IJCSN - International Journal of Computer Science and Network, Volume 6, Issue 5, October 2017
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Evidential Modeling for Telemedicine Continual Security

[1] Sofienne Mansouri, [2] Bel G Raggad

[1] U of Tunis El-Manar, ISTMT, Lab of Biophysics and Medical Technologies, Tunisia

[2] Seidenberg School of CS & IS, Pace U, New York, USA

Abstract - Telemedicine has not advanced at the same pace as IT and its own medical technologies. The long-awaited progress has been hindered aggressively by security risks that came with innovative information and communication technologies. One major technological factor to blame for this tardiness in telemedicine is its information security that lead to patients and doctors attrition and hence system infeasibility. Given the great deal of uncertainties and ambiguities in the telemedicine environment, Bayesian reasoning does not offer a sound approach to tackle all the security problems menacing telemedicine. For this article proposes an evidential reasoning model to manage risks due to security uncertainties and ambiguities characterizing most telemedicine environments. Dempster and Shafer Theory is used to process security management evidence for the purpose to forecast the overall security risks associated with the continual feasibility of a telemedicine system. This article also provides a numerical example to demonstrate the working of the proposed evidential reasoning model.

Keywords - *Telemedicine, Dempster and Shafer theory, evidential reasoning, Belief functions, security risk.*

1. Introduction

Telemedicine has been around now for several decades, but it is not advancing at the same pace as other technologies. In fact, telemedicine has shown greater deficiencies despite the advances in most information and telecommunication technologies. Most of the risks that continued to rise with the rise of technology has hit telemedicine very hard and slowed its adoption and progress. These risks are mainly associated with lacks in information privacy and concerns associated with computer and network security.

Even though you can see many major telemedicine networks, like American Well, MDLIVE, and Teladoc, they are all hit with all types of government regulations across state borders, in addition to major health standards like HIPAA, HL7, and regional data protection acts ([3], [4], [6]).

The significant progress made in the IT community should certainly advance the telemedicine field. Advancement in secure data sharing among patients, health providers, and insurance agencies with assured mutual trust and information privacy established a robust platform for real-time healthcare delivery. The entire nation started to accept the deployment of electronic health information systems and the federal government has sponsored it ([1], [10]).

The major part of telemedicine that has seen great development is the use of telecommunications to provide medical information and services. This includes simple data transfer among members of the telemedicine environment including emails and videoconferencing. A more advanced example would be the use of satellite technology to broadcast a consultation between providers at facilities in two countries, using videoconferencing equipment and robotic technology.

Telecommunication has been enhanced to allow physicians and specialists in remote health to deliver health care, diagnose patients, and provide therapy in a real-time manner. Telemedicine software systems have been also enhanced to allow for medical diagnostic activities but these have been limited to augmenting the performance of the communication effort and not necessarily the decision support part of the diagnosing effort [12].

Major applications involved in the telemedicine effort include radiology, pathology, cardiology and e-health education. Telemedicine adopted a variety of approaches including Store-and-Forward, Home-Health, Real-Time, and other asynchronous methods ([10], [11], [8]).

In this paper we refer to telemedicine simply as the use of technology to provide health care at a distance, and we are mainly concerned with the security of its computing environment. . We see that this recent field is certainly playing a great role in delivering healthcare nationwide and the entire nation is committed to it. There are then risks associated with the telemedicine's own information security that considerably depends on the security of all its subsystems on its network of health service deliveries: Remote patients, remote doctors, remote hospitals, remote data resources, mobile

units, insurance agencies, and its distributed computing environment.

This article proposes an evidential reasoning model aiming at assuring a continual feasibility of a telemedicine system through effective information security. The security posture of the telemedicine system is written in terms of the security postures of all its subsystems and the effectiveness of owners' efforts to assure continual security. While the strength of a security posture is expressed as the belief function of adequate security, in contrast, the system security risk is expressed as the plausibility of ineffective security.

2. Evidential reasoning model for the telemedicine system

Let us consider the environment of a generic telemedicine system as reported in most of the literature [] as having multiple subsystems H_1, …, H_M that are all connected together for the purpose of a feasible delivery of telehealth services as required by all state and national laws and regulations. Given the structure of a telemedicine system, all performance deficiencies and security threats on any of the telemedicine subsystems will affect the overall security of the telemedicine environment. This is to say that any factors affecting the security of one of the subsystems can propagate to the main telemedicine system and compromise it. One compromised, the telemedicine will lose its feasibility as an e-healthcare provider and my shut down. There is certainly no doubt that the information security of the telemedicine environment is a consequential variable to continuously manage below any security risk levels accepted and defined in the system security policy. Figure 1 depicts the generic constitution of a telemedicine environment and how information security propagates throughout its computing environment.

No matter how you define uncertainty, ambiguity, or ignorance [Han et al), Telemed is full it. The great deal of uncertainty in all its forms and lack of structure will make impossible for Bayesian theory to accommodate any decision modeling for most information security decision. An evidential reasoning model, using Dempster and Shafer Theory, becomes hence very essential.

Such a security evidential reasoning framework for a telemedicine environment has to define all information security parameters that affect the overall security of the telemedicine system. Let us say, after consulting with telemedicine owners and their information security management team, that it is sufficient to examine M+1 decision parameters: M security parameters s_1 through s_M defining the security postures of all subsystems H_1 through H_M constituting the telemedicine environment; and the additional security parameter s0 summarizing the continual security efforts applied by telemedicine owners to keep its security risks lower than the acceptable level defined in the telemedicine system security policy.

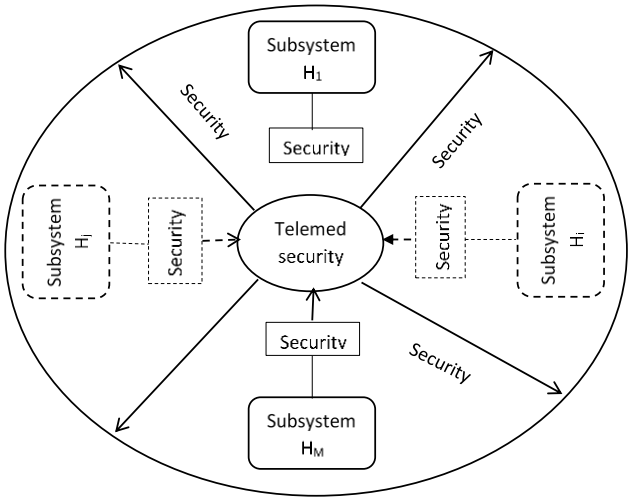

Figure 1: Generic telemedicine security structure

That is, in order to maintain an acceptable continual security level for the telemedicine security level, we need to continuously manage the security of all its subsystems $\{H_i\}_{i=1,M}$. and also exercise an adequate information security management level by system owners in a continuous manner. Let us assume that we can capture all information security management information using a belief scheme consisting of M+1 assertions, a_0, a_1, …, a_M. The assertions a_1, …, a_M are belief structures translating the adequate security postures of respectively the subsystems H_1, …, H_M. The assertion a_0 expresses the adequacy of the security posture for the overall telemedicine system.

Of course, there won't be any way to study those assertions unless we can define the basic belief assignments constituting their belief structures. And these belief structures can only be shaped up if we can elicit sufficient evidence to do so. Let us assume that for every assertion a_i, i=1,M, we collect a subset of evidence E_i constituting of $|E_i|$ belief structures e_{i1}, …, $e_{i|Ei|}$. The evidence of telemedicine owners' efforts to maintain a continuously adequate security posture is capture by a single belief structure e_0 that will be fused later with the rest of the evidence to produce information of the overall security posture of the

system. This evidential reasoning structure is depicted in Figure 2.

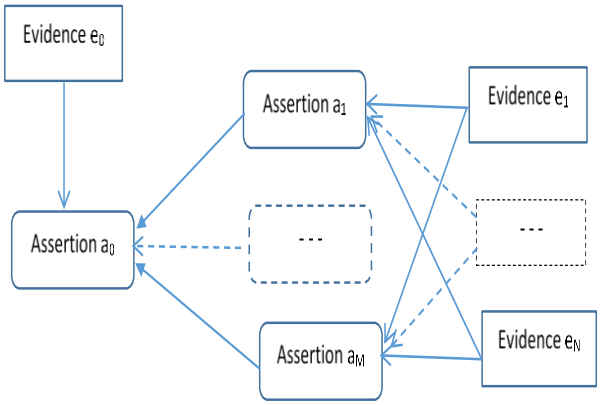

Figure 2: Evidential structure defining the security of the telemedicine system

Table 1: Evidential structure for security management

Layer 0:
Begin Layer 0:
Layer 0 = Sublayer 01, Sublayer 02}
Sublayer 01:
{
a_0: $m_{[Telemed]}$: $2^{\Phi 0} \rightarrow [0\ 1]$
$\Phi_0 = \{a_{01}, a_{02}\}$
a_{01} = 'Adequate overall Telemed's security posture'
a_{02} = 'Inadequate overall Telemed's security posture'
}

Sublayer 02:
{
$E_0 = \{e_0\}$
e_0: m_0: $2^{\Omega 0} \rightarrow [0\ 1]\}$
$\Omega_0 = \{e_{01}, e_{02}\}$
e_{01} = 'Adequate Telemed's owners effort for continual overall security of the system'
e_{02} = 'Inadequate Telemed's owners effort for continual overall security of the system'
}
}
End of Layer 0;

Layer 1:
Begin: Layer 1
Layer 1= {$Sublayer_{11}$, …, $Sublayer_{1M}$}
$Sublayer_{11}$:
{
a_1: m_1: $2^{\Phi 1} \rightarrow [0\ 1]$
$\Phi_1 = \{a_{11}, a_{12}\}$
a_{11} = 'Adequate H1's security posture'
a_{12} = 'Inadequate H1's security posture'
}
- - -
$Sublayer_{1M}$:
{
a_M: $m_M 2^{\Phi M} \rightarrow [0\ 1]$
$\Phi_M = \{a_{M1}, a_{M2}\}$
a_{M1} = 'Adequate H_M's security posture'
a_{M2} = 'Inadequate H_M's security posture'
}
End of Layer 1

Layer 2:
Begin Layer 2:
Layer 2= {$Sublayer_{21}$, …, $Sublayer_{2M}$}
$Sublayer_{21}$:
{
$E_1 = \{e_{11}, \ldots, e_{1|E1|}\}$
{
e_{11}: m_{11}: $2^{\Phi 11} \rightarrow [0\ 1]$
$\Phi_{11} = \{e_{111}, e_{112}\}$
e_{111} = 'Adequate Security Controls Set 1'
e_{112} = 'Inadequate Security Controls Set 1'
}
- - -
{
e_{1E1}: m_{1E1}: $2^{\Phi 1E1} \rightarrow [0\ 1]$
$\Phi_{1E1} = \{e_{1E11}, e_{1E12}\}$
e_{1E11} = 'Adequate Security Controls Set |E1|'
e_{1E12} = 'Inadequate Security Controls Set |E1|'
}
}
- - -
$Sublayer_{2M}$:
{
$E_M = \{e_{M1}, \ldots, e_{M|EM|}\}$
{
e_{M1}: m_{M1}: $2^{\Phi M1} \rightarrow [0\ 1]$
$\Phi_{M1} = \{e_{M11}, e_{M12}\}$
e_{M11} = 'Adequate Security Controls Set M'
e_{M12} = 'Inadequate Security Controls Set M'
}
- - -
{
e_{MEM}: m_{MEM}: $2^{\Phi MEM} \rightarrow [0\ 1]$
$\Phi_{MEM} = \{e_{MEM1}, e_{MEM2}\}$
e_{MEM1} = 'Adequate Security Controls Set |EM|'
e_{MEM2} = 'Inadequate Security Controls Set |EM|'
}
}
End of Layer 2.

3. Evidential reasoning process

Let us recall what we have achieved so far in terms of defining all the variable retained to manage the security of our telemedicine system. Only one assertion is studied and that is a_0 expressing the adequacy of the overall security of the telemedicine system. We then selected M assertions a_1, …, a_M to capture the adequacy of the security posture of the M telemedicine subsystems H_1, …, H_M. Additionally, we defined M evidence subsets E_1, …, E_M that will feed the needed information to construct respectively the assertions a_1, …, a_M. The following vectorial scheme shown in Table 1 gives a rather cumbersome representation of the evidential structure that we thought may help those who are interested to follow the mathematical computations of the root assertion associated with the overall security of the telemedicine environment:

3.1 Demonstration of the working of the ER model

Let us consider a simple telemedicine architecture, as shown in Figure 3, made of 7 main subsystems: Computing Environment (CE) subsystem, Patients subsystem, Doctors subsystem, Hospitals subsystem, Medical Data Resources subsystem, Mobile Units subsystem, and Insurance Agencies subsystem. We assume that the overall security of the telemedicine environment depends on 7 security postures associated with the 7 telemedicine subsystems identified in this example, in addition to the adequacy of the continual security efforts exercised by system owners. The computations are provided in Table 2.

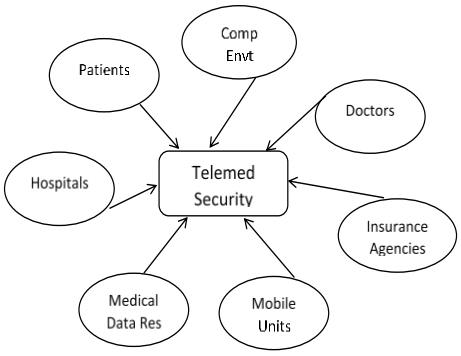

Figure 3: An example of a generic telemedicine architecture

.

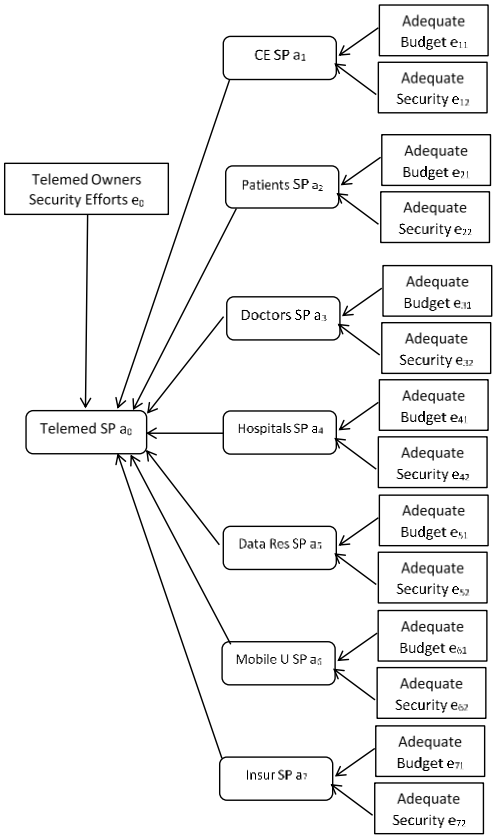

Figure 4: Evidential architecture for a Telemedicine system

4. Conclusion

The article looked into the telemedicine tardiness in following current advances in information and telecommunication technologies and proposed an evidential reasoning model to tackle its security problems believed to be one of the major hinders of telemedicine progress. Given the great deal of uncertainties and ambiguities in the telemedicine environment, Bayesian reasoning does not offer a sound approach to tackle all those security problems menacing telemedicine. We proposed an evidential reasoning model to manage risks due to security uncertainties and ambiguities characterizing most telemedicine environments.

We employed Dempster and Shafer Theory to process security management evidence for the purpose to forecast the overall security risks associated with the continual feasibility of a telemedicine system.

This article also provided a numerical example to demonstrate the working of the proposed evidential reasoning model.

References

[1] Blavin, F., et al., Final Report: Lessons from the Literature on Electronic Health Record Implementation, U.S. Department of Health and Human Services, http://www.healthit.gov/, (2013).

[2] Demiris G, and D. Tao, An analysis of the specialized literature in the field of telemedicine. Journal of telemedicine and telecare. 11(6): 316-327, (2010).

[3] De Moor, G. et al., Using electronic health records for clinical research: The case of the EHR4CR project, Journal of Biomedical Informatics, Vol 53, pp 162-173, (2015).

[4] Doherty, N., & H. Fulford, Aligning the information security policy with the strategic information a systems plan. Computers & Security, 25, pp 55-63, (2006).

[5] Duan, L., Street W.N., and Xu, E., Healthcare information systems: data mining methods in the creation of a clinical recommender system, Enterprise Information Systems, 5(2), 169-181, (2011).

[6] El Fadlya, A.et al., Electronic Healthcare Record and Clinical Research in Cardiovascular Radiology: HL7 CDA and CDISC ODM Interoperability, AMIA 2007 Symposium Proceedings, pp 216-220, (2007).

[7] John Craig, J., and V. Patterson, Introduction to the practice of telemedicine, Journal of Telemedicine and Telecare, 11(1), pp 1-9, (2005).

[8] Kiernan, TE. J. and Demaerschalk, B.M., Nursing Roles within a stroke Telemedicine network, Journal of Central Nervous System Disease, 2, 1–7, (2010).

[9] Paul K.J. Han, KJP, Klein, WMP, and Arora, NK, Varieties of uncertainty in health care: a conceptual taxonomy, Medical Decision Making, 31(6), pp 828–838. (2011).

[10] Stoten, S., 2009. Health Policy Issue with the Electronic Health Record, Online Journal of Nursing Informatics (OJNI), 13(2), 1-14, (2009).

[11] Talmon J. AE., et al., STARE-HI: statement on reporting of evaluation studies in health informatics. International Journal of Medical Informatics, 78(1), pp 1-9, (2009).

[12] Xu, E., Wermus, M., and D.B. Bauman, Development of an integrated medical supply information system, Enterprise Information Systems, 5(3), pp 385-399, (2011).

Table 2: Computations to fuse available evidence to produce the assertions

	Budget evidence				Adequate security				Iterative Fusion		
	Adeq	Inadeq	Either one		Adeq	Inadeq	Either one		Adeq	Inadeq	Either one
Computing Env sec posture	0.3	0.4	0.3		0.5	0.3	0.2		0.5	0.4	0.06
Patients sec posture	0.4	0.6	0		0.5	0.4	0.1		0.44	0.55	0
Doctors sec posture	0.6	0.3	0.1		0.6	0.3	0.1		0.75	0.23	0.01
Hospitals sec posture	0.3	0.7	0		0.7	0.1	0.2		0.56	0.43	0
Med Data sec posture	0.5	0.4	0.1		0.6	0.3	0.1		0.67	0.31	0.01
Mobile U sec posture	0.6	0.3	0.1		0.6	0.2	0.2		0.77	0.2	0.02
Ins agencies sec posture	0.7	0.3	0		0.3	0.5	0.2		0.62	0.37	0
Fuse a1-a2	0.5	0.4	0.06		0.44	0.55	0		0.46	0.48	0.04
Fuse a1-a3	0.46	0.48	0.04		0.75	0.23	0.01		0.74	0.24	0.01
Fuse a1-a4	0.74	0.24	0.01		0.56	0.43	0		0.79	0.2	0
Fuse a1-a5	0.79	0.209	0		0.67	0.31	0.01		0.87	0.1	0.01
Fuse a1-a6	0.87	0.1	0.01		0.77	0.2	0.02		0.95	0.03	0.01
Fuse a1-a7	0.95	0.03	0.01		0.62	0.375	0.01		0.98	0.02	0.01
a0 = Fusion of e0 and a1-a7	0.98	0.02	0		0.43	0.53	0.04		0.975	0.02	0

PS: Due to the approximations used in all computations, the m-values did not add to 1.