Įrodymais grįsto tinklo srauto duomenų modeliavimas ir analizė kibernetinių incidentų užkardymui

Ataskaita už 2023-2024 mokslo metus. Doktorantūros pradžios ir pabaigos metai: 2023-2027

Doktorantas: Virgilijus Krinickij
Darbo vadovas: Doc. Dr. Linas Bukauskas

Vilniaus Universitetas
Matematikos ir Informatikos Fakultetas
Informatikos Institutas

2024-10-04

Problema, Hipotezė

- **Problema:** Dabartiniai tinklo srauto analizės metodai yra neefektyvūs dėl didelių skaičiavimo resursų poreikio ir lėto veikimo, ypač kai reikia apdoroti didelės apimties duomenis. Realiam tinklo saugumo užtikrinimui reikalingi veiksmingesni algoritmai ir realaus laiko analizės sprendimai.
- **Hipotezė:** Tinklo srauto analizė yra neefektyvi dėl esamų algoritmų lėto veikimo, kuris kyla dėl didelių resursų reikalavimų apdorojant didelius duomenų kiekius.

Tyrimo objektas, tikslas, uždaviniai

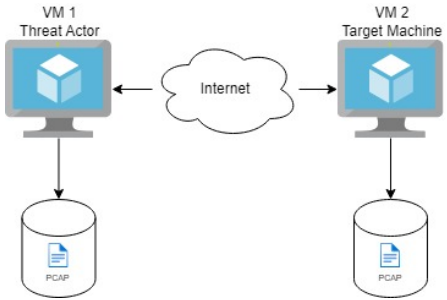
- **Tyrimo objektas** – Duomenų srautų gautu asinchroninio įrašymo metu modeliavimas.
- **Tyrimo tikslas** – Sukurtas naujas algoritminis modelis kompiuterių tinklu perduodamų duomenų efektyviam srautų panašumo vertinimui ir savybių atpažinimui.
- **Uždaviniai:**
  - Sintetiniai atvejai kompiuterių tinklo srauto transliacijai.
  - Duomenų srautų, gautų asinchroninio įrašymo metu simuliacija, modeliavimas ir jų vertinimas.
  - Tinklo srauto parametrų ir duomenų modelio sukūrimas.
  - Algoritmų kūrimas incidentų šablonų atpažinimui.
  - Sukurtų algoritmų efektyvumo vertinimas ir įtaka saugumui.
  - Gautų mokslinių rezultatų taikymas realių duomenų srautų vertinime.

Mokslinių rezultatų pristatymas

- Literatūros apžvalgos tikslas – asinchroniškai įrašytų tinklo srautų esamų algoritmų efektyvumo vertinimas, gretinimas (angl. alignment) ir incidentų aptikimui.
- Atlikta apžvalga leido padaryti išvadą, kad esami algoritmai turi būti tobulinami tinklo srautų gretinimui ir incidentų aptikimui.
- Esamų algoritmų problemos:
  - Tinklo srautas iš dviejų ar daugiau taškų tinkle veikia tik fiksuoto buferio (slenkančio lango kontekste) (Euclidean matching, Dynamic Time Warping, Needleman-Wunsch).
  - Nevienalytis (angl. heterogeneous) skirtingų tinklo taškų matomumas, naudojamų tinklo srautui užfiksuoti, ribotumo aspektas (Needleman-Wunsch).
  - Algoritmų sudėtingumas dviejų srautų vertinimo (Dynamic Time Warping) atveju.
  - Tinklo srauto sekų ilgis turi būti vienodas (Needleman-Wunsch, Smith Waterman).

Tyrimo metodas / aplinka

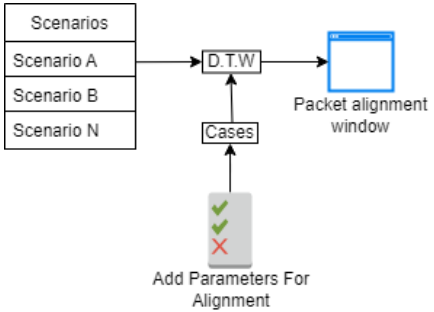
- Kontroliuojama, heterogeninė tinklo aplinka.
- Asinchroninis, automatizuotas tinklo srauto įrašymas tarp grėsmės aktoriaus ir aukos (taikinio) mašinos.
- Sintetiniai atakų scenarijai.



1 pav. Duomenu rinkimas naudojant virtualias mašinas

Modelis

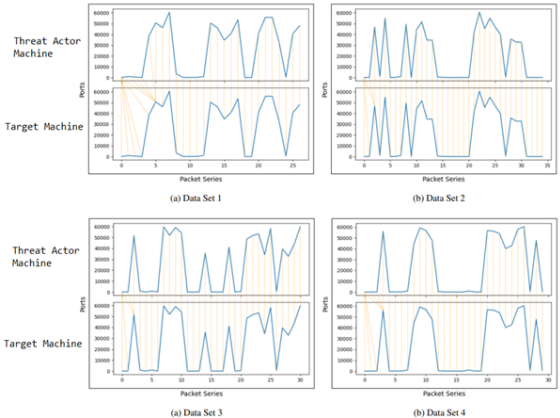
- Surinkti sintetinio scenarijaus duomenys perduodami DTW (Dynamic Time Warping).
- Paieškos atvejis duomenų sraute:
  - Tarkime A ir B yra tinklo srauto įrašai.
  - Rasti turinys(A) $\approx$ turiniui(B) $\wedge$ turinys(B) $\approx$ turiniui(A), kai Parametrai:
    - Tinklo srautų paketų požymiai, pvz:
    - SYN-ACK.
    - RST-ACK.
    - ir kiti.



2 pav. Asinchroninio tinklo srauto aprodojimo modelis

Tyrimo rezultatai

- Asinchroninis įrašų lygiavimas **yra įmanomas** nustatant tinklo anomalijas, įspėjimus ir incidentus.
- Asinchroninis įrašų lygiavimas **nesutrumpina laiko** nurodytų problemų sprendimui.
- Asinchroninio įrašų lygiavimo modelio tobulinimas **yra perspektyvus naudojant skirtingus metodus**.

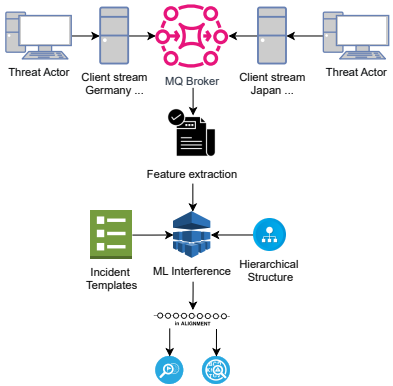


(a) Data Set 1 (b) Data Set 2

(a) Data Set 3 (b) Data Set 4

Ateities tyrimų planas

- Modelis incidentų atpažinimui ir sudėtingų kibernetinių atakų aptikimui dideliuose tinklo srautuose.
- Toliau gilinsimės į šablonų derinimą, hierarchines struktūras, ir klasifikatorius, tikimybinių modelių kūrimą, kurie leis atlikti veiksmingą tinklo srautų analizę realiuoju laiku siekiant aptikti kibernetinius incidentus.
- Taip pat mes pridėsime automatizaciją, mašinį mokymą, sofistikuotų kibernetinių atakų šablonus.



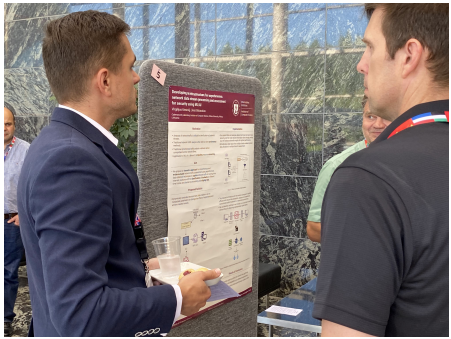
3 pav. Pasiūlyto modelio architektūra

2023/2024 m. m. I pusmečio atlikti darbai

1. **Surinkti** bendrųjų gebėjimų lavinimo kreditai, 3.75kr.
2. **Atlikta** Mokslinė literatūros ir publikacijų analizė:
   1. 15 proc. rengiant žurnalinį straipsnį;
   2. 100 proc. ruošiant straipsnį į „European Conference on Cyber Warfare and Security” (ECCWS) konferenciją;
   3. **Priimtas** mokslinis straipsnis į ECCWS konferencija (angl. academic research paper).

2023/2024 m. m. II pusmečio atlikti darbai

- Išlaikytas privalomas dalykas „Informatikos ir in formatikos inžinerijos tyrimo metodai ir metodika“.
- Sudalyvauta tarptautinėje konferencijoje su pranešimu „23rd European Conference on Cyber Warfare and Security - ECCWS 2024“.
- **Pristatytas** plakatas ECCWS konferencijoje.
- **Sukurta aplinka būsimies eksperimentams atlikti**.
- **Modelio kūrimas incidentų atpažinimui ir sudėtingų kibernetinių atakų aptikimui dideliuose tinklo srautuose.**
- **Atlikta** Mokslinė literatūros ir publikacijų analizė:
  - 30 proc. rengiant žurnalinį straipsnį į „Special Issue on “Advances in Robust Intrusion Detection through Machine Learning”, Computers & Security“.
  - 60 proc. rengiant žurnalinį straipnį į „International Journal of Electronic Security and Digital Forensics“.



4 pav. ECCWS konferencijos plakato pristatymas

Doktorantūros studijų planas

Studijų metai	Egzaminai	
	Planas	Įvykdyta
I (2023/2024)	1	1
II (2024/2025)		
III (2025/2026)	2	
IV (2026/2027)	1	

1 lentelė. Egzaminai pagal studijų planą

Studijų metai	Dalyvavimas konferencijose				Publikacijos					
	Tarptautinėse		Nacionalinėse		Su citav. rodikliu			Be citavimo rodiklio		
	Planas	Įvykdyta	Planas	Įvykdyta	Planas	Įvykdyta	Būklė	Planas	Įvykdyta	Būklė
I (2023/2024)	1	1						1	1	Priimta
II (2024/2025)					1					
III (2025/2026)					1					
IV (2026/2027)	1							1		
Iš viso:	2	1			2			2	1	

2 lentelė. Konferencijų ir publikacijų planas

Ataskaitinis studijų metai (2023/2024)

Dalyvavimas tarptautinėje konferencijoje 2023/2024 (II Pusmetis)		
Planas	**Įvykdyta**	**Konferencijos tipas**
23rd European Conference on Cyber Warfare and Security - ECCWS 2024	Virgilijus Krinickij and Linas Bukauskas, Asynchronous Record Alignment of Network Flows for Incident Detection and Reconstruction, 23rd European Conference on Cyber Warfare and Security - ECCWS 2024, Agora Building at University of Jyväskylä, Finland 26 - 28 June 2024	Tarptautinė

3 lentelė. Dalyvavimas tarptautinėje konferencijoje

Egzaminai 2023-2024 II pusmetis		
Planas	**Įvykdyta**	**Būklė**
Informatikos ir informatikos inžinerijos tyrimo metodai ir metodika (2024-06-25)	Informatikos ir informatikos inžinerijos tyrimo metodai ir metodika (2024-06-25)	Išlaikytas

4 lentelė. Išlaikyti egzaminai

Ataskaitinis studijų metai (2023/2024) (2)

Publikacijos 2023/2024 (II pusmetis))			
Planas	**Įvykdyta**	**Būklė**	**Publikacijos Tipas**
23rd European Conference on Cyber Warfare and Security - ECCWS 2024, Agora Building at University of Jyväskylä, Finland 26 - 28 June 2024	Krinickij, Virgilijus; Bukauskas, Linas. Asynchronous record alignment of network flows for incident detection and reconstruction // European Conference on Cyber Warfare and Security: Proceedings of the 23rd European Conference on Cyber Warfare and Security. Reading: Academic Conferences International Limited. ISSN 2048-8602. eISSN 2048-8610. 2024, vol. 23, no. 1, p. 249-256. DOI: 10.34190/eccws.23.1.2254.	Publikuota	Be cituojamumo rodiklio

5 lentelė. Publikacijos

Publikacijos (tik su citavimo rodikliu)		
	Bibliografinis aprašas	**Būklė**
1.		Ruošiama

6 lentelė. Publikacijos su cit. rodikliu

2024/2025 m. m. III pusmečio darbo planas

- Straipsnio rengimas į „Baltic Journal of Modern Computing“ žurnalą.
- Straipsnio rengimas į „Special Issue on Advances in Robust Intrusion Detection through Machine Learning, Computers & Security“ žurnalą.
- Išlaikyti dalyką Fundamentalieji informatikos ir informatikos inžinerijos metodai
- Išlaikyti dalyką Šiuolaikinės duomenų bazių sistemos.
- Kibernetinio saugumo vasaros mokykla.

Ačiū už dėmesį!