Dirbtinio intelekto metodų taikymas įsiskverbimų į kompiuterinius tinklus aptikimo sistemose

2016 – 2017 m. studijos

Doktorantas: Liudas Ališauskas
Vadovas: Virginijus Marcinkevičius

Disertacijos tikslas ir objektas

Tikslas

Pagerinti dirbtinio intelekto metodų tikslumą ir efektyvumą aptinkant įsiskverbimus į kompiuterinius tinklus.

Objektas

Dirbtinio intelekto metodai, jų tikslumas ir efektyvumas aptinkant įsiskverbimus į kompiuterinius tinklus.

2016 -2017 studijų uždaviniai

- Atlikti kompiuterinių tinklų duomenų srauto ir veiklą registruojančių įrašų analizę.
- Atlikti įsiskverbimų į kompiuterių tinklus atakos vektorių analizę.
- Atlikti dirbtinio intelekto metodų taikomų aptinkant įsiskverbimus į kompiuterių tinklus analizę.

Planuoti rezultatai

- Kompiuterinių tinklų veiklą atspindinčių duomenų modeliai.
- Įsiskverbimų į kompiuterių tinklus požymiai, kurių pagalba mokomi dirbtinio intelekto metodai.
- Nustatyti šiuo metu kompiuterių tinklų saugos sprendimuose taikomi dirbtinio intelekto metodai, jų taikymo aplinkybės.

Ataskaitinių metų darbo planas

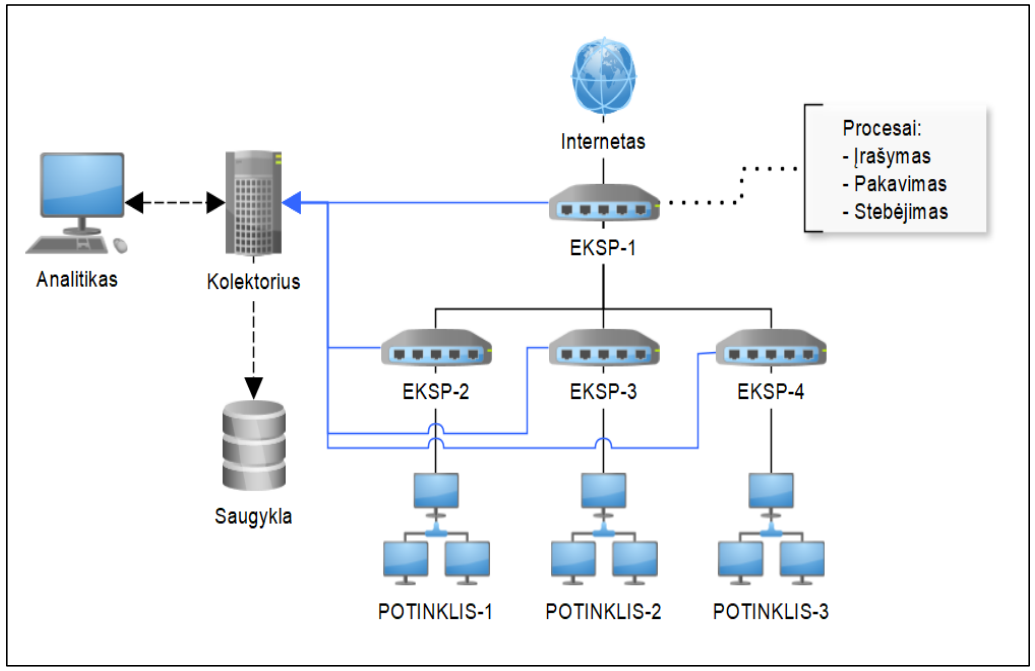
- **Mokslinių tyrimų disertacijos tema apžvalga ir analizė (Lietuvoje ir užsienyje):**
  - Disertacijos tyrimo objekto detalizavimas.
  - Esamų dirbtinio intelekto metodų, naudojamų srautinių kompiuterinio tinklo duomenų struktūrizavimui, analizė.
  - Esamų anomalijų kompiuteriniuose tinkluose nustatymo metodų apžvalga.
  - Metodų apžvalgos apibendrinimas ir pateikimas disertacijos analitinės dalies aprašyme.
- **Išlaikyti šių dalykų egzaminus:**
  - Duomenų analizės strategijos ir sprendimų priėmimas (prof. habil. dr. Gintautas Dzemyda).
  - Optimizavimo metodai ir jų taikymai (prof. habil. dr. Leonidas Sakalauskas).
  - Atpažinimo teorija (prof. habil. dr. Kazys Kazlauskas, dr. Gintautas Tamulevičius).

Kompiuterių tinklo srauto duomenys (1)

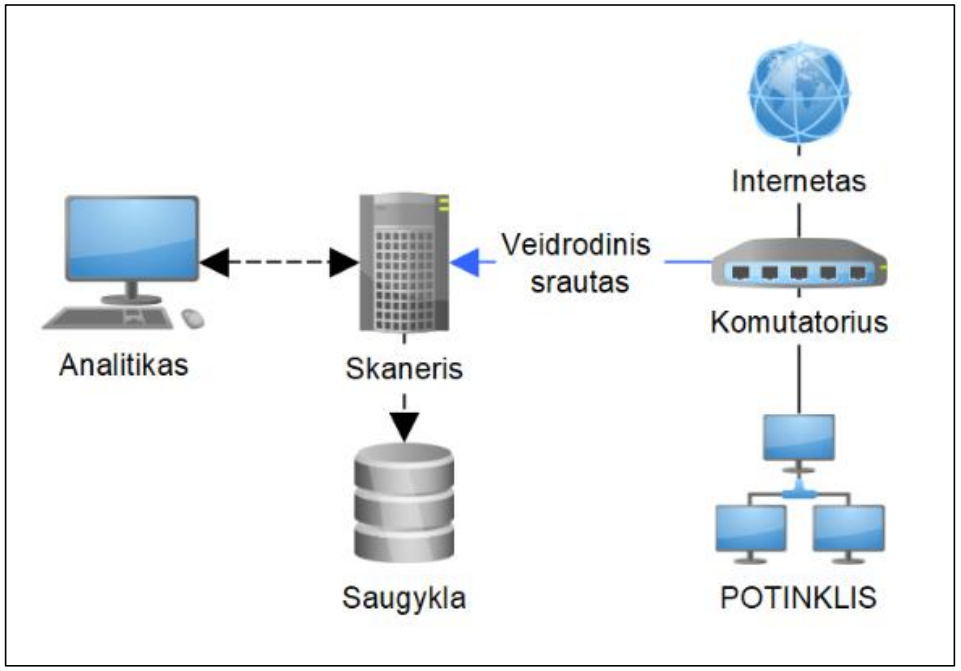
- Gaunami iš kompiuterių tinklų srautų analizės technologijų:
  - NetFlow (Flexible NetFlow)
  - JFlow
  - sFlow
  - NetStream

- Gaunami tiesiogiai nuskaitant tinklo duomenų paketus:
  - Tspdump, pcaplib
  - Argus

Kompiuterių tinklo srauto duomenys (2)



Principinė tinklo srautų analizės technologijų schema.



Principinė tinklo srauto nuskaitymo schema.

Kompiuterių tinklo srauto duomenys (3)

Kompiuterių tinklo srauto duomenys:

- Parametrų tipai:
  - skaitiniai (angl. Numerical data)
  - kategoriniai (angl. Categorical data)
- Duomenų rinkinį sudaro sekos duomenys (angl. Sequence data)
- Kiekvienas objektas turi laiko žymę (angl. Time series)

l_number	l_timestamp	l_sysuptime	l_ip_src	l_ip_dst	l_srcport	l_dstport	l_prot
1	08:24:05-03:24:06	436339	12.1.1.2	12.1.1.254	1734	23 telnet	tcp
98	08:24:05-03:33:52	1022315	12.1.1.2	12.1.1.254	1734	23 telnet	tcp
70	08:24:05-03:31:10	860037	12.1.1.2	12.1.255.255	137	137 netbios-ns	udp
171	08:24:05-03:41:10	1460041	12.1.1.2	12.1.255.255	137	137 netbios-ns	udp
230	08:24:05-03:47:08	1818629	12.1.1.2	12.1.255.255	137	137 netbios-ns	udp
273	08:24:05-03:51:26	2076055	12.1.1.2	12.1.255.255	137	137 netbios-ns	udp
373	08:24:05-04:01:42	2692093	12.1.1.2	12.1.255.255	137	137 netbios-ns	udp
473	08:24:05-04:11:42	3292076	12.1.1.2	12.1.255.255	137	137 netbios-ns	udp
572	08:24:05-04:21:50	3900105	12.1.1.2	12.1.255.255	137	137 netbios-ns	udp
672	08:24:05-04:31:58	4508138	12.1.1.2	12.1.255.255	137	137 netbios-ns	udp
772	08:24:05-04:42:11	5121151	12.1.1.2	12.1.255.255	137	137 netbios-ns	udp
873	08:24:05-04:52:22	5732189	12.1.1.2	12.1.255.255	137	137 netbios-ns	udp
932	08:24:05-04:58:10	6080760	12.1.1.2	12.1.255.255	137	137 netbios-ns	udp
1223	08:24:05-05:28:10	7880779	12.1.1.1	12.1.255.255	137	137 netbios-ns	udp

Kibernetinės atakos. Procesas.

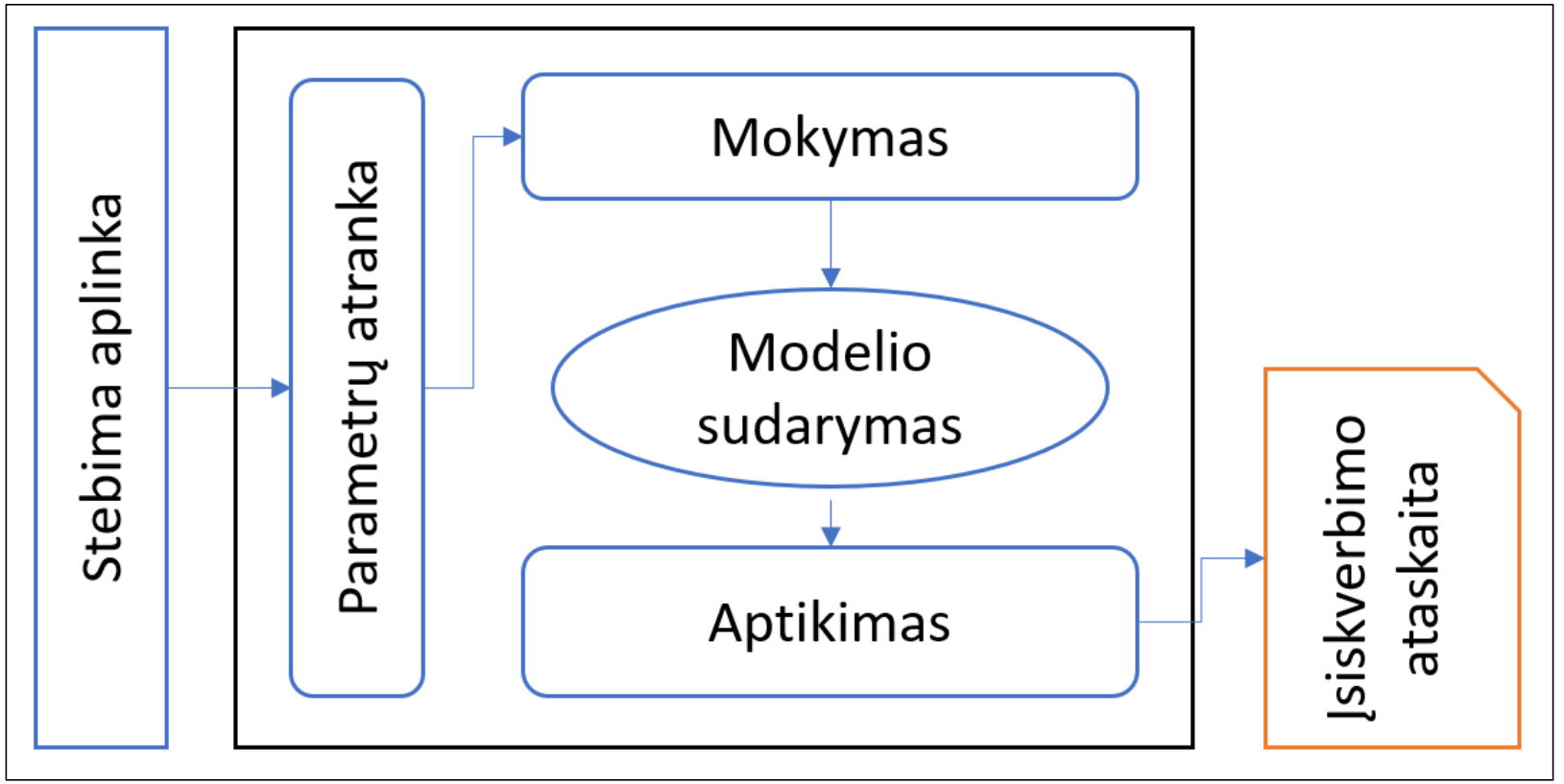
- 1 etapas: Žvalgyba (angl. Reconnaissance)
- 2 etapas: Pirminis įsilaužimas (angl. Initial compromise)
- 3 etapas: Vadovavimas ir valdymas (angl. Command & control)
- **4 etapas: Horizontalus judėjimas (angl. Lateral movement)***
- 5 etapas: Taikinių užvaldymas (angl. Target attainment)
- 6 etapas: Duomenų ištraukimas, sistemų sugadinimas ir sutrikdymas (angl. Exfiltration, corruption, and disruption)

* Tolimesnė tyrimų sritis

Kibernetinės atakos. Požymiai.

- Normalaus duomenų srauto požymiai tinkle.
- Laikas kai duomenų srautai pasiekia savo minimumą ar maksimumą.
- Aktyvūs tinklo įrenginiai ir klientai tam tikru laiko momentu.
- Vidutinė komunikacijų sesijų trukmė.
- Protokolų ir programų pasiskirstymas duomenų srautuose.
- Įeinantys ir išeinantys duomenų srautai.
- Sesijų užklausų skaičius.
- Įrenginiai generuojantys ir gaunantys duomenis tinkle.
- Tinklo skenavimas.

Principinė A-NIDS schema



A-NIDS – Anomaly based Network Intrution Detection System

Anomalijų aptikimu pagrįsti metodai

- **Bajeso tinklai** (angl. Bayesian networks). Modelis realizuoja tikimybės ryšius su dominančiais parametrais. Modelis dažniausiai taikomas kartu su statistiniais modeliais. Nors Bajeso tinklai demonstruoja gerus rezultatus, laikoma, kad šis modelis reikalauja didelių skaičiavimo pajėgumų.
- **Neuroniniai tinklai** (angl. Neural networks). Simuliuodami žmogaus smegenų veikimą, neuroniniai tinklai demonstruoja gerus rezultatus aptinkant įsiskverbimus dėl savo gebėjimo lanksčiai prisitaikyti prie besikeičiančios aplinkos. Metodas dažnai naudojamas sukurti kompiuterių tinklų naudotojų profiliams.
- **Neaiškioji logika** (angl. Fuzzy logic techniques). Šis metodas demosntruoja gerus rezultatus aptinkant tinklo prievadų skenavimus ir bandymus jungtis prie sistemų. Silpnoji pusė – reikalauja daug skaičiavimo resursų.
- **Genetiniai algoritmai** (angl. Genetic algorithms). Stipriojų šių metodų pusė – gebėjimas lanksčiai ir rezultatyviai rasti galimus sprendimus iš skirtingų šaltinių, neturint pirminės informacijos apie stebimos sistemos elgesį. Trūkumas – reikalauja daug resursų.
- **Klasterizavimas ir neatitikimų aptikimas** (angl. Clustering and outlier detection). Šie metodai dirba su pirminiais netransformuotais duomenimis, todėl sumažinamos pastangos ruošiant duomenis analizei.

Tyrimo išvados ir tolimesni darbai

- Išanalizuoti pagrindiniai kompiuterių tinklo srautų duomenys, jų gavybos būdai ir sprendimai. Siekiant gauti kompiuterių tinklo duomenis gali pasinaudoti sukurtomis technologijomis kaip: NetFlow, JFlow, sFlow, tai pat gaunant duomenis tiesiogiai nuskaitant kompiuterių tinklo duomenų paketus.
- Apžvelgti pagrindiniai kibernetinių atakų vektoriai kompiuterių tinkluose, nustatyti požymiai leidžiantys identifikuoti anomalijas tinklų veikloje dėl kibernetinių atakų.
- Apžvelgti pagrindiniai anomalijų (įsiskverbimų) aptikimo metodai, jų stipriosios ir silpnosios pusės.
- **Tolimesnis disertacijos tyrimas siaurinamas fokusuojantis į kibernetinės atakos proceso horizontalaus judėjimo (angl. Lateral movement) etapą, siekiant aptikti jau esamą pirminį įsilaužimą ir nusikaltėlių veiksmus kompiuterių tinkle.**

Ataskaitinių metų rezultatai

- Išlaikyti egzaminai:
  - Duomenų analizės strategijos ir sprendimų priėmimas (prof. habil. dr. Gintautas Dzemyda).
  - Optimizavimo metodai ir jų taikymai (prof. habil. dr. Leonidas Sakalauskas).
  - Atpažinimo teorija (prof. habil. dr. Kazys Kazlauskas, dr. Gintautas Tamulevičius).

- Atlikta literatūros apžvalga dirbtinio intelekto metodų taikymo įsiskverbimų į kompiuterinius tinklus aptikimo sistemose tematika.

Dėkoju už dėmesį