SECURITY IN THE HEALTH CARE APPLICATIONS OF DIGITAL TELEVISION

Samuli Niiranen¹, Artur Lugmayr¹, Heikki Lamminen¹ and Seppo Kalli¹

¹Institute of Signal Processing, Tampere University of Technology, P.O. Box 553, 33101 Tampere, Finland, {samuli.niiranen, artur.lugmayr, heikki.lamminen, seppo.kalli}@tut.fi

ABSTRACT

Digital television is an emerging media platform with many application areas. One of these areas is health care service provision where security related questions are especially important. In this paper we seek to explore the realization of secure health care applications (using an example application deployed in the Health Care TV project at the Digital Media Institute of the Tampere University of Technology) in standardized, DVB-MHP compliant digi-TV and recognize unified multimedia frameworks such as MPEG-21 as one future possibility in the provision of secure digi-TV health care services.

1. INTRODUCTION

Digital television (digi-TV) provides an interesting platform for health care service provision with scenarios ranging from health education to treatment related services. Security questions are critical in all health care applications of the new media, including those of digital television. The emphasis of security in health care applications results from both practical needs and legislative requirements. For example, confidentiality and integrity of patient record information should never be compromised as erroneous information can potentially result in serious complications for the patient.

Seven fundamental principles have been proposed for the ethical treatment of medical records including [1]:

1. **Principle of information-privacy and disposition**
   Everyone has a fundamental right to information privacy and hence a right to control over the collection, use and disposition of data about themselves.

2. **Principle of openness**
   The collection, use and disposition of personal data must always be disclosed to the subject of the data.

3. **Principle of access**
   The subject of an electronic record has a right to access the record and a right to correct the record with respect to its accurateness, completeness and relevance.

4. **Principle of legitimate infringement**
   The fundamental right over the collection, use and disposition of personal data is conditioned only by the legitimate information needs of the society and by the equal and competing rights of others.

5. **Principle of least intrusive alternative**
   Any infringement of the privacy rights of the individual may only occur in the least intrusive fashion.

6. **Principle of accountability**
   Any infringement of the privacy rights of the individual must be justified to the affected person.

7. **Principle of security**
   Data that has been legitimately collected about a person must be protected by all measures reasonable and appropriate against loss, degradation, unauthorized destruction, use, modification or disclosure.

As evident from the principles, ethical treatment of patient records and other sensitive health related information includes many aspects for which there is no technical security solution available or even imaginable; security of information in a health care environment depends also on compliance with policy not just on technical controls [2]. However, a digi-TV environment, as a media platform for accessing services utilizing patient record or related information, can provide the necessary technical security controls (primarily related to principle 7) as described in our paper.

2. APPLICATION OF DIGI-TV IN HEALTH CARE

2.1 Health care application areas of digi-TV

Application of digital television in (personal) health care services was reviewed in an earlier paper [3]. The identified three principle areas of personal health care services include informational, treatment related, and rehabilitation services. As patient record information is primarily handled in treatment related services the emphasis will be on their security aspects.

2.2 Follow-up of oral anticoagulant treatment through digi-TV

We use as an illustrative example of a treatment related service the digi-TV supported follow-up of oral anticoagulant treatment. In practice, the follow-up of oral anticoagulant treatment includes regular capillary blood sample testing by a patient on anticoagulation medication
using a portable meter. The results of these tests are used by the physician responsible for the treatment to set new treatment guidelines for the patient including anticoagulant medication dosages and dates of next follow-up tests.

As illustrated in Figure 1 the system consists of patient and physician terminals and a service core. The digi-TV part of the system is DVB-MHP (Digital Video Broadcasting - Multimedia Home Platform), the European standard for interactive digital television, compliant including a BSP (Broadcast Service Provider), a broadcast network, a STB (Set-Top-Box), an interaction channel and an ISP (Interaction Service Provider).

The patient terminal in our scenario is a digi-TV STB. In practice, the patient uses an end-user application multiplexed in a standard MPEG-2 transport stream transmitted to STB using a, e.g. terrestrial, broadcast network. The application provides an interface for accessing resources available in the service core of the ISP using the interaction channel, typically the public Internet, of the digi-TV system. In practice, the patient stores the capillary blood sample follow-up test results and monitors for new treatment guidelines set by the physician using a standard web service with an Internet-PC.

The service core provides data storage and management services, including maintenance of the treatment database, which is used to store the follow-up data, and provides interfaces for the different media environments of the system.

Figure 1. Digi-TV supported anticoagulant treatment follow-up

The described system is to be deployed in the HCTV (Health Care TV) project at DMI for a pilot study of digi-TV supported anticoagulation follow-up.

3. SECURITY REQUIREMENTS OF HEALTH CARE APPLICATIONS

Three general security goals (mostly related to principle 7 of section 1) have been identified for health information systems which are also relevant for our case study. These goals are data integrity, data availability and data privacy [4].

1. Data integrity: To maintain the integrity of health care data we must ensure that data is accurate, complete, and trustworthy.
2. Data availability: To provide reliable access to health care data by authorized persons with a legitimate need.
3. Data privacy: To ensure that health care data remains private and will not be disclosed without the permission of the owner of the data.

An additional digi-TV related security goal is also introduced here.

4. End-user application authentication: End-user application authentication ensures that the application the end-user is using for accessing health care data is provided by an authorized source.

4. REALIZATION OF SECURE HEALTH CARE APPLICATIONS IN DIGI-TV

We approach the question of realizing secure health care applications in digi-TV using the four security goals described earlier in the context of the digi-TV part of the anticoagulation follow-up system to be deployed in the HCTV project. The techniques and considerations identified are to be realized in the system.

4.1 Data integrity

Accuracy, completeness, and trustworthiness are maintained in the system in the following ways:

1. Validation of human submitted health data
   All health data submitted by the patients to the system has to be validated before it is stored permanently in the treatment database of the service core. In practice this can be provided by including input validation in the human UI of the digi-TV end-user application.
2. Reliable networking protocols
   Networking between the STB and the service core using the interaction channel is based on the reliable TCP protocol providing protection for data duplication and data loss.
3. Database integrity
   All the health data is stored in the treatment database of the service core. Used standard relational databases provide adequate safeguards for maintaining database integrity.

4.2 Data availability

Data availability is a multi-level question including system downtime minimization, reliable identification of users and data access rights control.
1. **Minimum system downtime**

The service should be available to users with minimum downtime. This can be achieved by using tested and reliable software and hardware resources throughout the system.

2. **Reliable identification**

Reliable identification can be provided in the system by using standard password user identification or smart card based secure identification. For example, the Finnish EID platform provides for the latter.

3. **Data access rights control**

Health care data should be available to only the users with a legitimate need. For example, individual patients must able to access only their own health data from the end-user application.

4. **Data privacy**

Data privacy in a digi-TV environment is mainly maintained in the networking context. The European standard for interactive digital television DVB-MHP [5] includes separate channels for data transfer in a digi-TV environment: the broadcast channel [6] and the interaction channel [7].

Encryption of data is the primary method for maintaining data privacy in the networking context. In a DVB-MHP compliant digi-TV system the interaction channel supports the use of the secure HTTPS protocol for encryption. The broadcast channel also provides mechanisms for encryption. However, in our scenario the interaction channel is exclusively used for the transmission of confidential health information.

4.4 **End-user application authentication**

In a DVB-MHP compliant digi-TV system the broadcasted application code, e.g. of our treatment end-user application, can be authenticated using file signing. Application authentication can be used to ensure that the end-user application is from an authorized source.

5. **FUTURE TRENDS OF HEALTH CARE SECURITY IN DIGI-TV**

The realization of a secure health care application described in section 4 was done in the context of a digi-TV system corresponding to the existing DVB-MHP standards. However, there are new emerging standards, such as MPEG-21, providing a context for a unified multimedia framework also for digital television including new approaches to security related questions.

The vision for MPEG-21 is to define a multimedia framework to enable transparent and augmented use of multimedia resources across a wide range of networks and devices used by different communities based on the concept of digital items [8]. One of the seven key elements defined in MPEG-21 is *Intellectual Property Management and Protection* including provisions for the authentication and identification of applications and data which could be applied in the development of secure health care digi-TV services. In fact, the MPEG-21 Use Case Scenarios [9] include a Medical Case Package where a MPEG-21 digital item is identified as a container for health related data to be used in health care data transactions throughout the diagnosis and treatment of a particular medical case (e.g. of our example application) and privacy is identified as one of major the implications for MPEG-21 of the scenario. We will next briefly describe the concept of a medical package which can be considered a derivative and more generalized form of the Medical Case Package. Figure 2 shows the medical package as central element for accessing medical content from multiple involved groups.

5.1 **Declaration of medical packages**

A medical package consists of medical content assets in form of patient records, treatment procedures, medical images, examination results, etc., wrapped together with its content descriptions to one digital entity stored in a medical database system. Thus, a digital item (DI) in the medical case consists of medical related content and its descriptions constituting a medical package or a digital medical item. Such a digital medical item is divided in its declaration (metadata annotations) as defined by MPEG-21’s digital item declaration language, its references to content assets (MPEG-21’s reference declarations), and medical content data (defined by medical standards). Each digital medical item groups medical sub-items of medical content (e.g. patient-, doctor-, or administrative records) in form of MPEG-21’s container structures.

To describe a digital medical item further structures are required, to provide a structured standard representation, unique identification, unified content transactions, and compilation of different assets. Relating content descriptors and content assets in a distributed network architecture is done via resource descriptors, pointing to concrete medical content (e.g. medical database).

A medical sub-item (Figure 3) can be of arbitrary content type (e.g. X-ray images), that are annotated by their content description (e.g. X-ray image content annotated by its medical diagnosis). This approach enables an end-to-end delivery of medical cases, and exchange between health personnel, patient, health administration, and social care institutions.
Due to the strict top-down approach, validation of submitted health data, and data integrity is enabled throughout the life-cycle of a digital medical item. Utilizing MPEG-21 requires a harmonization with purely medical based standards, such as HL-7 [11] or DICOM [12], as MPEG-21 only defines the structure of a common digital item, rather than how the concrete medical content has to be structured. For example, HL-7 provides standards for the exchange, management and integration of data that support clinical patient care and the management, delivery and evaluation of healthcare services. Specifically, to create flexible, cost effective approaches, standards, guidelines, methodologies, and related services for interoperability between healthcare information systems [11].

5.2. Delivery to authorized persons anytime, anyhow

MPEG-21 offers furthermore a unique identification of a medical package, and its sub-items in arbitrary forms (e.g. simple URI), but due to the early stage of the development of the standard, currently no medical related descriptions are available. A registration authority for maintaining lists of identification schemas is established.

A special feature of MPEG-21 is the rights expression language (REL), where users or principals are assigned with rights subject to conditions for accessing resources. Currently REL is based on XrML [10]. Defined is a model and core system for transparent and augmented use of right schemes (Figure 4) and the relation between parties based on a rights data dictionary (RDD).

Medical content is required to be accessed through the right person at the right time, and by multiple end-platforms. MPEG-21 addresses this issue by the definition of a digital item adaptation mechanism. To deliver to different platforms content assets and its descriptors are related to available hardware resources, such as available bandwidth, display facilities, preferences, etc. This guarantees service delivery in emergency cases, rapid content access, and data availability on multiple end-platforms one of which can be digi-TV.

5.3 Content protection and security mechanisms

Security and content protection evolves according the following axis:
- Secure transmission protocols on lower layers
- Medical content protection and authentication
- Invoking legacy standards to secure content
- User authorization for content access

Besides user rights management a more significant problem is the protection of medical content to maintain privacy and unauthorized data access. MPEG-21 provides description schemes for content protection, application authentication, and secure transmission protocols of any form. Therefore it is obsolete to rely on currently standardized protection mechanisms, such as defined by HL-7 [11], watermarking-, and encryption mechanisms.

6. CONCLUSIONS

Security is an important aspect for new media based health care services, especially for those related to treatments where confidential health information is typically stored and transmitted within the context of the service. Digi-TV, as a new media platform, can provide a secure media environment for health related services, e.g., in the follow up of oral anticoagulant treatment as was described in this paper through the fulfillment of general health information system security goals.

In addition, new developments in unified multimedia frameworks, such as MPEG-21, can in the future provide new approaches for providing security in the health care applications of digi-TV. For example, MPEG-21 digital item based medical packages, as described briefly in this paper, can provide a unified approach e.g. to the secure exchange of medical and other health related information in a media convergent setting with multiple end-platforms.

7. REFERENCES


