	item 3	item 4	item 5
Qset2							
Q2a	How much reliance is placed on the patient (e.g training, fault reporting)?	**target groups**	classify groups of patients	depends on culture	depends on condition & capability		
		cost/benefit	of relying or not on the patient				
		design	for the worst = not relying on patient	for the worst = 1 design fits all	battery lifetime		
Q2b	What are the issues of changing patient environment (e.g. home, hospital, trains, public areas)?	**reliable networks**	everywhere? 'dead' spots	scrambled	different networks (e.g. wifi, 3G/4G)	quality of service (QoS)	available bandwith
		remote actuation	should not be in a public place	plan B: emergency care	patient info for Y/N decision making	doctor info for Y/N decision making	
		location of patient	when does HC provider need-to-know?	different possibilities for plan B			

		Issues	item 1	item 2	item 3	item 4
Qset3						
Q3a	What are the constraints on using of third party services (e.g. public wireless networks, roaming)?	**intended use**	monitoring / remote intervention	criticality	determine "intended use"	training of users
		trust	third-party processing service is more problematic	network	availability, reliability, pricvacy, liability	secutity of data traffic
		price	higher trust is more expensive	getting a suitable contract		
Q3b	How should responsibility and liability be distributed over the involved parties?	**liability**	who earns is liable	delegation	patient should have only 1 party to hold liable (i.e. the HCP); other stakeholders should agree among themselves	physical security liability (HCP); logical security liability (IT/phone services, etc.)
		SLA	waterproof contracts	guarantees per contract		
		risk ownership	stakeholders	contractual controls	security responsibilities HCP - patient	apportionment of ownership

		Issues	item 1	item 2	item 3	item 4
Qset4						
Q4a	What are the constraints on patient mobility (e.g. travelling abroad, using public transport, avoiding wireless dead zones in e.g. a cellar)?	**criticality**	establish	risk benefit analysis	depends on frequency, length and urgency of connection	
		patient	needs to understand limitations, e.g. battery life, network coverage, intended use (monitoring, remote intervention) and criticality	emergency protocol if travelling	freedom not being allowed to travel is a serious constraint	needs to accept being part of tele-medicine, knowing its constraints
		doctor	informs patient and must make sure that patient understands			
Q4b	What issues (e.g. ethical, technical, regulatory, country) need to be resolved in remote intervention through implanted sensors?	**technical**	assurance of integrity, availability and security	capability to measure effect of intervention	testing	trust
		providers	liability leglislation (e.g. German vs. USA)	clarification of different responsibilities	should be subject to health care regulation when providing services to health care	
		remote	patient - doctor not co-located	intervention functionality		