JOURNAL OF HEALTH INFORMATICS

Acces-control authorization model for Health Information System (HIS) in Brazil

Modelos de autorização de controle de acesso em Sistemas de Informação em Saúde (SIS) no Brasil

Modelo de autorización de control de acceso en Sistemas de Información de Salud (SIS) en Brasil

Marcelo Antonio de Carvalho Junior[1], Paulo Bandiera-Paiva[2]

ABSTRACT

Keywords: Information systems; Information security; Gatekeeping; Standards

Objective: To report access-control implementations for authorization management in Health Information Systems (HIS) using opinion polls. **Method:** The selected target audience was Brazilian Society of Health Informatics (SBIS) members or participants in interest groups promoted by this association, totaling 1400 respondents. A 12 questions online survey was conducted using the REDCap tool, during the period of 30 days. **Results:** A total of 134 valid responses were collected. Most HIS currently implement RBAC, 82.7% report that this access-control model meets current demand, 23.8% stated that they did not adhere to the model recommended by the SBIS certification manual in version 4, 6.9%, 17.2% and 17.2% of the HIS' developers respondents declared future intention to use this model in the short, medium and long term, respectively and 17.9% stated intention to change to hybrid models with RBAC or extensions. **Conclusion**: The conducted survey shows Brazilian HIS current implementations of access-control and future expectations.

RESUMO

Descritores: Sistemas de informação; Segurança da informação; Controle de acesso; Normas

Objetivo: Reportar implementações de controle de acesso em Sistemas de Informação em Saúde (SIS), voltadas ao gerenciamento de autorização, por meio de pesquisa de opinião. **Método:** O público-alvo selecionado para a pesquisa de opinião composta por 1400 respondentes ligados ao tema de SIS por meio de associação ou participação em grupos de interesse promovidos pela Sociedade Brasileira de Informática em Saúde (SBIS) foi selecionado. Um questionário composto por 12 questões foi aplicado de forma online aos respondentes por meio da ferramenta REDCap, durante o período de 30 dias. **Resultados:** Um total de 134 respostas válidas foram coletadas. Segundo respostas obtidas, a maioria dos SIS implementa RBAC atualmente, 82,7% reportam que este modelo de controle de acesso atende a demanda atual, 23,8% declararam não aderência ao modelo recomendado pelo manual de certificação SBIS em sua versão 4, 6,9%, 17,2% e 17,2% dos respondentes desenvolvedores de SIS declararam intenção de mudança à curto, médio e longo prazo para este modelo, respectivamente e 17,9% declararam intenção de mudança para modelos híbridos com RBAC ou extensões do mesmo. **Conclusão:** A pesquisa de opinião realizada mostra implementações atuais de controle de acesso em SIS brasileiros e expectativas de mudança futura.

RESUMEN

Descriptores: Sistemas de información; Seguridad de la información; Control de acceso; Normalización

Objetivo: Informar implementaciones de control de acceso para la gestión de autorizaciones en Sistemas de Información de Salud (SIS), tilizando encuestas de opinión**Metodologia:** La audiencia seleccionada para la encuesta de opinión fue compuesta por 1.400 respondientes comprometidos con el tema de SIS por medio de asociación o participación en grupos de interés promovidos por la Sociedad Brasileña de Informática de la Salud (SBIS). Una encuesta online compuesta de 12 preguntas fue realizada utilizando la herramienta REDCap, durante el período de 30 días. **Resultes:** Se recogieron un total de 134 respuestas validas. De acuerdo con las respuestas obtenidas, la mayoría de los SIS actualmente implementan RBAC. 82.7% informan que este modelo de control de acceso satisface la demanda actual. 6,8%, 17,2% y 17,2% de los desarrolladores del SIS, declararon su intención futura de utilizar este modelo en el corto, mediano y largo plazo, respectivamente. Un total de 17,9% manifestó intención de cambiar a modelos híbridos con RBAC o sus extensiones. **Conclusión:** La encuesta realizada muestra actuales implementaciones de control de acceso en SIS brasileños y expectativas de cambio futuro.

[1] *Pós-graduando em Gestão e Informática em Saúde, Universidade Federal de São Paulo - UNIFESP, São Paulo (SP), Brasil.*

[2] *Departamento de Informática em Saúde, Escola Paulista de Medicina, Universidade Federal de São Paulo - UNIFESP, São Paulo (SP), Brasil.*

Autor Correspondente: **Marcelo Antonio de Carvalho Junior**
e-mail: **carvalho.junior@unifesp.br**

Artigo recebido: **13/07/2017**
Aprovado: **28/05/2018**

INTRODUCTION

Access control is a 3-step process intended to mediate interactions from users (subjects) and system resources (objects). In the third step, called authorization, it provides mapping of available objects and approved functions/ operations to a specific user or group. The authorization list (grants) is called access-control matrix and is deemed as the most basic abstract form of security policy enforcement.

Formal access control models based on this abstract concept include mandatory access control (MAC), discretionary access control (DAC) and Non-discretionary Access Control (N-DAC). A hybrid model combining elements from these models is also possible, although careful validation must be carried out to make sure no new weakness is added[1].

MAC refers to centralized authorization constraint imposed by the system directly, restricting operations on objects. DAC refers to object authorizations being controlled by the data-owner or other previously authorized user, passing the access-grants to others.

N-DAC refers to centralized authorization based on task or role binding with users. The most common implementation of this type is the Role-based Access Control (RBAC)[2]. Health Information Systems (HIS) are an example of environment that can benefit from the dynamic nature related to role-based access-control. The health-care industry uses RBAC massively on its systems leveraging security policy properties.

The Health Insurance Portability and Accountability Act (HIPAA) program for instance, requires user-based access control, role-based access control or context-based access control since 1996 (HIPAA security standard, at section 142.308 - https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations). Brazilian Society of Health Informatics (SBIS - http://www.sbis.org.br/) electronic health records (EHR) certification program checks RBAC characteristics for its systems certification program during audits as a mandatory requirement. Document version 4.2 (2016) of the requirements for this certification recently included the need of RBAC on its more basic format (Core). More specifically, the requirement NGS1.04 – Authorization access-control attest for RBAC features.

This report presents results from an online survey performed last semester (may – jun/2017) with the intent of identifying current security implementations for authorization control of HIS and future plans for improvement, if any. Internet surveys are commonly used to reach geographically dispersed respondents retrieving opinions from experts, to assess population desires or to determine current state of technology for example. Recently, HIMSS north America biennial publication presented a survey collecting opinion from 368 U.S. health IT leaders regarding their perspectives of the most important topics of interest for the health IT industry. Privacy, Security and Cybersecurity were among highly-ranked themes casting 5.86 points in scale[3]. This study comprises: (a) Methods, describing the group of respondents as well as the survey questionnaire, time-period for data collection and the tool that was used. (b) Results are presented segmented by theme; (c) Current

implementation and future predictions are discussed based on the interpretation of responses;(c) Current implementation and future predictions are discussed based upon responses interpretation; (d) Conclusions.

METHODS

The survey was conducted via the Internet, using REDCap tool for questionnaire production and web-publishing. REDCap installation used was hold within Escola Paulista de Medicina (EPM) IT servers infrastructure, accessible to users via the link: https://redcap.epm.br/surveys/?s=FFWP4TE8LX. The questionnaire was divided in two sections, the first dedicated to minimal demographic registration from respondents. Also, the presentation of research design and objectives, responsibilities, benefits to participants, rights to access the generated data and results, applied confidentiality and other terms were shown at appended informative TCLE document file on survey web-page. The second section was dedicated to collect opinion regarding the access-control used on HIS, applied security perception of its implementation and the preview for next steps in terms of authorization control improvements. The questionnaire browser transition (from one section to the following) was controlled by required fields and fully TCLE acceptance.

The entire questionnaire comprised 12 questions and the estimated time for completion was around 8-10 minutes. REDCap web forms automatically captured partial responses if not fully completed by respondents by the time of survey expiry.

The participants from our target population were invited by e-mail (See invitation file, TCLE details and full questionnaire – Portuguese only at http://www.bioinfo.unifesp.br/HIS-RBAC). The selection of respondents was made considering that the health IT opinion was concentrated on persons that are connected to SBIS activities and HIS certification program, either by formal association or participants in the special interest working groups (SIG). The SBIS interface was hence used to connect with participants. An invitation e-mail with the REDCap survey link was sent to a total of 1400 participants.

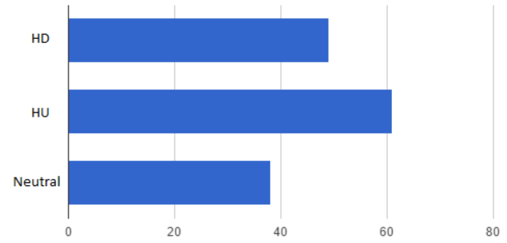

Figure 1 – Respondents' type graphical quantities

Participants were segregated in three different types (self-declared at survey' first section), namely: neutral, HIS developer (HD) or HIS user (HU) (See Figure 1). 4 additional

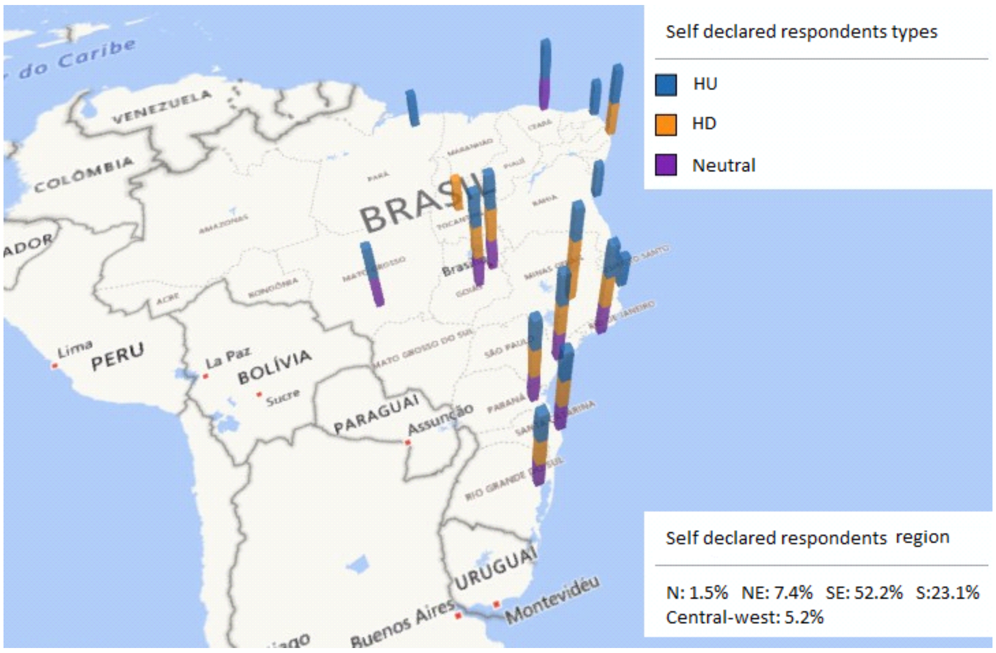

Figure 2 – Respondents' geographical distribution (type distinguished by color)

e-mails were sent to respondents (1 per week) as a friendly reminder to survey completion until the closing date. The findings here presented comprise the responses collected from 05/01/2017 to 06/05/2017. A total of 152 responses were collected during survey period. After assessing and filtering the data-set, non-valid respondent code identifiers and duplicates were removed. In the event of duplicity, only last contribution was considered for analysis. The geographical distribution from respondents is depicted at Figure 2.

A. Bias and uncertainties

Notice that, we did not control the respondent population division and distribution in terms of geographic spread or type of respondent. Therefore, despite the fairly distributed types among different regions of Brazil (See Figure 2), we cannot assure N=134 (roughly 9.6% of population) covers the population properly and hence being consider a representative sample[4]. By the same token, as we cannot distinguish the number of different HIS referred by respondents, the survey results may not reflect Brazilian market as a whole.

RESULTS

The majority of respondents were classified as HU type (44.7%). 23.8 % of responses reflects respondents influenced by SBIS' certified HIS. 21.6% declared RBAC implantation, therefore currently NGS1.04 compliant. The rest of the findings are described at the following table. Confidence interval of 95% considered for error-margin (MoE) is applied on current implementation voting extract.

DISCUSSION

Supporting Señor I.C. et al. (2012)[2] previous statement that RBAC is dominant access-control within the health IT industry, that survey shows 29 votes (considering core and full implementations. It is followed by basic access-control matrix based implementations.

Surprisingly, more advanced versions of RBAC are already present in Brazilian available HIS (bottom list options). The general perception is that hybrid or RBAC-based access control currently satisfies industry needs. Hybrid models (from classic models or RBAC variants) seems to be the predictions for the future.

Considering the amount of responses reflecting HIS certified experience, again the certification process seems to lean implementations to use hybrid models for

Table 1 - Survey responses considering current and planned access-control implementation on HIS

Access control	Current implementation and MoE	Currently satisfies industry	Planned implementation			SBIS certified	Confidence level avg %
			<12m	<36m	>36m		
AC matrix basic	19 (14.1% ± 5.8%)	9	2	0	0	2	32.4
DAC (Discretionary AC)	2 (1.5% ± 2%)	2	0	0	0	0	10
MAC (Mandatory AC)	11 (8.2% ±4.6%)	8	0	0	1	5	23.3
Hybrid (above)	11 (8.2% ±4.6%)	10	2	5	1	5	40.9
RBAC (Core)	22 (16.4% ±6.2%)	17	1	4	2	3	53.5
RBAC full	7 (5.2% ±3.7%)	7	1	1	3	4	50.5
Time RBAC	2 (8.2% ±2%)	1	0	0	1	2	13
Context RBAC	4 (3% ±2.8%)	3	0	2	0	2	50.7
Mixed RBAC extensions	18 (13.4% ±5.7%)	15	4	5	1	8	51.1

authorization control.

Considering the amount of respondents self-declared as experts (1-100 grading) the most technically confident respondents were those who vote for RBAC and its extensions.

CONCLUSION

The conducted survey shows HIS current implementations of access-control and fu-ture expectations. According to the obtained answers, most HIS currently implement RBAC. 82.7% report that this access control model meets current industry demand. 23.8% stated that they did not adhere to the model recommended by the SBIS certification manual in version 4. 6.9%, 17.2% and 17.2% of the HIS' developers respondents declared future intention to use this model in the short, medium and long term, respectively. 17.9% stated intention to change to hybrid models with RBAC or extensions.

REFRENCES

1. Stepien B, Khambhammettu H, Adi K, Logrippo L. CatBAC: A generic framework for designing and validating hybrid access control models. Proceedings of the IEEE International Conference on Communications; 2012 Jun 10-15; Ottawa, ON, Canadá. p.6721-6.
2. Señor IC, Fernández—Alemán JL, Lozoya PÁ, Toval A. Access control management in electronic health records: a systematic literature review. Gac Sanit. 2012 Sep-Oct;26(5):463-8.
3. HIMSS Workforce Study. 2017 HIMSS leadership and workforce survey; 2017.
4. Mingyue F, Xicang Z. Research on internet survey errors and control methods. Proceedings of the International Conference on Business Management and Electronic Information; 2011 May 13-15;Guangzhou, China. p. 346-9.