Evaluation of Security and Privacy Issues in Integrated Mobile Telemedical System

Zlatko Stapic, Neven Vrcek, Goran Hajdin
Faculty of Organization and Informatics
Pavlinska 2, 42 000 Varaždin, Croatia
zlatko.stapic@foi.hr, neven.vrcek@foi.hr, goran.hajdin@foi.hr

Abstract. Different modern information and communication technologies are emerging in all segments of our lives. The simplicity of using these high-tech and high-performance components enables us to build a wide range of enhanced and fast-in-reaction telemedical systems with the purpose of improving the quality of living. While building these systems it is easy to overlook or underestimate the need for data security and privacy protection. Telemedicine and e-health laws, regulations and standards, along with other telemedicine infrastructure components in the USA, Europe and Croatia are compared and discussed in this paper. After the common model for integrated mobile telemedical system is proposed with the example of heart-work monitoring system, all possible vulnerable and weak points in its architecture are identified and recommendations on design and implementation of similar systems are also discussed and given.


1. Introduction

The development of technology influences, directly or indirectly, the development of all other sciences and implicitly has an impact on life quality. Modern technology findings enable us to create new, highly sophisticated and flexible systems that will help us raise the quality of life in different ways.

One of the scientific fields that have great benefits from this rapid technology development is medicine. It gains the possibility to create new, highly sophisticated and flexible systems that will help us raise the quality of life in different ways.

The key concepts used at development of this system are interesting in terms of data security and privacy. For example mobility, as one of the heart monitoring and analysis basic system elements, makes data in such system vulnerable and reachable during their wireless transfer become everyday practice. By its definition, telemedicine indicates the usage of information and communication technologies for providing long distance medical assistance, but also for faster distribution of medical knowledge [3][7].

The mentioned systems which use different new information and communication technologies, can be constructed in two different ways: by constructing all of system components from beginning or by constructing it from existing commercial components. Either way the need for implementation of security, privacy and data integrity mechanisms remain high priority.

One such sophisticated system for monitoring and analysis of heart activity was developed in 2006 by a group of students at the Faculty of Organization and Informatics [10]. The system was built from existing commercial components (COTS components), which were connected to each other through developed intelligent software and also commercially available communication technologies (Fig. 1).

Figure 1: Overall system architecture [10]

The key concepts used at development of this system are interesting in terms of data security and privacy. For example mobility, as one of the heart monitoring and analysis basic system elements, makes data in such system vulnerable and reachable during their wireless transfer
between components, if they are not protected according to certain rules and standards.

Consequently, lack of these legislation rules and standards is a big problem in telemedicine and telehealth. For example, in Croatia the standards, guidelines and laws related to a patient’s data security and privacy and telemedicine practically do not exist, so a certain attention in this paper will be given to this issue. The current state in Croatia will be compared with the existing legislations in Europe and USA, related to this question.

This paper also presents a review of the system architecture for heart-work monitoring and analysis as a model for other common systems, with a goal to define all vulnerable and weak security and privacy concerning points. Finally, concluding proposals for the design and implementation of data privacy and security measures for this and similar systems will be given.

2. Security and privacy in telemedicine

2.1. Existing standards and laws

Some telemedicine guidelines and standards already exist in countries like USA, Australia and internationally [5] but there is still no global e-health policy developed [4]. For over thirty years that telemedicine exists in the world, there is still no legal basis available.

With problems like the lack of laws and guidelines concerning security and privacy issues in telemedicine, there is no existing consensus related to the question who should take the responsibility of formulating telemedicine guidelines and standards [5]. One of the main problems for the lack of legal basis is slow development of standards. Not only that firm policies and guidelines for telemedicine are missing, laws must also deal with questions concerning interactions between physicians and patients over the Internet because they have not been well defined [9].

Guidelines and standards defined by various meetings, workgroups and associations are often used as a substitute for standards and laws on state and/or international level. Those guidelines and standards are trying to disseminate vast amounts of medical knowledge in forms which can be easily used and applied in practice [5].

With its formation, European Union gives hope for the bright future in telemedical and e-health field. In Europe there is hope for eventual firming of regulatory and legal standings [9]. That can be compared with situation in the USA where there are also more states under federal law. Most of the states carry out their own different laws which in some points could be mismatched.

In the medical practice, compliance and enforcement of patient’s privacy and confidentiality is of utmost importance. None of the information regarding patient’s physical and/or psychological condition, healthcare and treatment should be declared without the patient’s consent.

2.2. Legislation in Croatia

The law and legislative situation in Croatia concerning telemedicine is really scarce, precisely, it does not exist while there are only three laws that can be related to telemedicine. Additionally these laws do not have any subordinate regulations in which the telemedicine, privacy and data security questions would be more closely defined [23][22][16]. These and some other legislative documents in Croatia are presented chronologically in Table 1.

Table 1. Legislative documents related with telemedicine law in Croatia

<table>
<thead>
<tr>
<th>No.</th>
<th>Legislative documents</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary documents</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>Codex of Medical Ethics and Deontology [16]</td>
<td>2002</td>
</tr>
<tr>
<td>3.</td>
<td>Appendix to Protection of Privacy Data Law [22]</td>
<td>2006</td>
</tr>
<tr>
<td>Secondary documents</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Medical Treatment Law (cro: Zakon o liječništvu, NN 121/03)</td>
<td>2003</td>
</tr>
<tr>
<td>7.</td>
<td>Nursing Code (cro: Zakon o sestrinstvu, NN 121/03)</td>
<td>2003</td>
</tr>
<tr>
<td>8.</td>
<td>Code of Ethics for Medical Nurses (cro: Etički kodeks medicinskih sestara)</td>
<td>2005</td>
</tr>
</tbody>
</table>
Listed documents and laws represent the necessary base for definition of laws and standards concerning the security and privacy in telemedicine. As can be seen in Table 1, all the documents are divided into two categories regarding their possible influence on security and privacy protection in telemedicine.

The Protection of Privacy Data Law and its Addition are related to the questions about security violations, unauthorized data manipulation and privacy data abuse on a very general level. They also touch the question of security and integrity of data in situations when it must be transferred into another country which may have different laws and standards. The Codex of Medical Ethics and Deontology concerns the questions of medical confidentiality. It is also related to the protection and privacy of all collected data [16][22][23].

### 2.3. Legislative in USA & Europe

In the USA there are a few agencies and organizations that deal with telemedicine issues related to legislation, standards and guidelines. On the official site of American Telemedicine Association (ATA) [21] there is a list of guidelines: clinical, patient-health professional online communications, technical standards and others. Beside ATA there is one more centre which greatly deals with questions of telemedicine and e-health - Center for Telehealth & E-Health Law.

The legal basis for most telemedical and e-health standards and guidelines can be found in Telecommunications Act of 1996 [18]. That agency is “one of the federal government’s primary tools for supporting telehealth” [11].

A few surveys were conducted regarding telemedicine issues. When site-visitors were questioned what advance in telehealth is most important to them, from the offered answers 43% responded funding, 29% de-regulation, 19% legislation, and only 9% pointed out advancements in technology.

Since 2004 in almost half of the states full medical licensure for telemedicine is available. Also, there is a complete list of legislature and law information related to the licensure available for every federal state [17]. Information consists of a complete State Code and Administrative Regulation, separately for nurses and physicians.

In Europe there are also several organizations that deal with telemedical issues. One of them is Telemedicine Information Exchange (TIE) Europe, which is in close collaboration with TIE USA. On their web site there is complete list of telemedicine and telecare programs in Europe, with information on where, who and what program is being performed [19]. For the legislative part of TIE, the European site has no information, while USA has a list of federal and state laws with concrete information on every law. There are two more sites dedicated to e-health and telemedicine issues in Europe. Hospital Healthcare Europe is designed to improve communication between European hospitals and support efficiency and effectiveness in systems in which those hospitals work, but it does not concern any legal or standardization issues [14].

<table>
<thead>
<tr>
<th>Infrastructure component</th>
<th>HR</th>
<th>US</th>
<th>EU</th>
</tr>
</thead>
<tbody>
<tr>
<td>High level abstraction (base) legislation laws defined</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Detailed legislation laws defined</td>
<td>-</td>
<td>+</td>
<td>+/-</td>
</tr>
<tr>
<td>Telemedicine concerning standards defined</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Codex of medical ethics defined</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Established and formed telemedicine organizations</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Created and maintained web sites and portals</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>International telemedicine law defined</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Aimed financial subventions arranged</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Methodical research and surveys performed</td>
<td>-</td>
<td>+</td>
<td>+/-</td>
</tr>
<tr>
<td>Data confidentiality and privacy importance perception</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Full medicine licensure available</td>
<td>-</td>
<td>+/-</td>
<td>-</td>
</tr>
<tr>
<td>Telemedical and telecare programmes running</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Legislative bills with concrete information available online</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2. Croatia, Europe and US telemedicine infrastructure comparison

Similar to that organization is E-Health Europe which is dedicated to e-health issues, but in some cases it does concern telehealth legislative questions. Answers to those questions are not based on laws, but are just guidelines which show the need for standardization and
solving of legislation questions [12]. E-Health Europe also focuses in more detail on telemedicine situation in Austria, France, Germany and Italy [13]. In Europe there is still a lack of standards and legislative background concerning telemedicine security and privacy issues. Although there are some detailed surveys, their results just address the need for standards and legal basis [6].

Comparing the telemedical infrastructure established via different organizations, defined standards, legislation laws and other infrastructure components of USA, Europe and Croatia we can conclude that Croatia lags way behind. See Table 2 for more details.

3. Integrated system security and privacy

While discussing system’s security and privacy issues, the first step should be a quick view at its architecture and components defining it. The connections between these components are probably the most vulnerable points and thus very important to be carefully considered. The heart work monitoring and analysis system architecture is in detail described in paper [10]. Pointing out system functionality and goals, short overview of this architecture will be presented in this chapter.

The mentioned system’s main characteristic is 24/7 heart work monitoring and analysis. Instead of using classic Holter devices patients can, while still being monitored, leave hospital and do their normal everyday activities. Consequently, mobility can be considered as the core of this system. Other uses of the system include heart work recording in extraordinary situations (e.g. in cases of natural disasters) or at places without proper medical infrastructure (like small islands, villages or similar).

Briefly, previously described functionality is accomplished in integration of several different components and technologies. As can be seen in Figures 1 and 2, the first component is wireless digital Holter ECG device which records heart work and transmits data to developed PDA application. After transmitted to the second component, the data is filtered, analysed, displayed and stored in the local database. If certain irregularities are found, critical or suspicious segment of data is automatically sent to the third component, web service. Patient’s GPS position is sent along with critical segment, enabling the hospital to locate and find the patient if necessary. A web service store received data into the main database and sends an alarming message to the doctor. Finally, the fifth component is the web application which can be accessed via any web browser, allowing the doctor to examine data and give a proper diagnose. If necessary, the doctor can upload a segment of data and ask for his colleagues’ opinions on specially developed community forum.

![Figure 2: Overall system architecture with out-pointed vulnerable points](image)

The overall system architecture is multi-tier, which requires additional security and privacy consideration because layer junctions are also vulnerable and could be system weak points. In order to clearly present the system architecture and to expose all vulnerable points, the system can be divided into a set of separate devices, modules and applications which communicate and work together. The architecture shown in Fig. 2 can also be used as a representative model
of other similar systems. The replacement of only four components will result in a system with slightly or completely different functionality. As the resulted system remains telemedical one, the privacy and security concerns and weak points pointed out in our example should also be taken into consideration in implementation of any other derived and similar system.

From the architectural point of view, such telemedicine system has only five architectural components. But as can be seen in Fig. 2, we identified at least seven (7) critical and vulnerable points which should be covered with a proper attention in process of implementation of this-like systems.

The first identified weak point is the wireless connection between heart work recording device (HWRD) and PDA application. Depending on the implementation, data can be transmitted via Bluetooth, IC or any other wireless technology. In general, two security methods can be used. Either the sensitive patient’s data should be encrypted before transmission or, wireless transmission should be secured with the use of proper security protection. There are several possible methods of counteracting security risks. Wi-Fi Protected Access (WPA) [2], IEEE 802.11i (WPA2) [15], IEEE 802.1x and RADIUS are security protocols that can be used and implemented. Additionally, it is important to say that this vulnerable point emphasis privacy as significant problem, while private and personal data (recorded data) can be retrieved from unauthorized application.

System’s second weak point pertains to wired and wireless data transmission. Although different technologies are used here, security could also be obtained in two different ways. Either via personal developed encryption and decryption system or by means of secure data transfer layer implementation. There are several different ways in gaining secure data transmission, including Secure Hyper-Text Transfer Protocol (HTTPS) implemented via Secure Socket Layer (SSL) or implementation of encryption algorithms. Authentication and authorisation methods should also be implemented as well in order to ensure senders and receivers identity and rights preservation. The same or similar measures should be implemented on the third, fifth and sixth vulnerable point, while communication between connected modules is also performed via wired or wireless networks. Depending on system topology and defined architecture, suitable analysis should be performed in order to determine optimal security settings.

As critical security point (the fourth indicated point in Fig. 2) of this system, we can identify the system database which is available on the Internet and where data related to all patients, history of their diseases and other sensitive information is stored. Unless certain security regulations and standards are applied during its implementation, system would become vulnerable in terms of patients security and privacy.

Finally, the last weak point can be medical-client computer (which will certainly have authorized access to sensitive data). If this computer is exposed to unauthorised access or if it is attacked by malware applications or any other software designed to infiltrate and steal confidential data, it represents a potential threat to the whole system in terms of security and privacy.

Following the medical and telemedicine standards and laws, if they are defined, this-like systems implementations should take into consideration all privacy and security aspects regarding patients privacy and data protection. Using different security principles and measures, defined in this section it is certainly possible to implement to all legally defined acts.

4. Conclusion

As we can conclude, the process of telemedicine standards and laws definition started in the USA and Europe a few years ago. Results are evident in the created telemedicine infrastructure that consists of constituted associations, developed web and support pages and relatively big financial subventions. On the contrary, in Croatia telemedicine infrastructure is not developed. Laws and standards are defined at very basic levels, and no financial expenditures are directed towards this infrastructure creation.

In this paper, the existing legality acts and documents along with other basic telemedicine infrastructure components are discussed and compared. The model for any integrated mobile telemedical system with an identified and out pointed vulnerability and weak points is also presented along with the recommendations on how to implement a safe and protective
telemedicine system in the terms of security and privacy.
In further research in this field, best US and European practices in telemedicine and e-health laws and standards should be recognised, listed and enumerated. The recommendations on how to apply these laws in Croatia’s legislation or in telemedical systems implementation should also be given.

5. References

[22] ** Zakon o dopunama Zakona o zaštiti osobnih podataka. NN 118/06; http://www.nn.hr/clanci/sluzbeno/2006/261 6.htm [01/12/2008]
[23] ** Zakon o zaštiti osobnih podataka. NN 103/03; http://www.nn.hr/clanci/sluzbeno /2003/1364.htm [01/12/2008]