MOKSLAS – LIETUVOS ATEITIS
SCIENCE – FUTURE OF LITHUANIA

ISSN 2029-2341 print / ISSN 2029-2252 online
2013 5(2): 88–91 doi:10.3846/mla.2013.15

Sistemų inžinerija, kompiuterių technologija T 120
Systems Engineering, Computer Technology T 120

Elektronika ir elektrotechnika
Electronics and Electrical Engineering

ONTOLOGIJOS NAUDOJIMAS INFORMACIJOS SAUGUMO REIKALAVIMAMS SUSIETI

Simona Ramanauskaitė[1], Eglė Radvilė[2], Dmitrij Olifer[3]

Vilniaus Gedimino technikos universitetas

El. paštas: [1]mima112it@gmail.com; [2]egle@semus.lt; [3]dmitrij.olifer@gmail.com

Santrauka. Esant daugybei informacijos saugą reglamentuojančių dokumentų, gairių ir standartų, aktualu tarpusavyje susieti juose apibrėžtus saugumo reikalavimus. Skirtinguose saugos dokumentuose aprašyti saugumo reikalavimai gali ne tik sutapti arba papildyti vienas kitą, bet ir prieštarauti vienas kitam. Tai labai apsunkina daugiau negu dviejų informacijos saugą reglamentuojančių dokumentų susiejimą. Vienas būdų susieti daugiau negu du saugą reglamentuojančius dokumentus galėtų būti ontologijos naudojimas. Straipsnyje apžvelgiami šiuo metu pagrindiniai saugą reglamentuojantys standartai, egzistuojančios saugumo ontologijos, išnagrinėta galimybė naudoti ontologiją saugą reglamentuojančių dokumentų reikalavimams susieti ir galimybę tokį susiejimą atvaizduoti grafais.

Reikšminiai žodžiai: ontologija, informacijos saugumo standartai, informacijos saugumo reikalavimai, susiejimas, grafai.

Įvadas

Informacija tapo vienu svarbiausių organizacijų turtų, jos apsauga tampa vienu iš prioritetinių organizacijos uždavinių. Tinkamai įgyvendinti informacijos saugumo reikalavimai gali ne tik užtikrinti organizacijos informacijos apsaugą, bet ir padidinti organizacijos vertę arba suteikti konkurencinį pranašumą. Siekiant užtikrinti minimalų informacijos apsaugos lygį, tam tikrose srityse (bankų, sveikatos apsaugos sektoriuose) buvo priimti standartai (PCI DSS, Sarbaney – Oxley aktas), reglamentuojantys minimalius saugumo reikalavimus, kuriuos turi atitikti organizacijos, veikiančios šiame sektoriuje.

Informacijos saugumo reikalavimų pasirinkimas ir įgyvendinimas – gana paprastas uždavinys tol, kol organizacija orientuojasi į vieną iš daugelio informacijos saugą reglamentuojančių dokumentų. Procesas tampa daug sudėtingesnis, jei įmonė siekia atitikti daugiau negu vieną saugos standartą. Pavyzdžiui, akredituotis pagal ISO 27001 tarptautinį standartą ir PCI DSS tarptautinį standartą. Tokiu atveju sudėtinga suderinti skirtingų standartų saugos reikalavimus, nes jie gali ne tik sutapti arba papildyti vienas kitą, bet ir prieštarauti vienas kitam.

Dar vienas iššūkis, su kuriuo susiduria informacinių sistemų auditoriai, informacijos saugos vadybininkai ir informacinių sistemų kūrėjai, siekiantys sukurti, modifikuoti arba įvertinti jau egzistuojančią informacijos saugos valdymo sistemą, yra specifinių žinių ir patirties trūkumas (Sikora *et al.* 2012). Tai tampa akivaizdžiau matoma padidėjus informacijos saugos įdiegimo poreikiui ir atsižvelgiant į sparčiai didėjančią ir nuolat besikeičiančią informacinių technologijų aplinką.

Išvardytas problemas ir iššūkius gali padėti išspręsti ontologija. Ontologijos yra efektyvios sprendžiant skirtingų žinių tipų atvaizdavimo ir tarpusavio susiejimo uždavinius (Gruber 1995). Per paskutinį dešimtmetį buvo pasiūlyta daug skirtingų saugumo ontologijų ir kiekvienais metais atsiranda naujų saugumo ontologijų.

Šiame straipsnyje išnagrinėjami šiuo metu populiariausi informacijos saugą reglamentuojantys dokumentai, tokie kaip informacijos saugos standartai ir geriausiosios praktikos, apžvelgiami saugos ontologijų tipai, pasirenkamos ontologijos, kurios ateityje galėtų būti pritaikytos informacijos susiejimo uždaviniams spręsti. Nagrinėjama galimybė taikyti pasirinktas ontologijas populiariausiems informacijos saugą reglamentuojantiems dokumentų reikalavimams susieti.

Tyrimo metodologija

Tyrimo metu buvo išnagrinėti informacijos saugą reglamentuojantys dokumentai ir juose apibrėžiami reikalavimai, straipsniai apie egzistuojančias informacijos saugos ontologijas ir jų taikymo sritis. Rengiant šį straipsnį buvo atliktas paieškomasis tyrimas, t. y. siekiant suformuoti tikslią problemos struktūrą ir geriau suvokti aplinką, kurioje keliama problema, buvo atlikta literatūros šaltinių analizė (Cooper, Schundler 1998).

Saugą reglamentuojančių dokumentų apžvalga

Yra aibė informacijos saugą reglamentuojančių dokumentų, kuriuos galima klasifikuoti skirtingais aspektais. Galima išskirti tokius pagrindinius klasifikatorius:

- **Taikymo sritys.** Vieni taikomi tik valstybiniame sektoriuje (FISMA, angl. *Federal Information Security Management Act*), kiti – tik sveikatos apsaugos (HIPAA, angl. *Health Insurance Portability and Accountability Act*) arba bankininkystės sektoriuje (SOX, angl. *Sarbanes-Oxley Act Committee Of Sponsoring*).
- **Taikymo būtinybė.** Vieni yra privalomi (PCI DSS, angl. *Payment Card Industry Data Security Standard*), kiti rekomendacinio pobūdžio (angl. *Standard of Good Practice for Information Security*).
- **Dokumento tipas.** Vieni parengti kaip tarptautiniai standartai (ISO 27001 / ISO 27002), kiti – kaip geriausių praktikų rinkinys (angl. *Generally Accepted information Security Practices*).

Šiame straipsnyje nagrinėjami trys saugą reglamentuojantys dokumentai. Du iš jų šiuo metu yra labiausiai paplitę saugos standartai pasaulyje (ISO 27001 ir PCI DSS), trečias saugą reglamentuojantis dokumentas yra aktas, reglamentuojantis informacinių sistemų saugos reikalavimus.

ISO 27001 – tarptautinis standartas, nustatantis reikalavimus, taikomus informacijos saugai valdyti. Tai vienas iš nedaugelio standartų, leidžiančių sertifikavimą. Pagrindinis šio standarto tikslas – sukurti ir palaikyti informacijos saugos valdymo sistemą (angl. *Information Security management System*). Standartas nustato pagrindinius tikslus, kurie turi būti nuolat stebimi, norint užtikrinti priimtiną informacijos saugos lygį. Kuriant informacijos saugos valdymo sistemą naudojamas PDCA (angl. *Plan – Do – Check – Act*) modelis, leidžiantis užtikrinti nuolatinį kuriamos arba egzistuojančios sistemos tobulinimą ir suderinamumą su organizacijos tikslais ir poreikiais. Šis standartas glaudžiai susijęs su kitu tarptautiniu standartu ISO 27002, kuriame nuodugniai aprašomos informacijos saugos reikalavimų įgyvendinimo gairės.

PCI DSS – plačiai priimtas politikų ir procedūrų rinkinys, sukurtas kreditinių, debetinių ir kitų kortelių transakcijų saugumui, taip pat ir kortelių savininkų asmeninės informacijos apsaugai užtikrinti. Vadovaujantis šiuo standartu, turi būti apsaugota tokia informacija:

- Pagrindinis sąskaitos numeris (PAN, angl. *Primary Account Number*).
- Kortelės savininko vardas (angl. *Cardholder Name*).
- Paslaugos kodas (angl. *Service Code*).
- Galiojimo data (angl. *Expiration Date*).

Šis standartas buvo sukurtas tokių kompanijų, kaip „Visa“, „MasterCard“, „Discover“ ir „American Express“ iniciatyva ir *de facto* tapo privalomu mokėjimo kortelių sektoriuje.

Šis standartas nustato šešias sritis ir dvylika kontrolės objektų, taip pat detalius techninius reikalavimus šiems kontrolės objektams įgyvendinti. Organizacijos gali būti sertifikuojamos vadovaujantis šiuo standartu, ir tik gavus sertifikavimą jiems leidžiama vykdyti veiklą su mokėjimo kortelėmis.

FISMA – šis aktas yra dalis Jungtinių Amerikos Valstijų e. valdžios akto, kuris reikalauja, kad JAV federalinės organizacijos sukurtų ir įgyvendintų procesą, leidžiantį užtikrinti informacijos saugą jų eksploatuojamose informacinėse sistemose. Pagrindiniai šio akto reikalavimai:

- Užtikrinti, kad saugumas būtų tęstinis procesas.
- Apibrėžti paskirtų asmenų atsakingumo ribas.
- Periodiškai tikrinti saugumo kriterijus jų sistemose.

Nors pačiame akte saugos reikalavimai apibrėžti abstrakčiai, Nacionalinis standartų ir technologijų institutas (NIST, angl. *National Institute of Standards and Technology*) sukūrė aibę papildomų dokumentų, reglamentuojančių informacijos saugos reikalavimus skirtingose srityse.

Organizacijos pačios sprendžia, kokį informacijos saugą reglamentuojantį dokumentą pasirinkti ir kokius saugos reikalavimus taikyti. Tai priklauso nuo įmonės tikslų ir šį procesą įgyvendinančio personalo kompetencijos.

Kai informacijos saugai užtikrinti naudojami du ir daugiau standartų, dažnai taikomi tokie metodai:

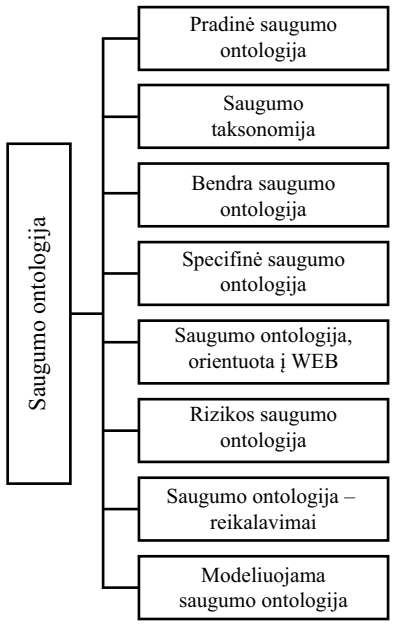
- *Sintaksinė analizė.* Lyginama kelių standartų terminija. Tačiau to nepakanka, jei modeliai nėra struktūriškai ir semantiškai suderinami.
- *Susiejimas.* Randami atitikmenys ir susiejami tarpusavyje, nurodant tapačius reikalavimus tarp standartų.
- *Sujungimas.* Keli standartai sujungiami į vieną bendrą schemą.

Mus labiausiai domino susiejimo metodas.

Saugumo ontologijų apžvalga

Nagrinėjant saugumo ontologijas Souag *et al.* (2012) išskiriamos aštuonios skirtingos ontologijų šeimos (1 pav.):

- *Pradinė saugumo ontologija* – žinių bazės ir informacinių sistemų valdymo sujungimas sistemos kūrimo pradžioje.
- *Saugumo taksonomija* – saugumo koncepcijų taksonomijos metodas, leidžiantis dalytis saugumo žiniomis.



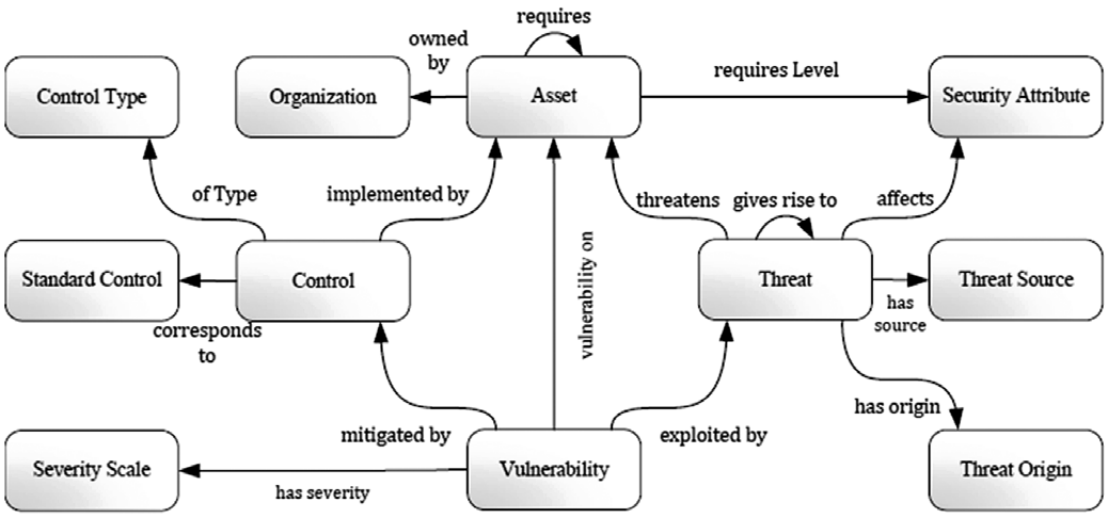
1 pav. Saugumo ontologijos šeimų klasifikacija
Fig. 1. Classification of security ontologies

– *Bendra saugumo ontologija* – ontologija, apimanti pagrindinius saugumo aspektus. Ji gali ne tik aprašyti bendrą koncepciją, bet ir nustatyti bendrą srities žodyną. Fenz, Skelhart (2009) pasiūlė ontologiją, kuri apibrėždavo ir organizacijos infrastruktūrą.
– *Specifinė saugumo ontologija* – kategorija ontologijų, kurios apibrėžia specifines sritis, tokias kaip kompiuterinės atakos.
– *Saugumo ontologija, orientuota į WEB* – ontologijos, sukurtos nuorodoms į agentus ir saityno paslaugoms (*web services*) aprašyti. Vėliau buvo sukurta saityno paslaugų saugumo atakų ontologija.
– *Rizikos saugumo ontologija* – skirta rizikos įvertinimui aprašyti. Fenz, Skelhart (2007) pasiūlė saugumo ontologijos šabloną, sudarytą iš keturių dalių: saugumo taksonomijos, rizikos analizės metodologijos, IT infrastruktūros dalies ir simuliacijos, leidžiančios tikrinti skirtingus scenarijus.
– *Saugumo ontologija – reikalavimai* – ontologijos glaudžiai susijusios su informacijos saugos reikalavimų apibrėžimais.
– *Modeliuojama saugumo ontologija* – pateikia metamodelius.

Iš pateiktų ontologijos šeimų labiausiai mūsų deklaruojamiems uždaviniams (informacijos saugos dokumentų reikalavimų susiejimas) spręsti tinka bendra saugumo ontologijos šeima, nes būtent šios šeimos ontologijos apima visus pagrindinius aspektus (saugumo tikslai, turtas, pažeidžiamumai, grėsmės, rizikos mažinimo priemonės ir organizacijos aspektai). Vienas iš tokių bendrų ontologijų pavyzdžių galėtų būti Fenz pasiūlyta ontologija (2 pav.).

Saugumo ontologija susiejant saugumo reikalavimus

Visi išnagrinėtų informacijos saugą reglamentuojančių dokumentų reikalavimai gali būti priskirti prie vienos iš keturių pagrindinių grupių, aprašytų Fenz saugumo ontologijoje (turtas, grėsmė, pažeidžiamumas, kontrolinis tikslas). Pavyzdžiui, dalis informacijos saugą reglamentuojančių dokumentų reikalavimų aprašo, kaip turi būti apsaugoti kritiniai organizacijos infrastruktūros mazgai, elektroninė ir kita informacija arba jos nešėjai. Visi tokie reikalavimai pateks į Fenz saugos ontologijos objektą „turtas“.



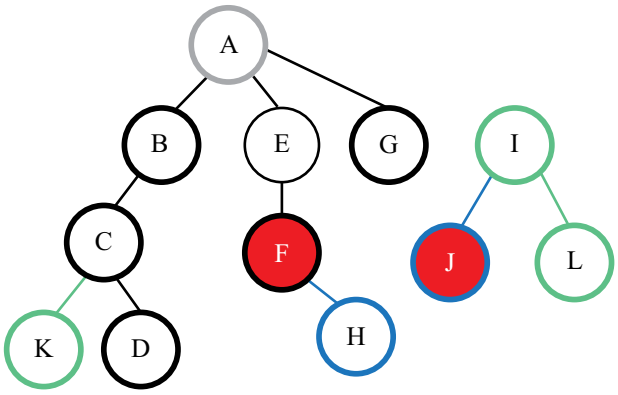
2 pav. Fenz saugumo ontologija
Fig. 2. Fenz security ontology

Toks požiūris, pritaikius tinkamą „mastelį“, leidžia susieti skirtingus informacijos saugą reglamentuojančius dokumentus ir jų reikalavimus. Tokio susiejimo rezultatai vėliau gali būti grafiškai pateikiami naudojant grafus.

Yra tikimybė, kad remiantis ontologija susieti informacijos saugą reglamentuojantys dokumentai bus sunkiai skaitomi, nes turės didelį kiekį informacijos. Grafų pritaikymas šiame susiejimo etape gali leisti palengvinti susiejimo informacijos atvaizdavimą ir padidinti informacijos analizės efektyvumą.

Taikant grafus, saugą reglamentuojančio dokumento klasės (kontrolės objektai, saugos reikalavimai) vaizduojamos kaip mazgai, o ryšiai tarp jų vaizduojami briaunomis (3 pav.). Dokumentai bus susiejami taip:

- Kito saugą reglamentuojančio dokumento mazgai vaizduojami kita spalva.
- Sutampantys mazgai vaizduojami storėjančia linija (linijos storis priklauso nuo sutapimų skirtinguose dokumentuose skaičiaus).
- Prieštaringi reikalavimai vaizduojami skirtingu fonu.



3 pav. Saugos reikalavimų susiejimas grafais

Fig. 3. Garph use for security requirements mapping

Taikomi grafai leistų peržiūrėti susietą informaciją skirtingais aspektais, efektyviai analizuoti skirtingų saugą reglamentuojančių dokumentų skirtumus ir panašumus. Analogiškas požiūris gali būti pritaikytas vertinant organizacijos atitiktį vienam arba kitam saugą reglamentuojančiam dokumentui.

Išvados

1. Atliktas tyrimas parodė, kad ontologijos gali būti naudojamos saugą reglamentuojančių dokumentų ir jų reikalavimų tarpusavio susiejimo procese.
2. Atsižvelgiant į informacijos saugos reglamentuojančių dokumentų reikalavimų aspektus, geriausia susiejimui naudoti bendros saugumo šeimos ontologijas. Pavyzdžiui, Fenz saugumo ontologiją.
3. Skirtingų saugą reglamentuojančių dokumentų susiejimo vaizdiniam pateikimui gali būti naudojami grafai.

Padėka

Šiame straipsnyje aprašomos veiklos, atliekamos vykdant Europos Sąjungos ir Lietuvos Respublikos Vyriausybės finansuojamą projektą VP1-3.1-ŠMM-08-K-01-012 „Virtualizavimo, vizualizavimo ir saugos e. paslaugų technologijų kūrimas ir tyrimai“.

Literatūra

Cooper, D.; Schindler, P. 1998. *Business Research Methods*.

Ekelhart, A.; Fenz, S.; Klemen, M.; Weippl, E. 2007. *Security Ontologies: Improving Quantitative Risk Analysis* (HICSS‘07).

Fenz, S.; Ekelhart, A. 2009. Formalizing information security knowledge, *ASIACCS’09*, 183–194. http://dx.doi.org/10.1145/1533057.1533084

Gruber, T. R. 1995. Toward principles for the design of ontologies used for knowledge sharing, *International Journal Human-Computer Studies* 43(5–6): 907–928. http://dx.doi.org/10.1006/ijhc.1995.1081

Sikora, E., Tenbergen, B., Pohl, K. 2012. *Industry Needs and Research Directions in Requirements Engineering for Embedded Systems*.

Souag, A.; Salinesi, C.; Wattiau, I. 2012. *Ontologies for Security Requirements: A Literature Survey and Classification*.

USE OF ONTOLOGIES IN MAPPING OF INFORMATION SECURITY REQUIREMENTS

S. Ramanauskaite, E. Radvile, D. Olifer

Abstract

A large amount of different security documents, standards, guidelines and best practices requires to ensure mapping between different security requirements. As the result of mapping, security requirements of different standards can coincide or require to be amended or harmonised. This is the reason why it is so difficult to map more than two different security documents. Ontologies can be used to solve this issue. The article offers a review of different security documents and ontology types as well as investigates possible use of ontologies for mapping of security standards.

Keywords: ontology, information security standard, information security requirements, mapping, graph.