VILNIAUS UNIVERSITETAS
DUOMENŲ MOKSLO IR SKAITMENINIŲ TECHNOLOGIJŲ INSTITUTAS
IŠMANIŲJŲ TECHNOLOGIJŲ TYRIMŲ GRUPĖ

Raimundas Savukynas

MULTIMODALINIO DAIKTŲ INTERNETO OBJEKTŲ IDENTIFIKAVIMO IR AUTENTIFIKAVIMO METODO TYRIMAS IR TOBULINIMAS

Doktorantūros metinė ataskaita už 2018 – 2019 m.
Doktorantūros laikotarpis 2016 – 2020 m.

Informatikos inžinerijos studijų programa
Informatikos inžinerijos mokslo kryptis (07T)

Darbo vadovas: dr. Virginijus Marcinkevičius
Darbo konsultantas: prof. dr. Albertas Čaplinskas

Vilnius, 2019

TYRIMAS

Tyrimo objektas:

- išmaniosios aplinkos daiktų integracijos metodai taikomi daiktų interneto objektų identifikavimui ir autentifikavimui.

Tyrimo tikslas:

- sukurti heterogeniškų daiktų interneto objektų decentralizuotą identifikavimo ir autentifikavimo metodą, skirtą transporto išmaniosioms aplinkoms.

Tyrimo uždaviniai:

- apžvelgti daiktų interneto objektų identifikavimo ir autentifikavimo metodus, kurie leistų susieti vienas nuo kito nutolusius objektus ir paslaugas;
- sukurti daiktų interneto objektų decentralizuotą identifikavimo ir autentifikavimo metodą, skirtą automobilių transporto išmaniosioms aplinkoms;
- išanalizuoti sukurto daiktų interneto objektų identifikavimo ir autentifikavimo metodo efektyvumą transporto išmaniųjų aplinkų simuliacijoje;
- atlikti daiktų interneto objektų identifikavimo ir autentifikavimo metodo eksperimentinį tyrimą.

Tyrimo metodika:

- kokybinė analizė, lyginamoji analizė, mokslinė analizė, statistinė analizė, klasifikavimas ir apibendrinimas.

TYRIMAS (2)

Planuojami rezultatai:

- Empiriniai tyrimai:
  - ✓ atlikta daiktų interneto objektų saugumo rizikų, grėsmių ir apsaugos priemonių sisteminė mokslinės literatūros apžvalga;
  - ✓ sukurtas daiktų interneto objektų identifikavimo ir autentifikavimo metodas transporto priemonių valdymo sistemų saugai;
  - ✓ atliktas sukurto metodo eksperimentinis tyrimas analizuojant jo efektyvumą simuliacijoje ir pasiūlytos apsaugos priemonės.

ATASKAITINIŲ METŲ DARBO PLANAS

2018 - 2019 m. m. darbo planas:

- Atlikti empirinį tyrimą:
  - ✓ palyginti esamus daiktų interneto identifikavimo ir autentifikavimo metodus;
  - ✓ patobulinti daiktų interneto objektų identifikavimo ir autentifikavimo metodą;
  - ✓ išanalizuoti patobulinto metodo efektyvumą simuliacijoje ir realioje aplinkoje.
- Dalyvauti tarptautinėje mokslinėje konferencijoje.
- Parengti mokslinę publikaciją recenzuojamame periodiniame leidinyje.

ATASKAITINIŲ METŲ ATLIKTI DARBAI

2018 - 2019 m. m. atlikti darbai:

- Išlaikyti dalykų egzaminai:
  1. Žiniomis grindžiami metodai ir sistemos belaidžių technologijų taikymuose. Komisijos sudėtis: prof. dr. Dalė Dzemydienė (pirmininkė), prof. dr. Albertas Čaplinskas, prof. dr. Saulius Gudas. Egzamino laikymo data 2017 m. birželio 5 d. **Įvertinimas 9 (labai gerai)**.
  2. Informatikos ir informatikos inžinerijos tyrimo metodai ir metodika. Komisijos sudėtis: prof. dr. Albertas Čaplinskas (pirmininkas), prof. dr. Saulius Gudas, doc. dr. Audronė Lupeikienė. Egzamino laikymo data 2017 m. birželio 16 d. **Įvertinimas 8 (gerai).**
  3. Kompiuterinės mokymo technologijos. Komisijos sudėtis: prof. dr. Valentina Dagienė (pirmininkė), dr. Tatjana Jevsikova, dr. Anita Juškevičienė. Egzamino laikymo data 2017 m. rugpjūčio 23 d. **Įvertinimas 10 (puikiai)**.
  4. Informatikos inžinerijos matematiniai metodai. Komisijos sudėtis: dr. Gintautas Tamulevičius (pirmininkas), dr. Jolita Bernatavičienė, dr. Gražina Korvel. Egzamino laikymo data 2018 m. rugsėjo 28 d. **Įvertinimas 8 (gerai)**.

ATASKAITINIŲ METŲ ATLIKTI DARBAI (2)

2018 - 2019 m. m. atlikti darbai:

- Atlikti moksliniai tyrimai:
  - ✓ atliktas empirinis tyrimas.
- Dalyvauta vasaros mokyklose:
  - ✓ Cyber Security Summer School Blockchain: „Applications and Security", University of Tartu, Voore, Estonia, July 1-5, 2019.
- Dalyvauta mokslinėse konferencijose:
  1. Blockchain Technology for Security and Privacy in Internet of Things: *10th International Workshop on Data Analysis Methods for Software Systems (DAMSS)*, Druskininkai, November 29-December 1, 2018.
  2. Application of the Reference Model for Security Risk Management in the Internet of Things Systems: *9th Doctoral Consortium on Informatics Education and Educational Software Engineering Research*, Druskininkai, November 30-December 5, 2018.
  3. Security Means for Identification and Access to Objects in the Internet of Things Environment: *24th International Conference on Information Technology (IVUS 2019)*, Kaunas, April 25, 2019.

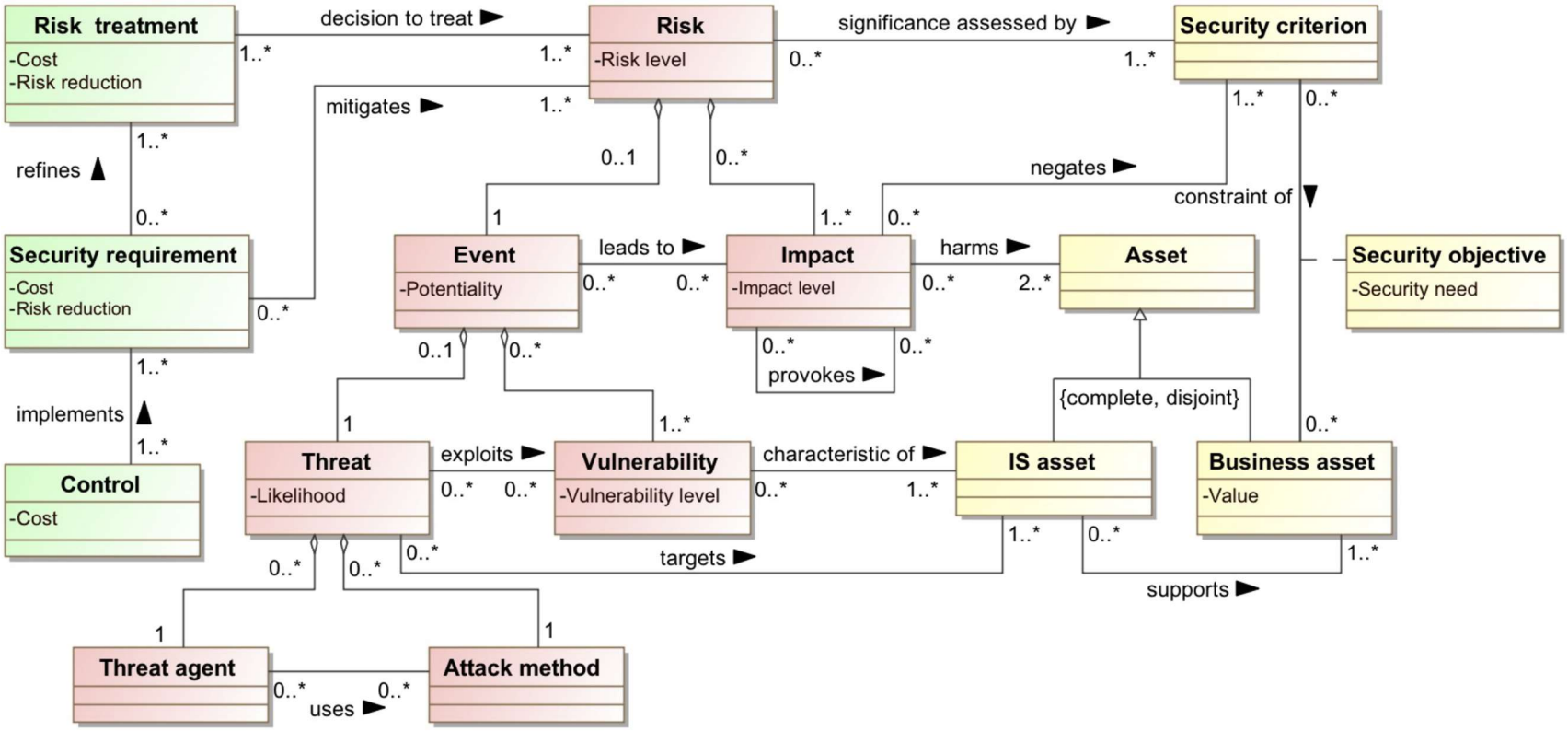
ATASKAITINIŲ METŲ ATLIKTI DARBAI (3)

2018 - 2019 m. atlikti darbai:

- Parengtos mokslinės publikacijos:

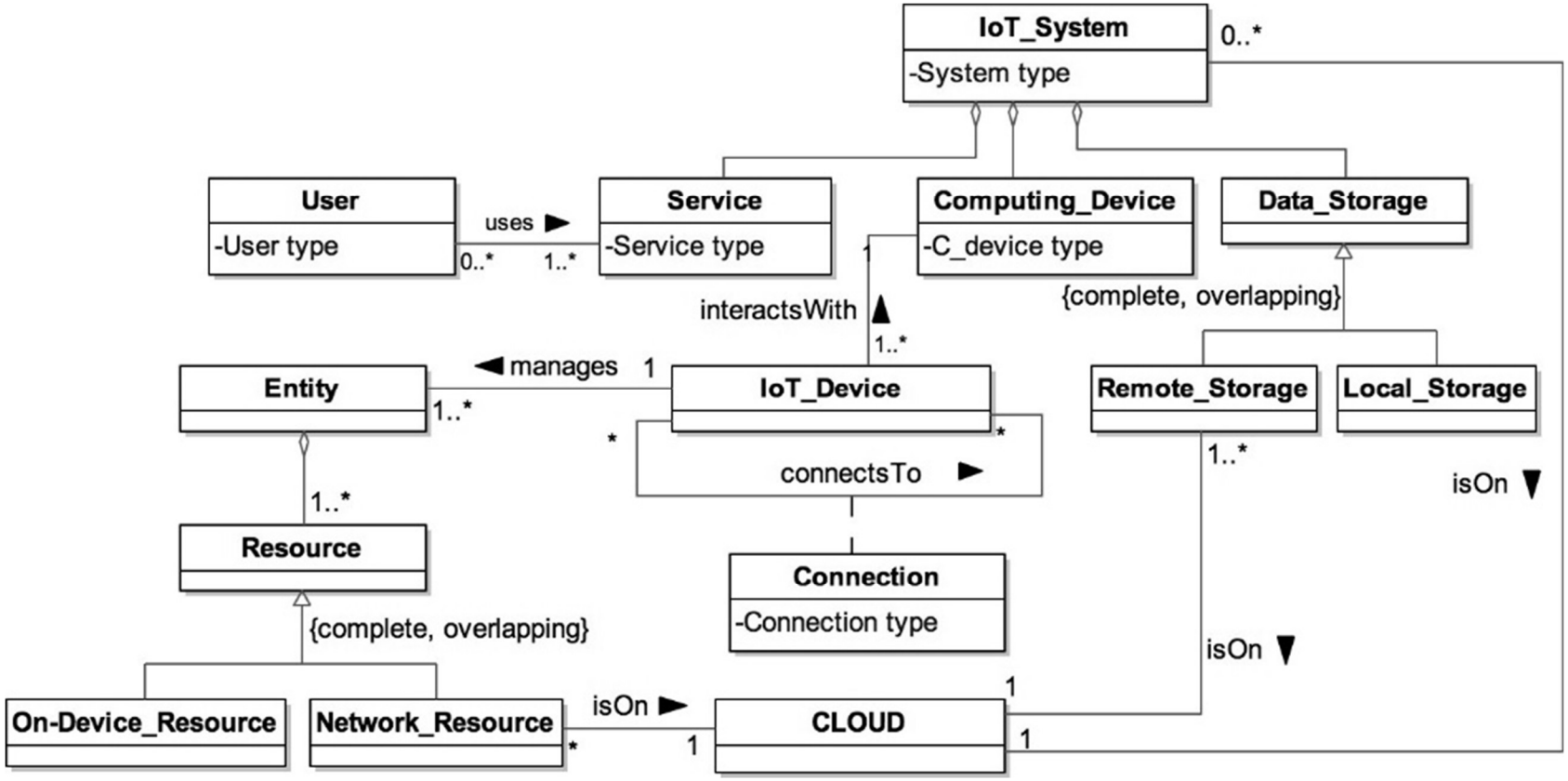
1. Savukynas, R.; Dzemydienė, V. (2018). Security Means in Multilayered Architecture of Internet of Things for Secure Communication and Data Transmission, in *Proceedings of Baltic DB&IS 2018 Conference Forum and Doctoral Consortium co-located with the 13th International Baltic Conference on Databases and Information Systems (Baltic DB&IS 2018)*, Trakai, Lithuania, July 1-4, 127-134. ISSN 1613-0073.
2. Savukynas, R.; Marcinkevičius V. (2018). Blockchain Technology for Security and Privacy in Internet of Things, in *Proceedings of 10th International Workshop on Data Analysis Methods for Software Systems (DAMSS)*, Druskininkai, Lithuania, November 29-December 1, 74-75. ISBN 978-609-07-0043-3. DOI: 10.15388/DAMSS.2018.1.
3. Matulevičius, R.; Savukynas, R. (2019). Application of the Reference Model for Security Risk Management in the Internet of Things Systems. In: Lupeikienė, A., Vasilecas, O., Dzemyda, G. (Ed). *Databases and Information Systems X*. IOS Press (Frontiers in Artificial Intelligence and Applications), 65-78. ISBN 978-1-61499-940-9. DOI:10.3233/978-1-61499-941-6-65.

EMPIRINIS TYRIMAS



1 pav. Informacinių sistemų saugumo rizikos valdymo modelis, adaptuota (Dubois et al., 2010)

EMPIRINIS TYRIMAS (2)



2 pav. Daiktų interneto architektūros modelis (Vasilomanolakis et al., 2015)

EMPIRINIS TYRIMAS (3)

Pažeidžiamumas yra daiktų interneto silpnoji vieta, kuri atsirado projektavimo eigoje arba diegimo metu ir leidžia įsibrovėliui pakenkti programoms bei vartotojams (Shapaval et al., 2018). Šių pažeidžiamumų klasės:

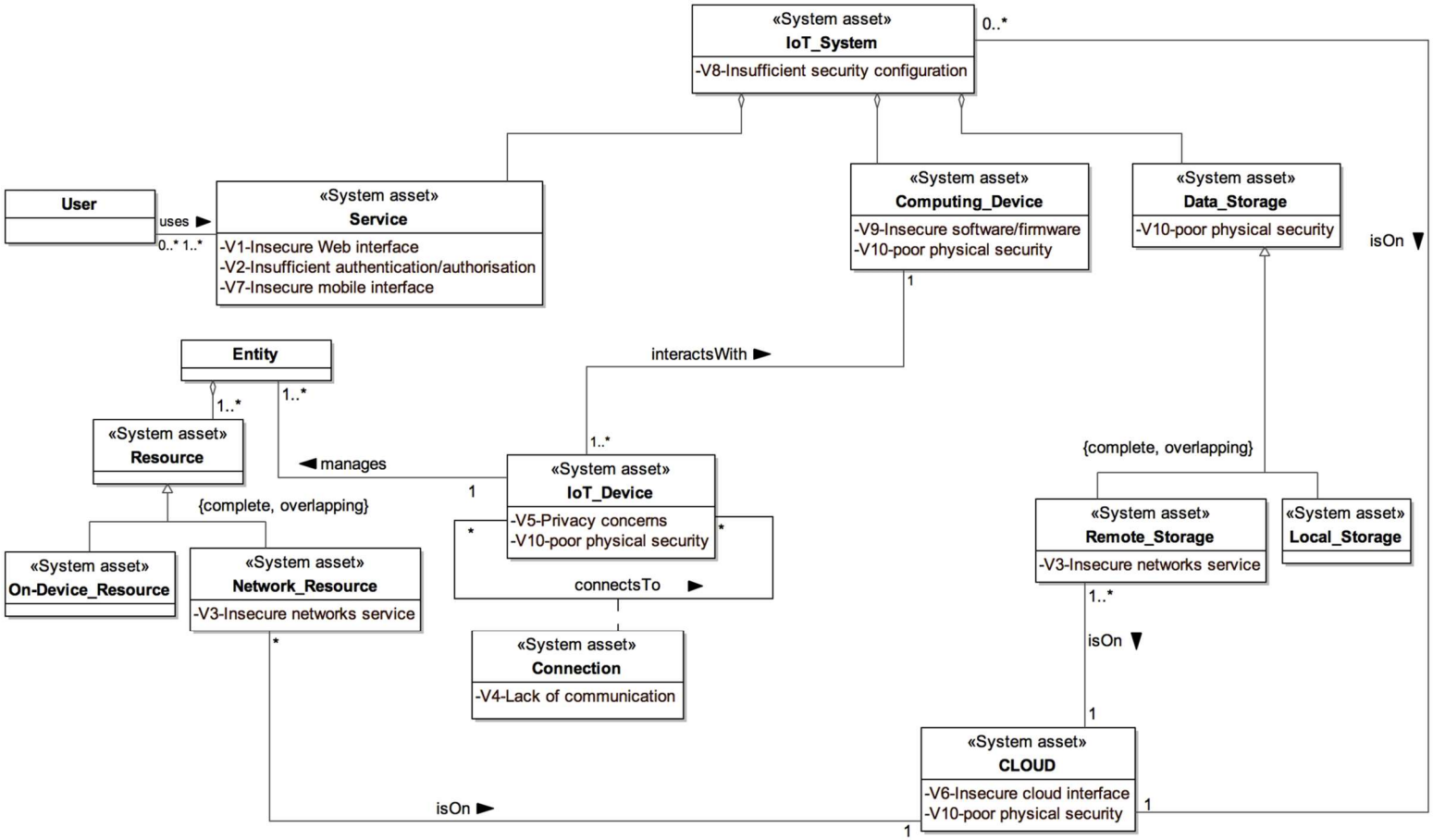
- V#1: Nesaugi žiniatinklio sąsaja.
- V#2: Nesaugus autentifikavimas ar autorizavimas.
- V#3: Nesaugios tinklo paslaugos.
- V#4: Trūksta komunikacijos šifravimo.
- V#5: Nepakankamas konfidencialumas.
- V#6: Nesaugi debesies sąsaja.
- V#7: Nesaugi mobilioji sąsaja.
- V#8: Nepakankamas saugos konfigūravimas.
- V#9: Nesaugi programinė ar aparatinė įranga.
- V#10: Prastas fizinis saugumas.

EMPIRINIS TYRIMAS (4)

Saugos reikalavimai, kurie apibrėžia sąlygas norint sumažinti daiktų interneto pažeidžiamumus yra sugrupuoti (Qian et al., 2018):

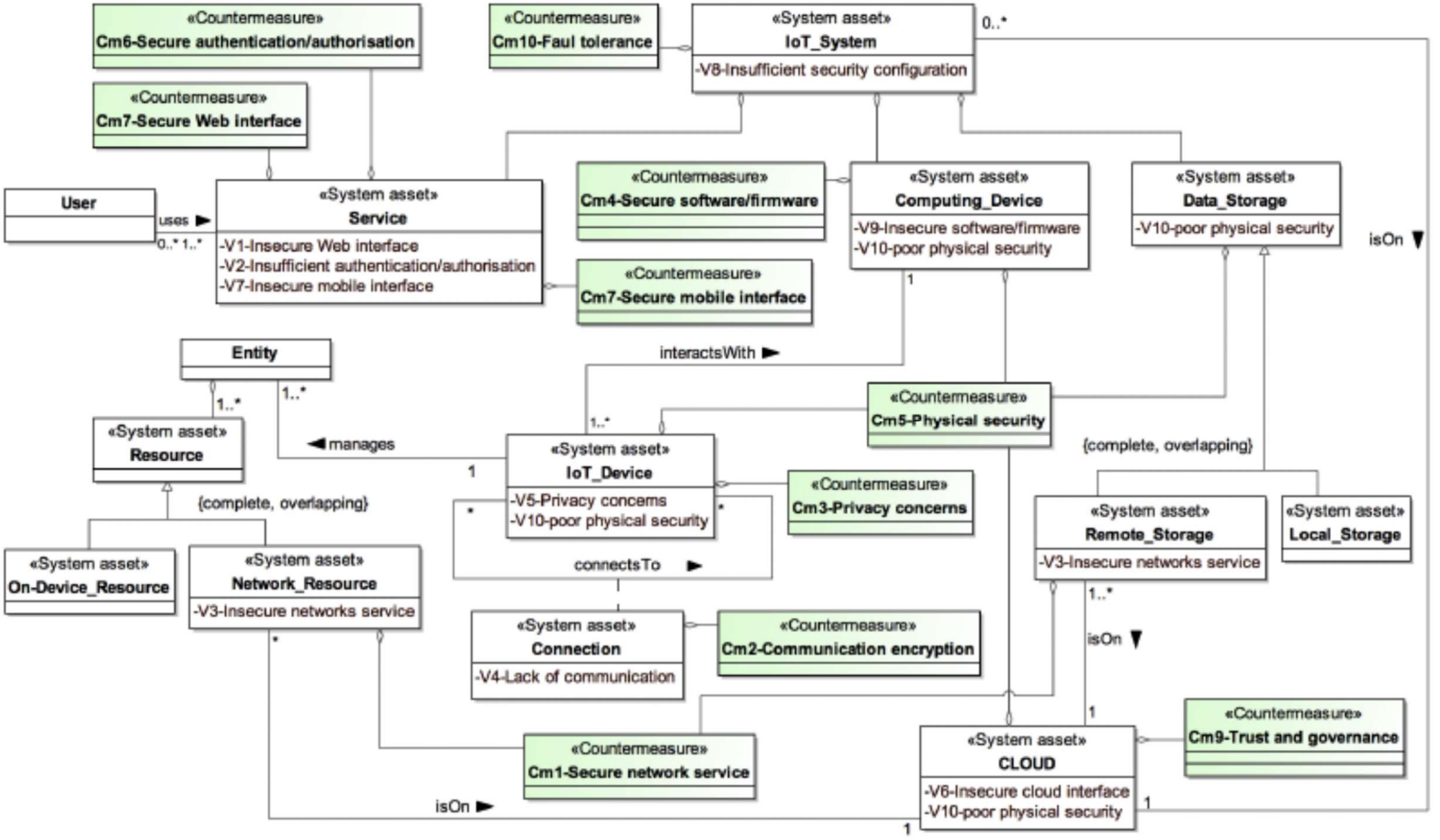
1. Protokolo ir tinklo sauga (Cm#1: saugios tinklo paslaugos ir Cm#2: ryšio šifravimas).
2. Duomenys ir privatumas (Cm#3: privatumo užtikrinimas, Cm#4: saugi programinė ar aparatinė įranga ir Cm#5: fizinis saugumas).
3. Tapatybės valdymas (i.e., Cm#6: saugus autentifikavimas ar autorizavimas, Cm#7: saugi interneto sąsaja ir Cm#8: saugi mobilioji sąsaja).
4. Patikimumas ir valdymas (Cm#9: patikimumas ir valdymas).
5. Gedimų tolerancija (Cm#10: gedimų tolerancija).

EMPIRINIS TYRIMAS (5)



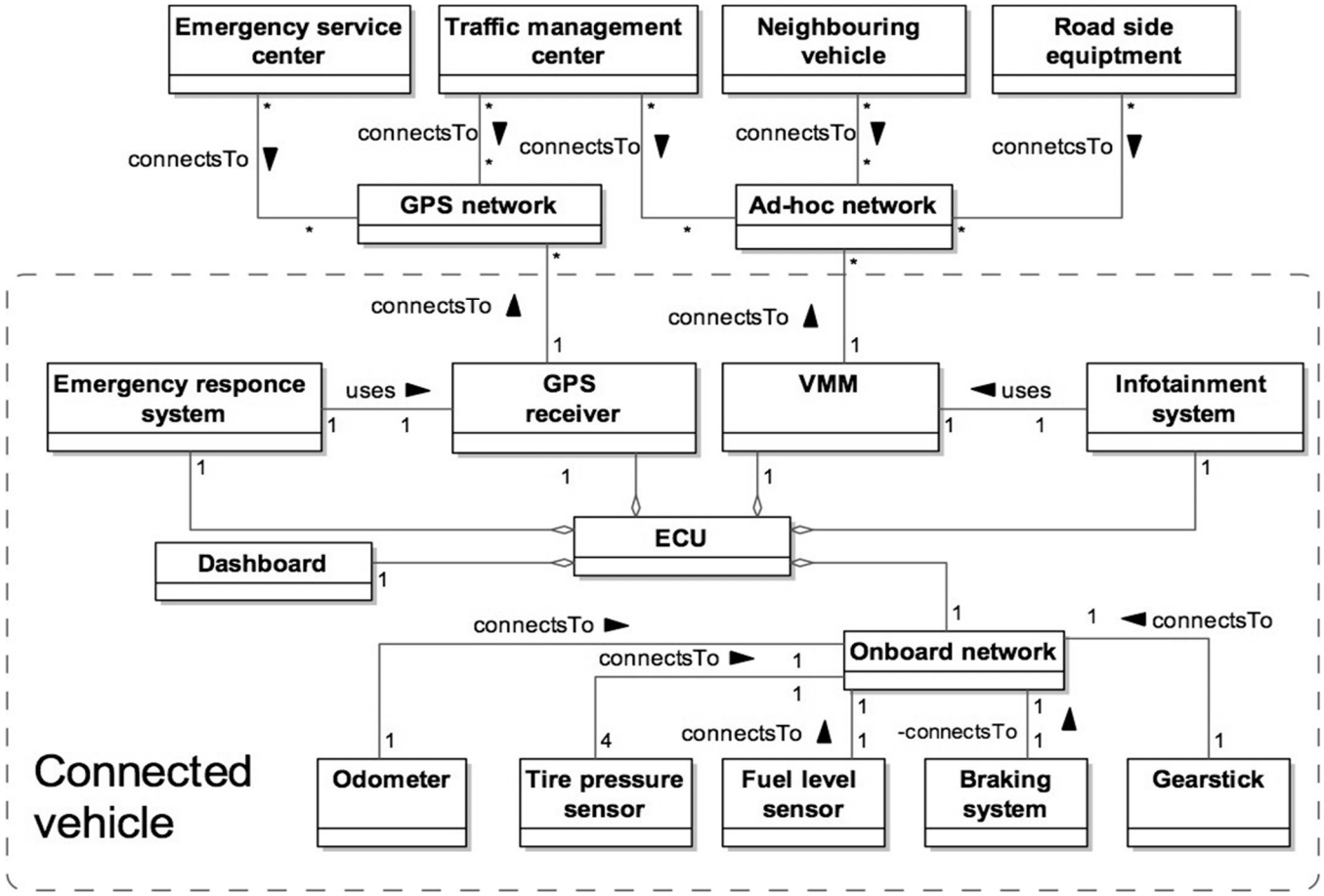
3 pav. Daiktų interneto pažeidžiamumų modelis (Qian et al., 2018)

EMPIRINIS TYRIMAS (6)



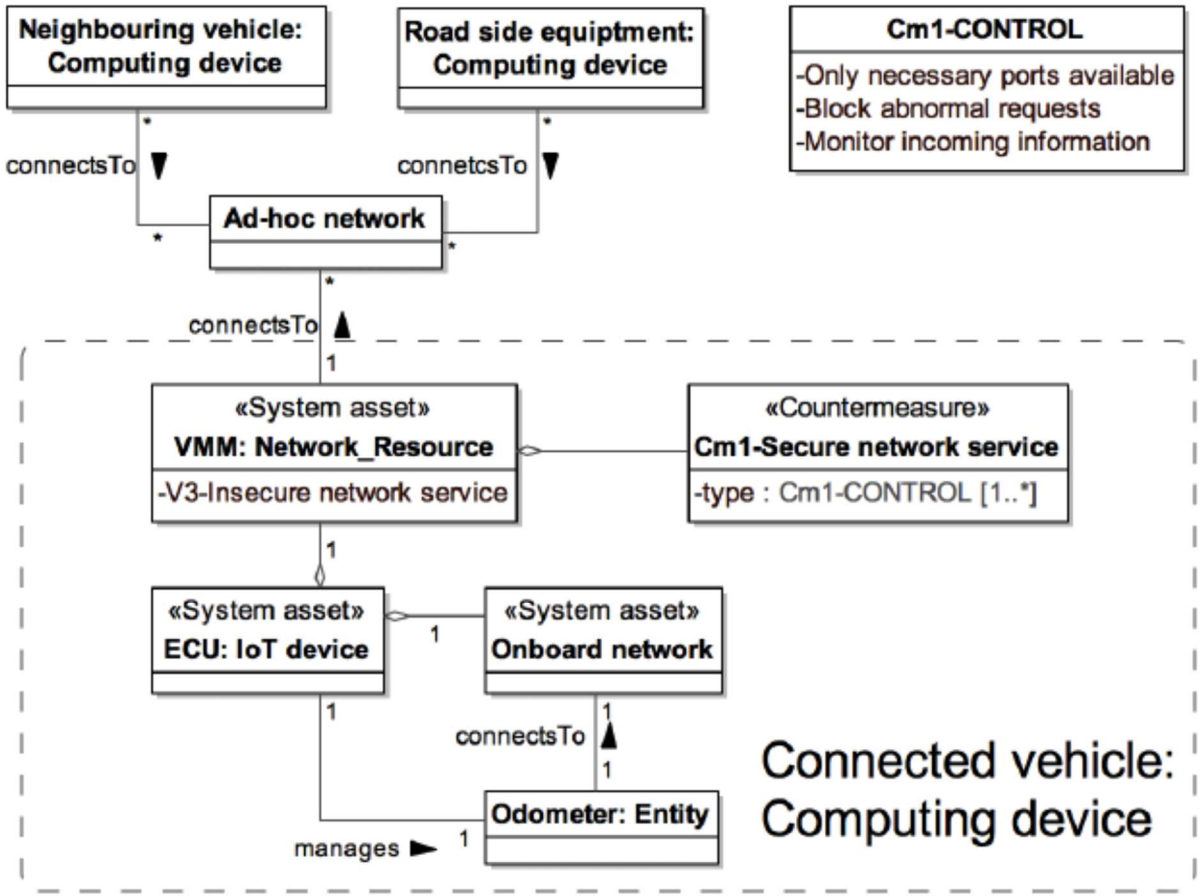
4 pav. Daiktų interneto informacinių sistemų saugumo rizikos valdymo modelis

EMPIRINIS TYRIMAS (7)



5 pav. Sąveikaujančio automobilio modelis (Othmane et al., 2013)

EMPIRINIS TYRIMAS (8)



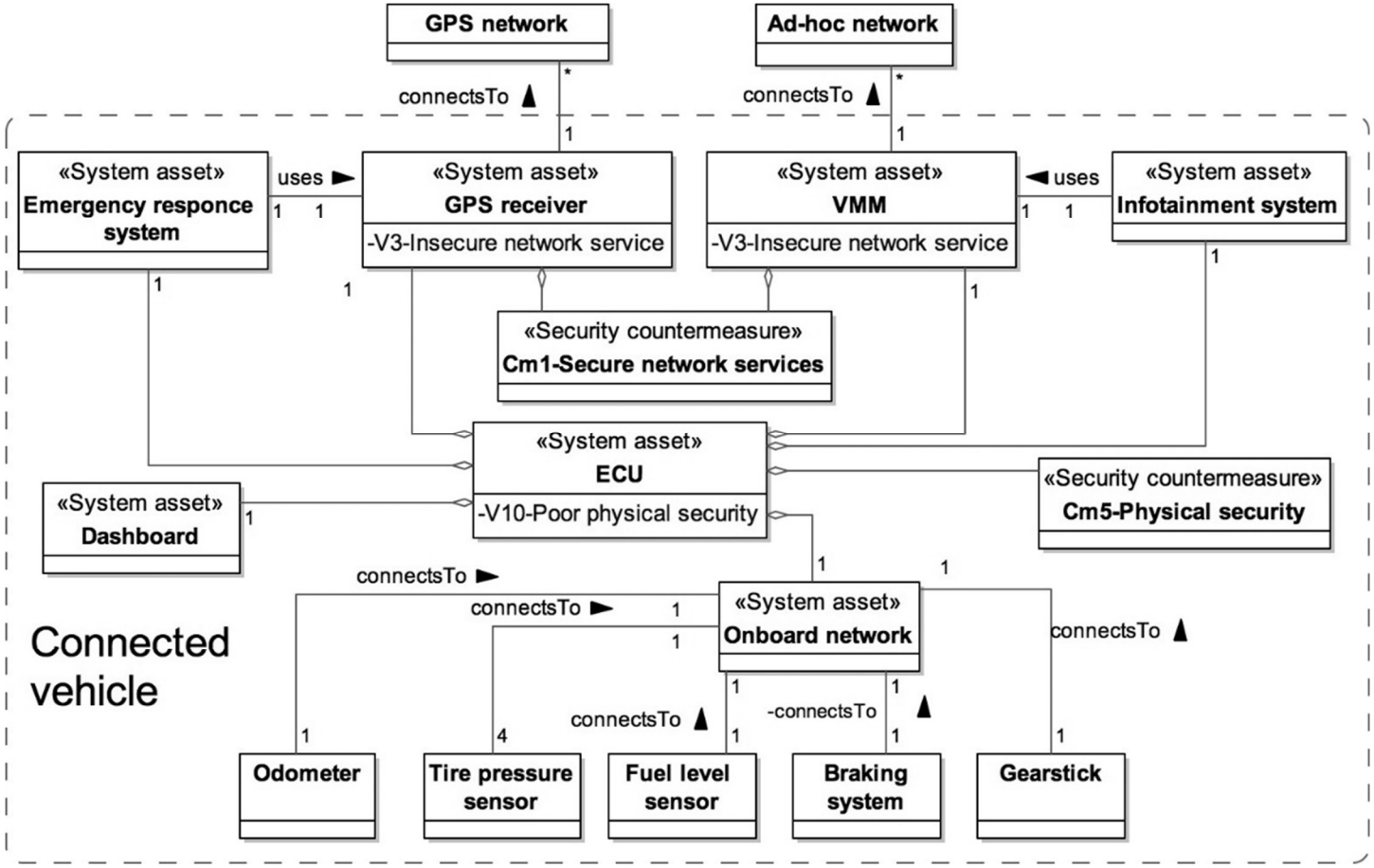
6 pav. Nesaugus tinklo ryšys sąveikaujančioje transporto priemonėje (Othmane et al., 2013)

EMPIRINIS TYRIMAS (9)

1 lentelė. Pažeidžiamumai sąveikaujančioje transporto priemonėje, adaptuota (Othmane et al., 2013)

Sąvoka	Pažeidžiamumas 1	Pažeidžiamumas 2
Pavojus	Atakuojantysis prijungia užkrėstą elektroninį valdymo bloką prie transporto priemonės.	Atakuojantysis sudaro ryšį su transporto priemone (arba kelyje esančia įranga) ir keičia jos sistemos rodmenis.
Poveikis	Keičiasi greičio rodmenys. Sudaromi klaidingi maršrutai.	Keičiasi greičio rodmenys. Sudaromi klaidingi maršrutai.
Pažeidžiamumas	Transporto priemonės USB prievadą galima fiziškai pasiekti.	Silpnas informacijos perdavimas iš transporto priemonės ryšio įrenginio.
Grėsmė	Atakuojantysis sukuria kenkėjišką valdymo bloką ir fiziškai jį prijungia prie transporto priemonės.	Atakuojantysis gali naudoti transporto priemonę (arba kelio įrangą), kad sudarytų ryšį su tiksline transporto priemone.
Atakos metodas	Prijungtas kenksmingas elektroninis valdymo blokas naudojant transporto priemonės USB prievadą.	Sudarytas ryšys tarp atakuojančio transporto priemonės ir tikslinės transporto priemonės (arba kelio įrangos).
Apsaugos priemonės	Apsaugoti transporto priemonės USB prievadai.	Draudžiamos neatpažintos užklausos ar paslaugos.

EMPIRINIS TYRIMAS (10)



7 pav. Patikslintas sąveikaujančios transporto priemonės modelis (Othmane et al., 2013)

IŠVADOS

1. Atlikta daiktų interneto objektų saugumo rizikų, grėsmių ir apsaugos priemonių sisteminė mokslinės literatūros apžvalga parodė, kad prieigos kontrolės panaudojimas leidžia apsaugoti daiktų interneto objektų duomenis nuo nesankcionuoto naudojimo ir leidžia informaciją pasiekti tik įgaliotiems vartotojams.
2. Sukurtas daiktų interneto objektų decentralizuotas identifikavimo ir autentifikavimo metodas transporto priemonių valdymo sistemų saugai, kuris leidžia užtikrinti efektyvius duomenų mainus tarp globalaus masto heterogeniškų tinklo daiktų, efektyvią duomenų integraciją ir patikimumą esant dinamiškai aplinkai.
3. Atliktas sukurto metodo eksperimentinis tyrimas leidžia analizuojant jo efektyvumą simuliacijoje išspręsti pagrindines daiktų interneto saugos problemas, o pasiūlytos apsaugos priemonės užtikrina pakankamą informacijos saugos lygį ribotų skaičiavimo ir atminties resursų heterogeniškuose tinklo daiktuose.

LITERATŪRA

1. Dubois, E., Heymans, P., Mayer, N., Matulevičius, R. A Systematic Approach to Define the Domain of Information System Security Risk Management, in *Proc. of the International Conference on Intentional Perspectives on Information Systems Engineering (IPISE)*, Heidelberg, Germany, 2010. Berlin: Springer-Verlag, 289–306.
2. Othmane, L., Fuqaha, A., Hamida, E., Brand, M. Towards Extended Safety in Connected Vehicles, In *Proc. of the 16th International IEEE Annual Conference on Intelligent Transportation Systems (ITS)*, Hague, Netherlands, October 6–9, 2013, 652–657.
3. Qian, K., Parizi, R. M., Lo, D. OWASP Risk Analysis Driven Security Requirements Specification for Secure Android Mobile Software Development, In *Proc. of the International 2018 IEEE Conference on Dependable and Secure Computing,* Kaohsiung, Taiwan, December 10–13, 2018, 1–2.
4. Shapaval, R., Matulevičius, R. Towards the Reference Model for Security Risk ManagementinInternet of Things, In: *Proc. of the International Baltic Conference on Databases and Information Systems (Baltic DB&IS)*, Trakai, LT, July 1–4, 2018, 58–72.
5. Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., Kikiras, P. On the Security and Privacy of Internet of Things Architectures and Systems. In: *Proceedings of the International IoT Workshop on Secure Internet of Things (SIoT)*, Vienna, Austria, September 21–25, 2015, 49–57.

KITŲ MOKSLO METŲ DARBO PLANAS

2019 - 2020 m. m. darbo planas:

- Atlikti gautų duomenų analizę, apibendrinimą ir parengti išvadas:
  - apibendrinti teorinį tyrimą;
  - apibendrinti empirinį tyrimą;
  - apibendrinti ir išskirti esminius rezultatus bei parengti išvadas.
- Parengti atskiras daktaro disertacijos dalis:
  - patikslinti atskiras daktaro disertacijos dalis;
  - parengti analitinę disertacijos dalį;
  - parengti teorinės disertacijos dalį;
  - parengti eksperimentinę disertacijos dalį;
  - suformuluoti bendrąsias išvadas.
- Parengti daktaro disertaciją ir pateikti svarstymui.
- Apginti daktaro disertaciją.
- Dalyvauti tarptautinėje mokslinėje konferencijoje.
- Parengti mokslinę publikaciją recenzuojamame periodiniame leidinyje.

Ačiū už dėmesį