INTERNATIONAL JOURNAL OF MEDICAL INFORMATICS 76 (2007) 484–490

journal homepage: www.intl.elsevierhealth.com/journals/ijmi

End-to-end Security in Telemedical Networks – A Practical Guideline

Florian Wozak, Thomas Schabetsberger, Elske Ammmenwerth*

Institute for Health Information Systems, UMIT, University for Health Sciences, Medical Informatics and Technology, Eduard Wallnöfer Zentrum 1, Hall in Tyrol, Austria

ARTICLE INFO

Keywords:
Medical informatics
Computer security
Medical network security
Systems analysis

ABSTRACT

The interconnection of medical networks in different healthcare institutions will be constantly increasing over the next few years, which will require concepts for securing medical data during transfer, since transmitting patient related data via potentially insecure public networks is considered a violation of data privacy.

The aim of our work was to develop a model-based approach towards end-to-end security which is defined as continuous security from point of origin to point of destination in a communication process. We show that end-to-end security must be seen as a holistic security concept, which comprises the following three major parts: *authentication and access control, transport security, as well as system security*. For integration into existing security infrastructures abuse case models were used, which extend UML use cases, by elements necessary to describe abusive interactions. Abuse case models can be constructed for each part mentioned above, allowing for potential security risks in communication from point of origin to point of destination to be identified and counteractive measures to be directly derived from the abuse case models.

The model-based approach is a guideline to continuous risk assessment and improvement of end-to-end security in medical networks. Validity and relevance to practice will be systematically evaluated using close-to-reality test networks as well as in production environments.

1. Introduction

The electronic processing of medical data which is expected to improve quality and efficiency of health care systems [1], will lead to an increasing amount of medical data exchanged across institutional boundaries [2].

1.1. Motivation

The transmission of patient related data over public networks can be seen as a violation of national and international data protection acts [3–5]. Therefore, a universal security infrastructure is required for the exchange of medical data [6,7]. *End-to-end security* is introduced to safeguard information in an information system from point of *origin* to point of *destination* [8].

1.2. Drawbacks of present situation

As stated in the annual Symantec Internet Security Threat Report 2005, medical institutions have been repeatedly affected by targeted network attacks [9]. Given the sensitivity of medical data a high threat potential can be assumed.

* *Corresponding author*. Tel.: +43 50 8648 3813; fax: +43 50 8648 673813.
E-mail address: florian.wozak@umit.at (F. Wozak).
1386-5056/$ – see front matter © 2006 Published by Elsevier Ireland Ltd.
doi:10.1016/j.ijmedinf.2006.09.020

The threat potential for *telemedical networks*, which was not analyzed by the Symantec report, is expected to be much higher than for individual institutions, since medical data are transferred via potentially insecure networks.

Security concepts are currently mainly based on *authentication*, *authorization and transport security* (encrypted data transfer). At the moment there are no adequate methods to assess the security standard and threat potential. The abovementioned security standards are implemented as independent components. There is no experience as to how they can be integrated within a holistic security concept which provides end to end security.

1.3. Aim of this work

The aim of this work is on the one hand to develop a model-based approach to assess the security level and threat potential for telemedical networks. On the other hand knowledge gained by the development of such security models will be used to build concepts for end-to-end security. This comprises the following steps:

(1) Development of security models which allow the assessment of threat potential and deduction of counter measures.
(2) Combining the individual security measures to form a holistic security concept.
(3) Validation of models on the basis of a realistic test network.

In this article, we describe preliminary results for the development of an integrative security concept and its validation on the basis of a test network.

2. Introduction to abuse case models

Abuse cases are defined as an interaction of an actor with an information system which causes *harm* to either the system itself or other actors. By definition an illegitimate interaction with a system only becomes an abuse case if effective damage is caused, for example, the compromise of a cryptographic key is not an abuse case as such, but if the attacker decrypts data without authority, an abuse case arises. To complete an abuse case the attacker needs to abuse *privileges* that allow the abusive interaction to succeed [10].

Abuse case models and their graphic representation are based on standard UML use cases [11,12]. This facilitates the design process with common UML design tools. Abuse case models are extended by elements which provide for the detailed description of the abuser and the abusive interaction [10]. The following characteristics of the *actors* are crucial for understanding an abuse case:

- Resources.
- Skills.
- Objectives.

The *abuse case* as an illegitimate interaction with an information system is described by:

- Harm.
- Privilege range.
- Abusive interactions.

Technical and financial resources of potential attackers are modeled as *Resources*, whereas their knowledge such as experience in programming or networking is represented as *Skills*. Long-term goals can be recorded as *Objectives*.

The maximum damage that a successful attack might cause is described as *Harm*. The *Privilege range* reflects the minimum range of security privileges that have to be abused in order for an attack to be successful. This parameter is closely related to components that might be exploited.

3. Methods

The abuse case models we used for security modeling, which are described in Section 2, differ from the original models developed by McDermott and Fox [10] through the introduction of an *attack vector* instead of abusive interaction. With this modification, we expect to facilitate the detection of vulnerabilities and the development of counter measures. The attack vector depicts the possible *attack route* as a collection of network attacks rather than an attack scenario. The abuse cases comprise attack description, abuse case description in textual representation, and an abuse case diagram in graphic, UML conform representation.

Depending on the intention and the methods used, attacks can be classified as *targeted attacks* and *non-targeted attacks*. We mainly concentrated on targeted attacks because it can be assumed that the abuser is highly interested in gaining access to medical data.

Abuse case models are developed in three steps:

(1) Initially goals and interests of possible attackers are summarized as objectives. The *actors* are identified by associating individuals with the previously obtained objectives. Abusers and objectives cannot be recognized in automated attacks since they randomly hit information systems.
(2) Hence, a second step is necessary to identify automated attacks. Attack vectors of already known automated attacks can be found in various security forums. Abuse case models for these types of attacks are focused on the systems used in the specific telemedical network.
(3) After objectives and actors are identified, resources, skills, harm and privilege range can be easily assigned to the abuse cases. The sum of interactions exploiting different vulnerabilities is described as attack vector. A prioritization is possible by considering the *maximum harm* expected by a specific attack.

3.1. Considerations toward an integrative security concept

The previously developed models allow attacks to be classified by their *attack vector*. Based on this classification, security techniques to block a specific attack vector can be identified as “axes”.

The integrative security concept can be developed based on this classification in combination with the abuse case models. The feasibility of attack scenarios is therefore evaluated in the context of the information systems currently in use. A theoretic success of an attack vector identifies a specific vulnerability. The threat potential that emerges from the abuse case can be estimated by means of *harm* and *privilege range*. Additionally, information about possible intentions of the attacker is determined by the *objectives*.

The integrative security concept is based on the obstruction of the attack vector on the entirety of axes. Furthermore, security measures to reduce the potential harm of an abuse case can of course improve overall security, but the primary goal is to block the attack vector rather than rely on symptomatic protection against its effects.

3.2. *Validation of abuse case models by means of a test network*

The validity of abuse case models will be evaluated on the basis of a realistic test network. This approach was chosen because network attacks will have to be carried out, which would undermine existing security policies in a productive environment. We selected the branch *man in the middle attack* (see Fig. 1) described for the abuse case *intruder* for the experimental proof of concept. A detailed description of the attack can be found in Section 4.3.

The aim of this approach is to validate our assumption that an abuse case can be prevented by the obstruction of the attack vector. Thus, an unsuccessful attack following blockage of the attack vectors is considered proof of the integrative security concept.

4. Results

4.1. *Identified abuse cases*

As the coverage of all possible abuse cases seems to be extremely complex, this study focused on abuse scenarios which seem to be the most relevant for telemedical networks. As a result, the following actors have been identified:

Non-targeted attacks:

- Malware (software which causes damage to the host system such as virus, worms, Trojan horses, Spyware).
- Script Kiddies (inexperienced attackers who use software not developed by them to hack randomly chosen systems by exploiting known vulnerabilities).

Targeted attacks:

- Saboteur (actors who try to cause damage to systems or destroy data without the intention to access medical data).

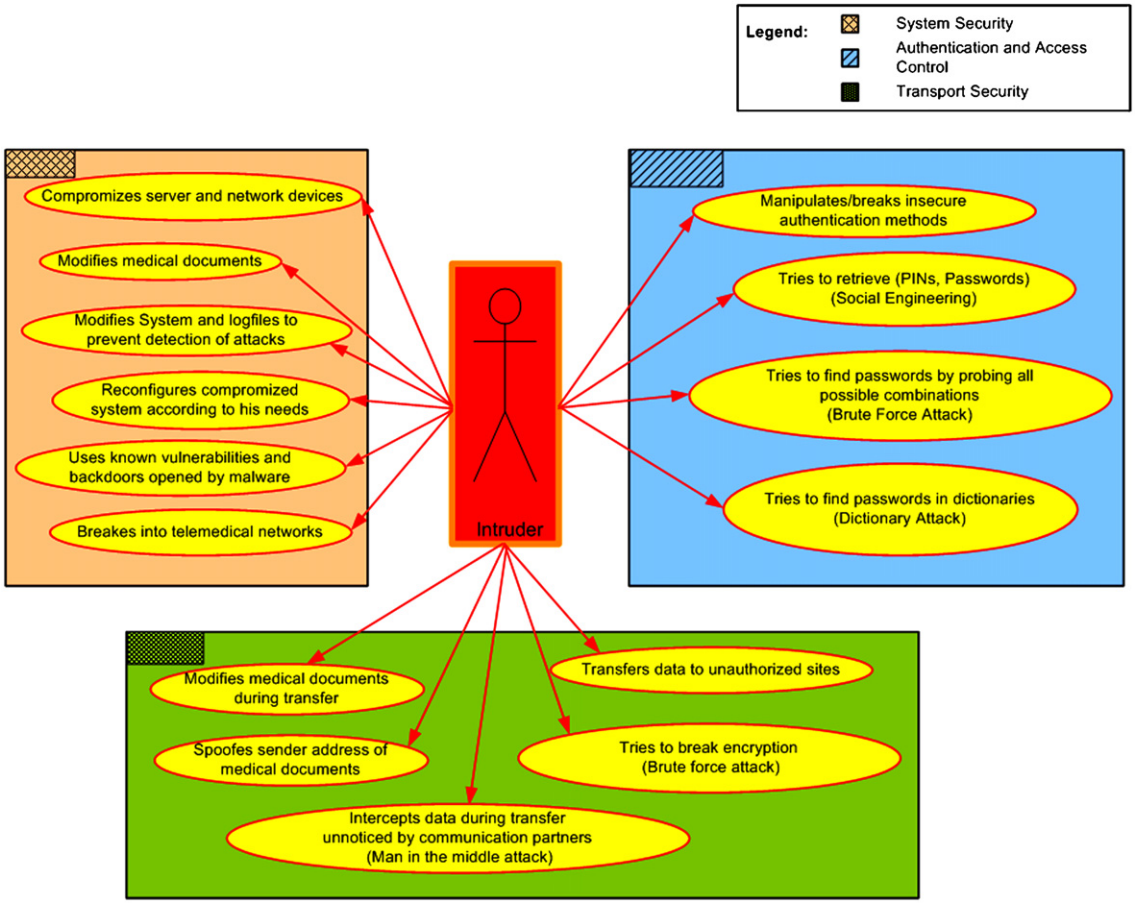

Fig. 1 – Abuse case diagram intruder. For further details refer to the text.

Table 1 – Actor description intruder

Resources	
	Individuals or group of people with the same intentions
	Support by criminal organizations
	Multiple PCs or servers with internet connection
	Potentially physical access to internal LANs
	Specially crafted software (exploits)
	Hardware and software tools for breaking cryptographic keys (brute force attacks)
Skills	
	Superior skills in networking and programming
	Detailed knowledge of network protocols
	Profound knowledge of cryptographic algorithms and protocols
Objectives	
	Criminality
	Highly interested in medical data
	Aggressive methods for getting access to medical data
	Targeted search for medical documents of individuals or groups of persons

For further details refer to the text.

- Intruder (actors with strong interest in medical data using unlawful methods to complete their objectives).

Exemplary we depict the abuse case intruder since the highest threat potential can be assumed for this class of attack. Table 1 shows the abuse case description for "intruder", or actors, who aggressively try to gain access to medical data by spending a lot of time and even money to achieve their aim.

Fig. 1 shows the abuse case diagram for "intruder". The diagram shows that abusive interactions can be classified as attacks against:

- Information systems.
- Authentication and access control systems.
- Transport security.

As shown in Table 2 an intruder can abuse high privileges and gain full control over information systems.

4.2. *Considerations towards an integrative security concept*

As shown in abuse case diagram (Fig. 1) and abuse case description (Table 2) a categorization of the attacks against information systems, authentication and access control systems and transport security can be performed.

Based on the insights gained, three *principal axes* are identified:

Authentication and access control: authentication methods such as user-name and password, token based or biometric authentication methods. Authentication furthermore comprises a trust relationship between systems guaranteed by digital certificates. Due to their sensitivity against dictionary attacks, brute force attacks and social engineering password based authentication methods should no longer be used in a high security environment.

Table 2 – Abuse case description intruder

Harm	
	Unauthorized access to the entirety of medical documents transferred via or processed by the compromised information system
	A compromised host inside a telemedical network can serve as starting point and so facilitate attacks against other systems
	Terms of data protection can no longer be sustained by affected institutions
	Deliberate modifications of medical data can lead to errors in treatment
Privilege range	
	User or service privileges that have access permissions for medical data of interest as a minimum requirement
	Administrative or root permissions on compromised systems for arbitrary access to processed or transferred data
	Installation of backdoors facilitates access at a later point of time
Attack vector	
	Exploitation of vulnerabilities in programs or operating systems
	Insecure authentication methods
	Inadequate (too short) key length of cryptographic keys
	Tricking users into revealing login credentials, usually username and password (social engineering)
	Brute force attacks against authentication methods of server and active network devices (Router, Firewalls)
	Man in the middle attacks to intercept data flow unnoticeable by the communicating partners internal attacks originating from an institution's LAN
	External attacks originating from the internet

For further details refer to the text.

Transport security: methods for protecting data during transfer over public networks comprise: authenticity of communicating partners, data privacy by encryption, integrity by cryptographic checksums and non-repudiation by digital signatures. These requirements are met by the application of *cryptographic protocols*.

System security: preventing manipulation of information systems which can lead to unauthorized access to medical data can be accomplished by measures of system security such as patch management, firewalling, intrusion detection/prevention.

Vulnerabilities in any of the three principal axes can be the basis of a successful attack. End to end security therefore demands for their integration into a *holistic* security concept. Based on the identified vulnerabilities, counter measures, which result in an obstruction of the attack vector can be directly derived. As shown in Table 2, the attack vector *Inadequate (too short) key length of cryptographic keys* can be blocked by the application of strong cryptography.

The threat potential of an abuse case is considered averted only if all the attack vectors are blocked. In some cases a specific attack vector can be obstructed by independent methods. If in this case the obstruction occurs on distinct principal axes, then the overall security can be improved.

Therefore, to ensure the highest level of security, we recommend to use at least two distinct security methods (on different principal axes) to protect medical data from unauthorized access.

The development of an integrative security concept is not a static, but rather a *dynamic* process. Objectives of potential abusers change over time as do their methods. New attack vectors will be found. Then again improvement of security methods will be able to prevent a subset of them.

Based on these facts strong emphasis has to be placed on the dynamic adaptation of the abuse case models according to the current security threats. The analysis of firewall, intrusion detection/prevention logfiles can therefore be helpful. The lessons learned should be the basis for a continuous amelioration of the security concept.

4.3. *Validation of abuse case models by means of a test network*

Given the constraints of testing in production environments a realistic test network was chosen to prove the validity of the integrative security concept. In this setup the data transfer via the file transfer protocol (FTP) from the clinical information system (CIS) to the transmission gateway server responsible for sending discharge letters to providers of health care networks is simulated.

Fig. 2(a) shows the test network setup and the original data flow, and Fig. 2(b) describes the man in the middle attack.

The attack described here is accomplished by manipulating the assignment of Ethernet address (MAC) to IP address. After the successful attack the IP addresses of both, the FTP client and FTP server point to the MAC address of the intruder. This results in all packets transferred from the client to the server and vice versa, wrongly being sent to the attacking host.

Packets are then forwarded to the originally intended system to allow communication between client and server without allowing them to notice the redirected data flow. Techniques to manipulate the address resolution protocol (ARP) cache, known as *ARP cache poisoning* or *ARP spoofing* are used to manipulate the MAC to IP assignment on the Ethernet switch. Without having received an ARP request the attacker sends spoofed ARP replies with the IP addresses of client and server pointing to his station's MAC address. The following spoofed ARP reply is used to manipulate the ARP cache for the FTP client machine:

[IP : 10.4.1.80 to MAC : 00 : 08 : 02 : C9 : 2B : EF]

The ARP cache manipulation of the server machine is achieved by the following spoofed ARP reply:

[IP : 10.4.1.43 to MAC : 00 : 08 : 02 : C9 : 2B : EF]

As a result, the Ethernet switch stores the spoofed IP to MAC assignments in the ARP cache and then incorrectly forwards all packets to the attacker. It has been shown that in the test setup an attacker can intercept the data flow without being detected by the communicating partners and retrieve confidential information such as username and plaintext password as shown in Fig. 3.

To prevent the man in the middle attack from being successfully executed counter measures can be taken at each principal axis as follows. This results in improved overall security if integrated within a holistic security concept.

The attack vector (see Section 3) of the man in the middle attack can be obstructed by system security, transport security and authentication and access control. *System security* comprises the activation of security measures in the Ethernet switch configuration to detect spoofed MAC to IP address assignments. Cryptographic protocols such as IPSec on the network layer or secure file transfer protocol (SFTP) on the application layer provide *transport security*. In the case of the man in the middle attack on the one hand authenticity of communication partners is provided by digital certificates. On the other hand, the transferred data is protected by payload encryption of the transport protocol. As the third principal axis *authentication and access control* has to be integrated to replace the insecure user name and password authentication. SmartCard or token-based authentication methods do not require login credentials to be transferred as plain text. As a measure to minimize the potential harm of this abuse case (unauthorized access to medical documents), data should be encrypted independently from the transport protocol.

After the identified settings had been applied, a second run of the man in the middle attack was started. As expected the

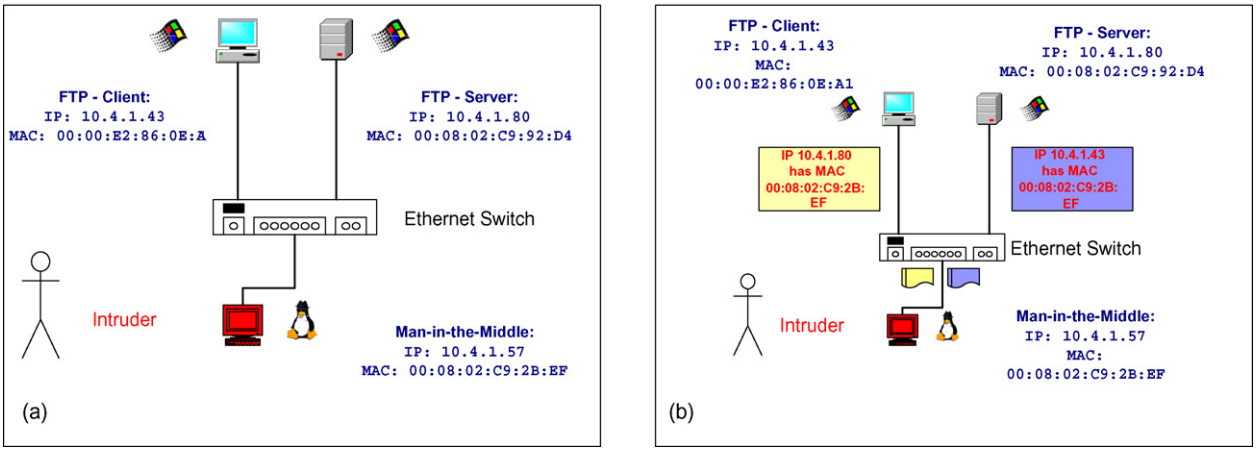

Fig. 2 – Test network for proving the validity of the integrative security concept. In (a) the original setup is shown, (b) describes the man in the middle attack and the redirected data flow. For further details refer to the text.

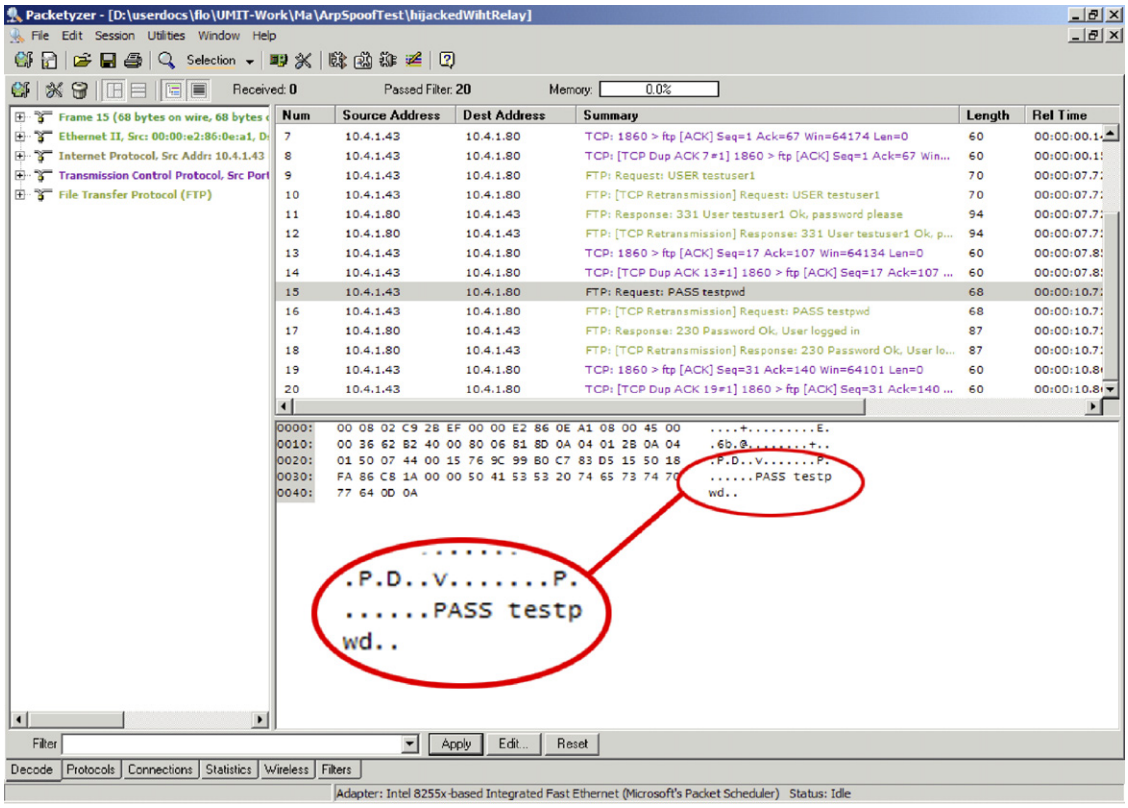

Fig. 3 – Plaintext password retrieved by the intruder during the man in the middle attack. For further details refer to the text.

attack vector was obstructed by security measures activated in the Ethernet switch, so the attack failed.

The analysis of the abuse case intruder in the test network has shown that the proposed methods for an integrative security concept towards end to end security improved overall security.

5. Discussion

The aim of this paper is the development of abuse case based security models for telemedical networks and the deduction of an integrative security concept towards end to end security based on them. The applied Abuse case security models are well suited as *overview models* for networks with a limited degree of complexity.

They reach their limits if detailed modeling of networks with high complexity is required. On the other hand the models depend on sufficient knowledge about the actors, which makes them less appropriate for evaluating the threat potential of specific systems when these are widely unknown. Furthermore, the completeness of abuse case models can not be guaranteed, which is why it is currently impossible to prove that all potential abuse cases have been considered. The evaluation of threat potential and vulnerabilities as a system centered view can be achieved by using attack tree models introduced by Bruce Schneier [13], which are based on possible attack targets rather than on potential abusers. Attack tree models can easily be reused for systems with a similar setup.

Abuse case models can be constructed with sufficient granularity for the assessment of threat potential and vulnerabilities. As proven in the experimental setup the models are suited for the deduction of countermeasures which can then be used to create the integrative security concept towards end to end security. Limitations are again expected when actors are widely unknown and high granularity is required. In this case, attack tree models seem to be more appropriate [14]. Practical experiences will show whether the identified principal axes are sufficient or if further axes have to be considered.

Due to rapid changes of attack scenarios and the fact that completeness of models cannot be guaranteed abuse case models have to be *constantly adapted* to ambient conditions. Outdated models become invalid, which endangers the complete security concept. Analysis of attempted or successful misuse should be used to extend and update the models.

6. Outlook

For a quantitative study reliable measuring methods will have to be developed for acquisition of attacks against telemedical networks. Security issues that will arise in distributed, heterogenous environments are currently not solved adequately. The adaptation of the proposed security models to meet the requirements for distributed systems is the subject of our recent work.

REFERENCES

[1] N. Maglaveras, I. Chouvarda, V. Koutkias, S. Meletiadis, K. Haris, E.A. Balas, Information technology can enhance quality in regional health delivery, Meth. Inf. Med. 41 (5) (2002) 393–400.

[2] R. Haux, E. Ammenwerth, W. Herzog, P. Knaup, Health care in the information society. A prognosis for the year 2013, Int. J. Med. Inform. 66 (1–3) (2002) 3–21.

[3] BGBl. I Nr. 165/1999 idF: BGBl. I Nr. 136/2001, Bundesgesetz ueber den Schutz personenbezogener Daten (Datenschutzgesetz 2000—DSG 2000), http://ris.bka.gv.at/bgbl-pdf/, 2000 (accessed on May 12, 2005).

[4] Council of Europe, Convention for the Protection of individuals with regard to automatic processing of personal data Convention No. 108 (Strasbourg: CoE), http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm, 2000 (accessed on Aug 22, 2005).

[5] Food and Drug Administration, Department of Health and Human Services, 21 CFR Part 11, http://www.21cfrpart11.com/files/library/government/21cfrpart11_final_rule.pdf, 2000 (accessed on May 16, 2005).

[6] C. Dierks, Legal and social implications of health telematics in the EU, in: B. Blobel, P. Pharow (Eds.), Advanced Health Telematics and Telemedicine, vol. 96, IOS Press, Amsterdam, Netherlands, 2003, pp. 143–148.

[7] S. Callens, Telemedicine and European law, Med. Law 22 (4) (2003) 733–741.

[8] Committee on National Security Systems, National Information Systems Security (Infosec) Glossary, http://security.isu.edu/pdf/4009.pdf, 2000 (accessed on Dec 12, 2004).

[9] Symmantec, INC, Symantec Internet Security Threat Report Volume VI, http://enterprisesecurity.symantec.com/content.cfm?articleid=1539, 2000, (accessed on Mar 12, 2004).

[10] J. McDermott, C. Fox, 15th Annual Computer Security Applications Conference (ACSAC '99), 1999, p. 55.

[11] Object Management Group, OMG Unified Modeling Language Specification, http://www.omg.org/docs/formal/03-03-01.pdf, 2004 (accessed on May 23, 2005).

[12] B. Oestereich, Die UML-Kurzreferenz fr die Praxis, 2nd ed., Oldenbourg Wissenschaftsverlag GmbH, Muenchen, Deutschland, 2002.

[13] B. Schneier, Attack Trees, http://www.schneier.com/paper-attacktrees-ddj-ft.html, 2000 (accessed on June 03, 2004).

[14] F. Wozak, Modellierung der Intrusion Detection fuer einen Krankenhaus Verbund, FH-Salzburg Fachhochschulgesellschaft mbH, Salzburg, Austria, 2002.