Institute of Computer Science

Įrodymais grįsto tinklo srauto duomenų modeliavimas ir analizė kibernetinių incidentų užkardymui

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

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

Doktorantūros studijų planas

Studijų metai	Egzaminai	
	Planas	Įvykdyta
I (2023/2024)	1	
II (2024/2025)		
III (2025/2026)	2	
IV (2026/2027)	1	
Iš viso:	4	

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	Priimta
II (2024/2025)					1					
III (2025/2026)					1					
IV (2026/2027)	1							1		
Iš viso:	2				2			2	1	

Ataskaitinis studijų pusmetis (I: 2023/2024 - I pusmetis)

Egzaminai 2023-2024 I pusmetis		
Planas	Įvykdyta	Būklė
0		

Dalyvavimas konferencijose 2023/2024 (I Pusmetis)		
Planas	Įvykdyta	Konferencijos tipas
0		

Publikacijos 2023/2024 (I pusmetis)			
Planas	Įvykdyta	Būklė	Publikacijos Tipas
1	1	Priimta	Be cituojamumo rodiklio

Doktorantūros studijų pasiekimai

Dalyvavimas tarptautinėse konferencijose	
	Aprašas
1. **Virgilijus Krinickij**, Linas, Bukauskas, „*Asynchronous Record Alignment of Network Flows for Incident Detection and Reconstruction*“, 23rd European Conference on Cyber Warfare and Security, 27 - 28 June 2024, Jyväskylä, Finland.	

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

Moksliniu tyrimu ir disertacijos rengimo etapai

1.	**Mokslinių tyrimų disertacijos tema apžvalga ir analizė (Lietuvoje ir užsienyje):**		
1.1.	Mokslinės literatūros ir publikacijų analizė.	2023 m. IV ketvirtis	2024 m. I ketvirtis
1.2.	Kitų publikacijų analizė.	2024 m. I ketvirtis	2024 m. III ketvirtis
2.	**Mokslinio tyrimo vykdymas:**		
2.1.	**Tyrimo metodikos sudarymas:**		
2.1.1.	Tinklų srauto probleminės srities suformulavimas.	2024 m. I ketvirtis	2024 m. III ketvirtis
2.1.2.	Probleminių uždavinių aprašymas.	2024 m. I ketvirtis	2024 m. III ketvirtis

Tyrimo objektas, tikslas

- **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.

Tyrimo 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.

2023/2024 m. m. I pusmečio atlikti darbai

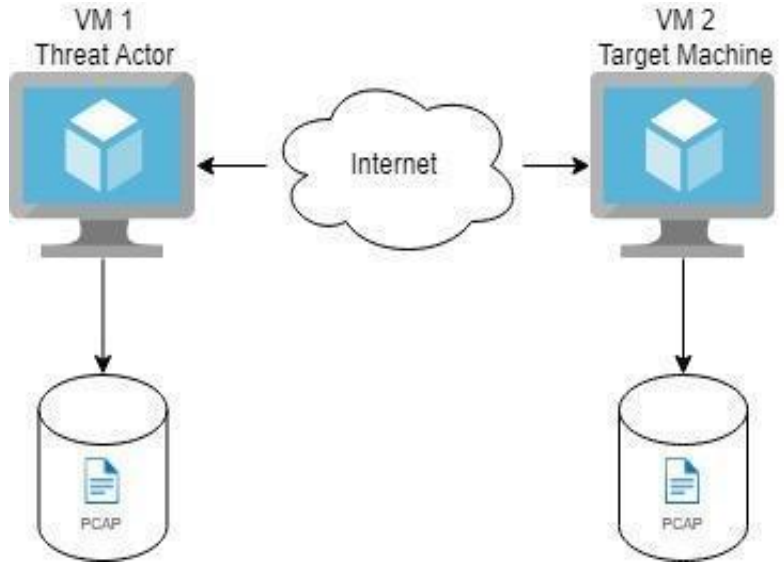
- **Surinkti** bendrųjų gebėjimų lavinimo kreditai, 3.25kr.
- **Atlikta** Mokslinė literatūros ir publikacijų analizė:
  - 15 proc. rengiant žurnalinį straipsnį;
  - 100 proc. ruošiant straipsnį į European Conference on Cyber Warfare and Security (ECCWS) konferenciją;
- **Priimtas** mokslinis straipsnis į ECCWS konferencija (angl. academic research paper).

2023/2024 m. m. I pusmečio 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*).
  - Nevienalytis (angl. heterogeneous) skirtingų tinklo taškų matomumas, naudojamų tinklo srautui užfiksuoti, ribotumo aspektas (*Needleman-Wunsch*).
  - Algoritmų sudėtingumas dviejų srautų vertinimo (*Dynamic Time Warping*) atveju.

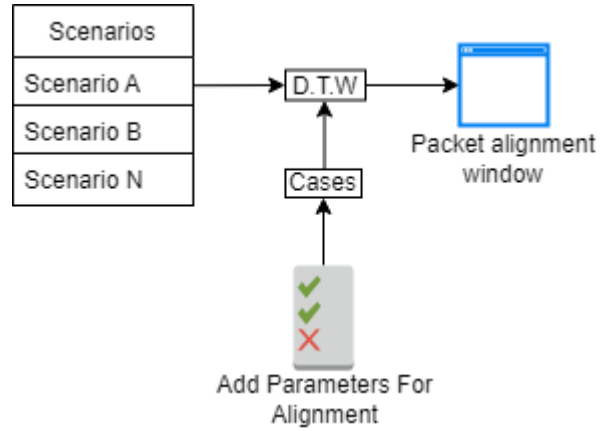
Tyrimo metodas / aplinka

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

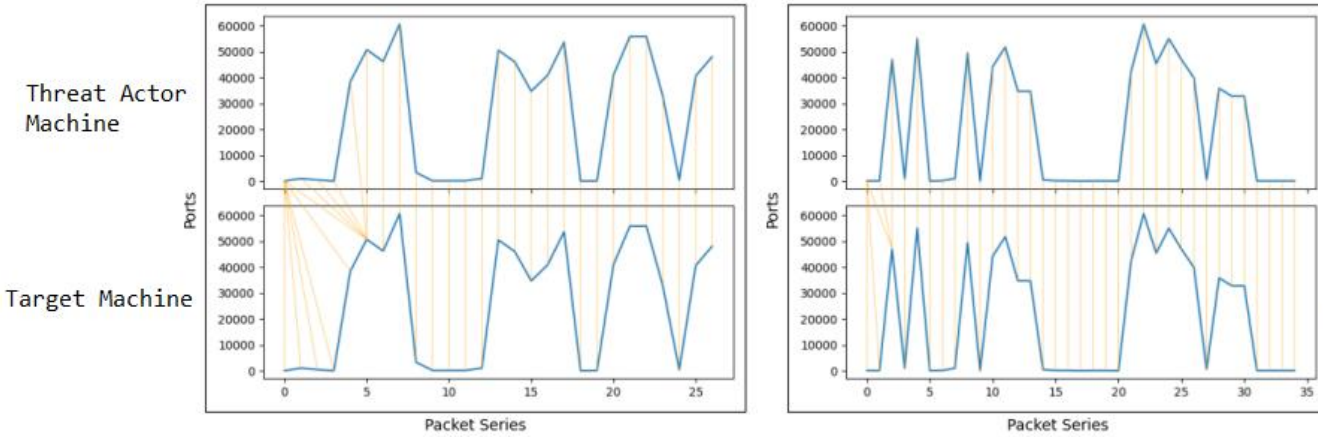


Algoritmas

- Surinkti sintetinio scenarijaus duomenys perduodami DTW.
- Paieškos atvejis duomenų sraute:
  - Tarkime A ir B yra tinklo srauto įrašai.
  - Rasti *turinys(A) ≈ turiniui(B) ∧ turinys(B) ≈ turiniui(A)*, kai Parametrai:
  - Tinklo srautų paketų požymiai, pvz.,
    - SYN-ACK
    - RST-ACK
    - ir kiti

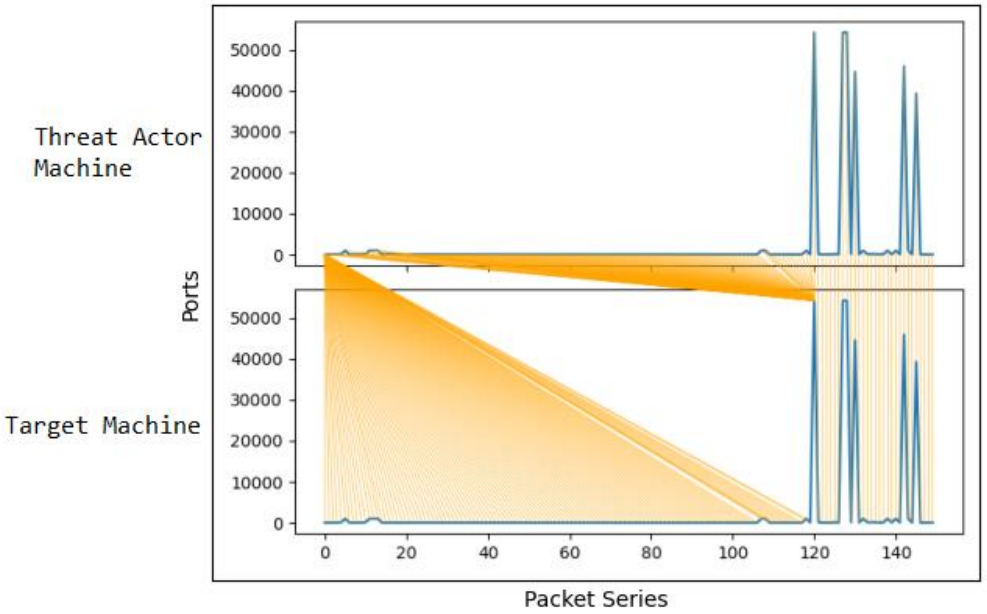


Rezultatai



(a) Data Set 1

(b) Data Set 2



Vilnius University

Kito pusmečio darbo planas

- Pranešimas ,,European Conference on Cyber Warfare and Security (ECCWS)“ konferencijoje.
- Sudaryti ir aprašyti tyrimo metodiką.
- Sukurti naują metodą duomenų modeliavimui ir analizei kibernetinių incidentų užkardymui.
- Kibernetinio saugumo vasaros mokykla.

Ačiū už dėmesį

Virgilijus Krinickij,
Kibernetinio saugumo laboratorija,
Didlaukio g. 47, 502, 506 kab.
virgilijus.krinickij@mif.vu.lt