Vilniaus universitetas

Mašininiu mokymusi grindžiami metodai apgaulingoms ir obfuskuotoms kenkėjiškoms programoms generuoti stiprinant kibernetinį saugumą

Informatikos inžinerija (T 007)
Doktorantūros pradžios/pabaigos metai: 2023-2027
Studijų metai: 2023/2024 antras pusmetis

Doktorantas: Juozas Dautartas
Vadovas: Dr. Viktor Medvedev

Studijų planas ir jo vykdymo suvestinė

Vilniaus universitetas

Studijų metai	Egzaminai	
	Planas	Įvykdyta
I (2023/2024)	**3**	**3**
II (2024/2025)	1	
III (2025/2026)		
IV (2026/2027)		
Iš viso:	4	3

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

Ataskaitinio pusmečio darbo planas ir jo vykdymo suvestinė

Vilniaus universitetas

Egzaminai 2023/2024 (II pusmetis)		
Planas	**Įvykdyta**	**Būklė**
Informatikos ir informatikos inžinerijos tyrimo metodai ir metodika. 2024 m. birželio mėn.	Informatikos ir informatikos inžinerijos tyrimo metodai ir metodika 2024 m. II ketvirtis	Išlaikytas
Gilieji neuroniniai tinklai. 2024 m. birželio mėn.	Gilieji neuroniniai tinklai 2024 m. II ketvirtis	Išlaikytas

Dalyvavimas konferencijose 2023/2024 (II pusmetis)		
Planas	**Įvykdyta**	**Konferencijos tipas**

Publikacijos 2023/2024 (II pusmetis)			
Planas	**Įvykdyta**	**Būklė**	**Publikacijos tipas**

Tyrimų objektas

- Mašininio mokymosi algoritmai, skirti generuoti ir obfuskuoti C2 (angl. Command and Control) sistemų agentus, naudojamus kenkėjiškos programinės įrangos (angl. malware) kūrimui ir diegimui.
- Tyrimas orientuotas į inovatyvių metodų kūrimą, siekiant sukurti kenkėjišką programinę įrangą, kuri išnaudoja mašininiu mokymusi pagrįstų aptikimo sistemų pažeidžiamumus.
- Naujų C2 sistemų agentų generavimo metodų sukūrimas, leidžiantis efektyviai paslėpti kenkėjišką veiklą nuo pažangių saugumo priemonių, tokių kaip antivirusinės ir Endpoint Detection and Response sistemos, pasitelkiant pažangius mašininio mokymosi metodus, tokius kaip generatyviniai priešiški tinklai (GAN), variaciniai autoencoderiai ir kt.

Tikslas

Pasiūlyti ir ištirti naują kenkėjiškos programinės įrangos generavimo metodą, skirtą veiksmingai išnaudoti mašininiu mokymusi pagrįstų kenkėjiškų programų aptikimo sistemų pažeidžiamumą, siekiant padidinti kibernetinių grėsmių atsparumą ir pagerinti bendrą jų aptikimo tikslumą ir patikimumą.

Uždaviniai

- Atlikti išsamią analitinės literatūros apžvalgą, siekiant nustatyti esamus mašininio mokymosi metodus ir būdus, skirtus kenkėjiškoms programoms aptikti, klasifikuoti ir generuoti kenkėjiškas programas.
- Analizuoti antivirusinių ir galinių įrenginių aptikimo ir reagavimo (angl. Endpoint Detection and Responce, EDR) sistemų kenkėjiškos programinės įrangos aptikimo mechanizmus, siekiant suprasti kenkėjiškos programinės įrangos klasifikavimo ypatybes.
- Įvertinti ir išskirti pagrindinius kenkėjiškos programinės įrangos požymius, turinčius įtakos jų aptikimui, siekiant pagerinti kenksmingų programų klasifikavimo tikslumą.

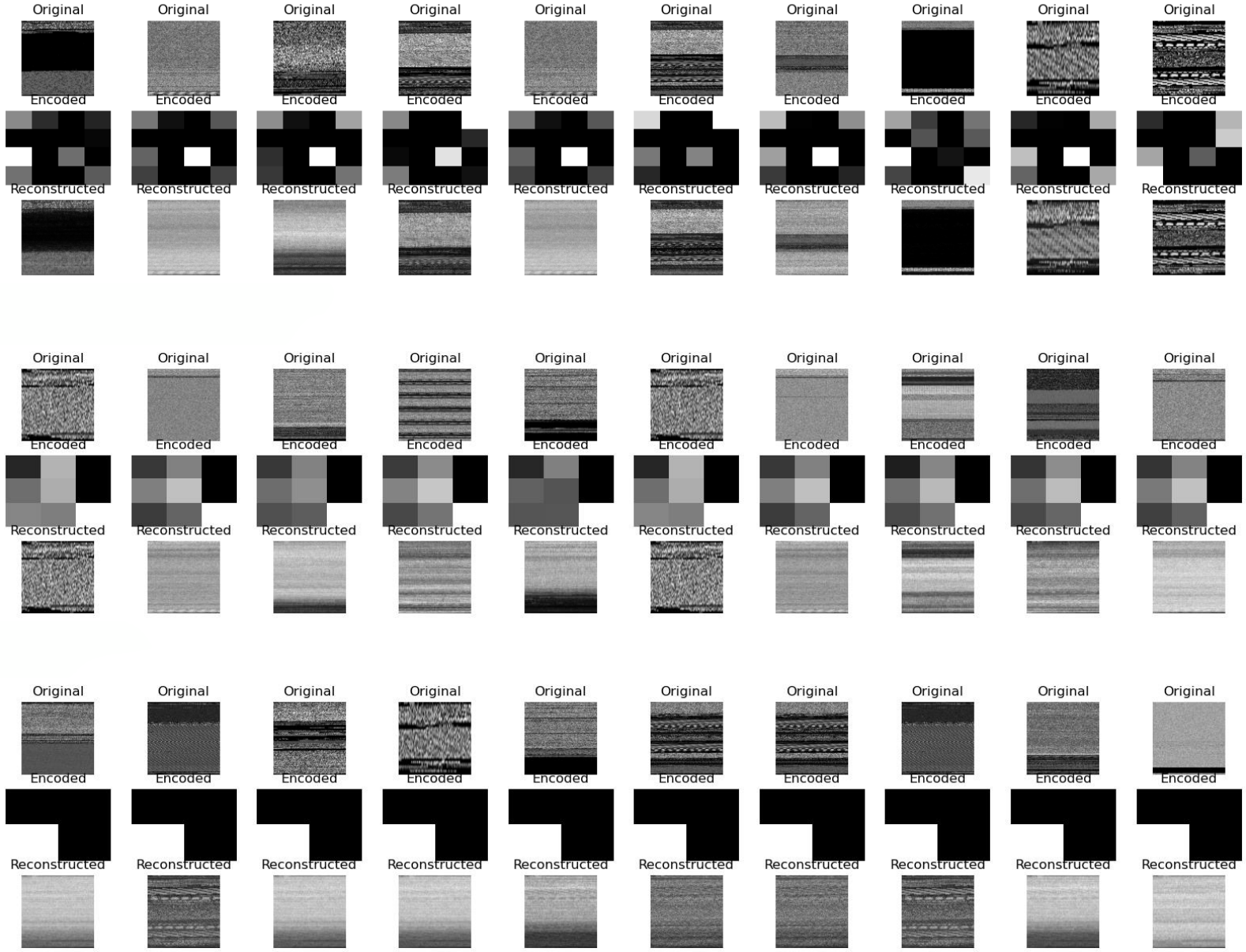
Uždaviniai

- Sukurti naują arba modifikuoti esamą kenkėjiškų programų (angl. Command and Control framework agents) generavimo metodą, kuriuo siekiama sukurti klaidinančius ir sunkiai aptinkamus C2 sistemų agentų pavyzdžius, galinčius klaidinti mašininiu mokymusi pagrįstus kenkėjiškų programų aptikimo modelius.
- Įvertinti sugeneruotus kenkėjiškų programų pavyzdžius, naudojant įvairius kenkėjiškų programų aptikimo sprendimus ir mašininiu mokymusi grindžiamas kibernetinio saugumo sistemas.
- Ištirti esamas ir pasiūlyti naują strategiją, kaip padidinti mašininio mokymosi modelių atsparumą priešiškoms atakoms.

Per pusmetį gauti rezultatai

- Mašininio mokymosi metodai, ypač gilieji neuroniniai tinklai, turi didelį potencialą kenkėjiškos programinės įrangos aptikimui ir klasifikavimui, tačiau jie yra jautrūs priešiškoms atakoms, naudojant baltosios ir juodosios „dėžės“ metodologijas.
- Generatyviniai tinklai (GAN) susiduria su iššūkiais, kai bandoma modifikuoti kenkėjiškas programas ir išlaikyti jų veiksmingumą, tačiau jie turi potencialo tiek maskavimui, tiek aptikimo tobulinimui kibernetinio saugumo srityje.
- Autoencoderiai efektyviai suspaudžia duomenis ir gali būti naudojami kenkėjiškų programų klasifikavimui, tačiau per didelis suspaudimas gali lemti pradinės informacijos praradimą, kas neigiamai veikia aptikimo kokybę.

Atlikti eksperimentai su klasikiniais autoencoderiais



Dalyvavimas bendruosius gebėjimus stiprinančiose veiklose

Vilniaus universitetas

Locked Shields 2024

- Šių metų balandžio 22-26 dienomis, Estijoje (Talinas) dalyvauta (dalyvauta gyvai) didžiausiuose NATO kibernetinio saugumo pratybose Locked Shields 2024 atstovaujant Lietuvą ir atliekant kibernetines atakas prieš tarptautines „Mėlynąsias komandas“ siekiant pagerinti specialistų pasiruošimą kibernetinėms grėsmėms.

Vilniaus universitetas

Online mokymai, kurių trukmė apie pusę metų. Sertifikuoto įsiskverbimo specialisto kursas (angl. Certified Penetration Testing Specialist) iš „Hack the Box“ yra praktinio pobūdžio kursas, kurio metu mokomasi rasti pažeidžiamumus įvairiuose dažnai naudojamuose technologijose.

Vilniaus universitetas

Global Information Assurance Certification

GIAC
CERTIFICATIONS

GIAC presents this certification to:

Juozas Dautartas

who has met the necessary requirements and demonstrated a mastery of the subject matter and security skills to earn the

GIAC Red Team Professional

2024/7/31
Received on this date

189
Analyst number

GIAC RED TEAM
GRTP
PROFESSIONAL

2028/7/31
Valid through this date

Jeremy Rabson

Jeremy Rabson, General Manager
Global Information Assurance Certification

Kursas vyko 2024 m. Balandžio mėn. JAV (dalyvauta gyvai). Išlaikytas SANS instituto SEC565 kurso, teorinio pobūdžio egzaminas. Kurso metu buvome mokomi kaip planuoti ir vykdyti „Raudonosios komandos“ operacijas.

Vilniaus universitetas

Online mokymai, kurių trukmė apie pusę metų. Šių mokymų metu buvo mokomi įvairūs būdai kaip pažengusios grėsmės (angl. APT – Advanced Persistance Threat) išlieka Windows operacinėse sistemose po sistemos perkrovimų arba pradinio implanto aptikimo.

Vilniaus universitetas

Mokslininkų grupių projektai LMT:

- Pavadinimas: Valdymo ir kontrolės sistemos, pagrįstos priešišku mašininiu mokymusi, kūrimas kibernetiniam saugumui gerinti ir įgūdžiams tobulinti
- Projektu siekiama prisidėti prie naujos C2 sistemos, skirtos pagerinti kibernetinio saugumo sritį, sukūrimo, įtraukiant varžymosi principais pagrįsto ML metodus (Adversarial ML, AML) į C2 sistemas.
- Projekto tikslas – sukurti valdymo ir kontrolės sistemą (C2), kurioje būtų taikomas varžymosi principais pagrįstas mašininis mokymasis ir kuri generuotų etišką kenkėjišką programinę įrangą, skirtą puolamiesiems kibernetinio saugumo veiksmams vykdyti kontroliuojamoje aplinkoje, ir taip užtikrinti svarbų ir tikrovišką kibernetinio saugumo ekspertų mokymą.


IŠ ČIA KYLĄMA
Į ŽVAIGŽDES
SVEIKINAME ATVYKUS Į ISKS KLUBĄ!
Matematikos ir informatikos fakultetas

Kito pusmečio darbo planas

- Išlaikyti egzaminą: Fundamentalieji informatikos ir informatikos inžinerijos metodai.
- Atlikti išsamesnę mokslinių problemų analizę, susijusią su kenkėjiškos programinės įrangos generavimu, aptikimu ir klasifikavimu kibernetinio saugumo kontekste, taikant mašininio mokymosi metodus.
- Atlikti išsamesnę mašininio mokymosi metodų, skirtų kenkėjiškų programų aptikimui, klasifikavimui ir obfuskavimui (maskavimui), analitinę apžvalgą, įtraukiant naujausias mokslines publikacijas.
- Parinkti tinkamas tyrimo metodikas iškeltiems uždaviniams spręsti.
- Suplanuoti teorinį ir empirinį tyrimus pagal pasirinktą metodiką.

KLAUSIMAI

Juozas Dautartas
juozas.dautartas@mif.stud.vu.lt

Darbo pavadinimas		Atlikimo terminai		Pastabos
		Nuo	Iki	
1.	**Mokslinių tyrimų disertacijos tema apžvalga ir analizė (Lietuvoje ir užsienyje):**			
1.1.	Disertacijos tyrimo objekto detalizavimas.	2023 m. IV ketvirtis	2024 m. I ketvirtis	Suformuluotas disertacijos tyrimų objektas.
1.2.	Tyrimo tikslo suformavimas.	2023 m. IV ketvirtis	2024 m. I ketvirtis	Suformuluotas tyrimo tikslas ir uždaviniai.
1.3.	Identifikuoti (nustatyti) mokslines problemas, susijusias su kenkėjiškos programines įrangos generavimu, aptikimu ir klasifikavimu kibernetinio saugumo kontekste taikant mašininio mokymosi metodus.	2023 m. IV ketvirtis	2024 m. III ketvirtis	Atlikta kenkėjiškos programinės įrangos generavimo, aptikimo ir klasifikavimo problemų pradinė analizė. Taip pat buvo nustatyta, kad kenkėjiška programinė įranga, modifikuota naudojant varžymosi principais pagrįstus mašininio mokymosi algoritmus, dažnai tampa nefunkcionali, kas apsunkina jos praktinį panaudojimą.
1.4.	Atlikti mašininio mokymosi metodų, skirtų kenkėjiškų programų aptikimui, klasifikavimui ir obfuskavimui (maskavimui), analitinę apžvalgą.	2023 m. IV ketvirtis	2024 m. III ketvirtis	Tęsiama mašininio mokymosi metodų, taikomų kenkėjiškų programų aptikimui, klasifikavimui ir obfuskavimui, analitinė apžvalga.