Vilniaus universitetas

Matematikos ir informatikos institutas

INFORMATIKOS INŽINERIJA (07 T)

DIRBTINIO INTELEKTO METODŲ TAIKYMAS ĮSISKVERBIMŲ Į KOMPIUTERIUS TINKLUS APTIKIMO SISTEMOSE

Doktorantas Liudas Ališauskas

2017 m. spalis

Mokslinė ataskaita MII-DS-07T-xx-1

VU Matematikos ir informatikos institutas, Akademijos g. 4, Vilnius LT-08663

www.mii.lt

Santrauka

Ataskaitoje pateikiama 2016 – 2017 metais atliktos apžvalgos rezultatai. Buvo išanalizuoti pagrindiniai kompiuterių tinklo srautų duomenys, jų gavybos būdai ir sprendimai. Siekiant gauti kompiuterių tinklo duomenis gali pasinaudoti jau sukurtomis technologijomis kai 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 bus siaurinamas akcentuojantis į kibernetinės atakos horizontalus judėjimas (angl. Lateral movement) etapą, siekiant aptikti jau esamą pirminį įsilaužimą ir nusikaltėlių veiksmus kompiuterių tinkle.

Reikšminiai žodžiai: Kibernetinis saugumas, Kompiuterių tinklai, Anomalijos, Dirbtinio intelekto metodai.

Turinys

1. Įvadas

Šių metų Valstybės saugumo departamento (VSD, 2017) ir Krašto apsaugos ministerijos (KAM, 2017) ataskaitose teigiama, kad šalies ypatingos svarbos infrastruktūra yra aktyviai stebima, yra nuolatos bandoma į ją įsilaužti, yra fiksuoti sėkmingi tokių įsilaužimų pavyzdžiai. Daugeliu atveju įsilaužimo tikslas buvo informacijos vagystė, tačiau įsilaužus į industrinio valdymo sistemas sudaromos sąlygos fiziškai paveikti ypatingos svarbos infrastruktūrą.

Siekiant užkirsti kelia panašiems įsilaužimams yra kuriamos įvairios apsaugos sistemos. Dažnai tai skirtingo pobūdžio sistemos, orientuojamos į tam tikrų kompiuterių komunikacijos duomenų analizę. Apsaugos sistemos turinčios įsiskverbimo indikatorius (angl. Indicator of Compromise) pasižymi gebėjimu greitai aptikti kibernetines atakas (angl. Cyber attack). Apsaugos sistemos neturinčios įsiskverbimo indikatorių nėra pajėgios aptikti įsilaužimų. Sistemos, kurios kibernetinių atakų aptikimui naudoja pažangesnius metodus pasižymi gebėjimu aptikti nežinomas kibernetines atakas, tačiau tokios sistemos dažnai būna lėtos ir turi nemažą klaidingo nustatymo procentą. Vertinant skirtingų apsaugos sistemų pranašumus ir trūkumus, dažnai kombinuojami tarpusavyje kibernetinių atakų aptikimo metodai siekiant efektyvaus apsaugos sistemų veikimo.

2. 2016 – 2017 metų tyrimas

2.1 Tyrimo objektas

Disertacijos tyrimo objektas: Dirbtinio intelekto metodai, jų tikslumas ir efektyvumas aptinkant įsiskverbimus į kompiuterius tinklus.

2.2 Tyrimo tikslas

Disertacijos tyrimo tikslas: Pagerinti dirbtinio intelekto metodų tikslumą ir efektyvumą aptinkant įsiskverbimus į kompiuterius tinklus.

Šioje ataskaitoje apžvelgiami šioje srityje jau atlikti tyrimai, vertinami tyrimų gauti rezultatai. Nustatyti duomenų, reikalingų siekiant vykdyti įsiskverbimų aptikimą galimi, šaltiniai, duomenų modelis. Pateikiami dirbtinio intelekto metodų naudojamų siekiant aptikti įsiskverbimus į kompiuterius tinklus panaudojimo atvejai.

2.3 Tyrimo uždaviniai

2016 - 2017 metams kelti uždaviniai:

- Atlikti kompiuterių 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.

2.4 Tyrimo duomenys, jų gavyba

Informaciją apie tai kas vyksta kompiuterių tinkluose (angl. Computer network) gaunama analizuojant kompiuterių tinklo srautų (angl. Network flows, Network streams) duomenis. Kompiuterių tinklo duomenys gaunami iš kompiuterių tinklo įrenginių (angl. Network devices), tokių kaip maršrutizatorius (angl. Router), komutatorius (angl. Switch) pasinaudojant plačiai naudojamomis duomenų apie tinklo srautus išgavimo technologijomis, arba tiesiogiai nuskaitant paketus (angl. Packet capturing) kompiuterių tinkle judančius kompiuterių tinklų duomenų.

2.4.1 Tinklo srauto analizės technologijos

Pasauliniai tinklo įrenginių gamintojai tinklo srautų duomenims gauti naudoja skirtingas technologijas. Čia pateikiamos kelios kompanijos ir jų taikomos technologijos:

- Kompanijos Cisco pagaminti tinklo įrenginiai tinklo srautų duomenis išgauna ir apdoroja naudojantis kompanijos sukurta ir plačiai paplitusia NetFlow (Cisco, 2012) technologija, taip pat kompanijos Cisco vystoma nauja technologija Flexible NetFlow (Cisco, 2006).
- Kompanijos Juniper pagaminti tinklo įrenginiai tinklo srautų duomenis išgauna ir apdoroja naudojantis kompanijos sukurta technologija JFlow (Juniper, 2011).
- Kompanijos Huawei pagaminti tinklo įrenginiai tinklo srautų duomenis išgauna ir apdoroja naudojantis kompanijos sukurta technologija NetStream (HUAWEI, 2012).

Be tinklo įrangos gamintojų autonomiškai vystomų savo tinklo srautų technologijų, plačiai paplitusi yra kompanijos InMon sukurta sFlow (sFlow, 2003) technologija. Pastebėtina, kad daugelyje skirtingų gamintojų tinklo įrenginių galima naudoti skirtingas tinklo srauto duomenų gavimo technologijomis.

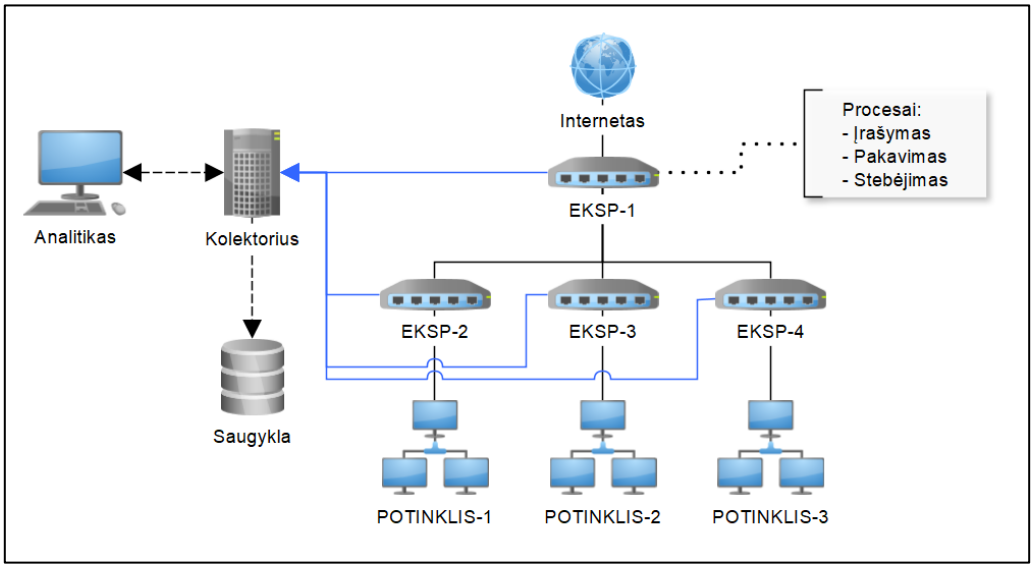
NetFlow ir JFlow technologijos savo realizavimu ir galimybėmis yra labai panašios. Abi technologijos analizuoja kiekvieną pro tinklo įrenginį praeinantį duomenų paketą, ištraukia iš duomenų paketo reikiamus duomenis, juos agreguoja, transformuoja nustatytu tinkamu formatu ir perduoda į tinklo srauto duomenų surinkimo tašką.

sFlow technologijos esminis skirtumas nuo NetFlow ir JFlow technologijų yra tai, kad čia yra analizuojamas yra tik 1 iš N per tinklo įrenginį praeinančių duomenų paketų. Taip pat galimas atsitiktinis duomenų paketų nuskaitymas, arba duomenų paketų nuskaitymas tam tikru laiko intervalu. Tokiu būdu yra sumažinamas tinklo įrangos apkrovimas, atsiranda galimybė analizuoti didelius tinklo srautus (> 1 Gbps), tačiau gaunami mažiau tikslūs tinklo duomenų srauto duomenys (Berk, 2014).

Kompanijos Cisco vystoma naujoji Flexible NetFlow (Cisco, 2006) technologija sudaro sąlygas išlaikyti NetFlow technologijos tikslumą, leidžia analizuoti 1 iš N pro tinklo įrenginį praeinantį duomenų paketą, įgalina papildomai analizuoti duomenų paketo patį turinį (angl. Payload)

Pastaruoju metu tinklo įrangos gamintojai tinklo srautų duomenų perdavimui stengiasi taikyti IPTF (angl. The Internet Engineering Task Force)[1] bendruomenės, patvirtintą IPFIX (angl. IP Flow Information Export) tinklo srauto duomenų perdavimo standartą.

Principinė visų minėtų technologijų schema pateikiama 1 paveikslėlyje. Šioje schemoje juodomis linijomis pavaizduoti tinklo duomenų komunikacijos kanalas, o mėlynomis – duomenų srautų komunikacijos kanalai tarp tinklo įrenginių, kurie atlieka duomenų gavimo funkciją (angl. Exporter) ir tinklo srauto duomenų surinkimo funkciją (angl. Collector).



1 pav. Principinė tinklo srautų analizės technologijų schema.

Tinklo srautų analizės technologijų dalyviai ir jų funkcijos (Murphy, Configuring Flexible NetFlow Export on Cisco Routers, 2014):

- Tinklo įrenginiai:
  - Skaito (angl. Records) IPv4 ir IPv6 protokolų duomenų paketus.
  - Akumuliuoja duomenų perdavimo sesijos paketą grupuodami vienakrypčius duomenų paketus turinčius vienodas reikšme šiuose laukuose:
    - Šaltinio IP adresas (angl. Source IP address)
    - Šaltinio prievadas (angl. Source port)
    - Paskirties IP adresas (angl. Destination IP address)

[1] Nuoroda: https://www.ietf.org/

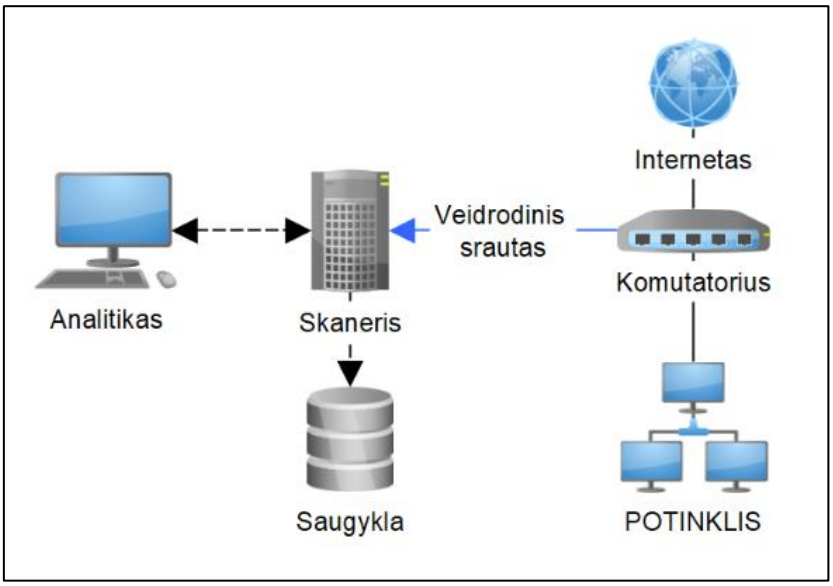
        - Paskirties prievadas (angl. Destination port)
        - Įėjimo sąsaja (angl. Ingress interface)
        - IP protokolas (angl. IP protocol)
        - IP paslaugos tipas (angl. IP Type of Service)
    - Pasibaigus duomenų perdavimo sesijai, arba nutraukus sesijos agregavimą, kopijuoja tam tikras nuskaitytų duomenų paketų parametrų reikšmes į tinklo srauto duomenų paketą, apskaičiuoja papildomas duomenų perdavimo sesijos reikšmės (neapsiribojant):
        - Sesijos pradžios ir pabaigos laikas.
        - Sesijos trukmė milisekundėmis.
        - Perduotų paketų skaičius sesijos metu.
        - Sesijos paketo dydis baitais.
        - Sesijos dydis baitais.
    - Pakuoja (angl. Exports) duomenis į tinklo srauto duomenų paketus pagal naudojamą šabloną (NetFlow, IPFIX, SFlow, JFlow).
    - Stebi (angl. Monitors) įrenginio tinklo sąsajas ir taiko duomenų surinkimo taisykles.
- Gavėjai:
    - Kaupia ir saugo tinklo srauto duomenis saugykloje (angl. Flow storage).
    - Atlieka analizę, arba teikia duomenis analitikos sistemoms.

Tinklo srautų analizės technologijos pirmiausiai buvo sukurtos siekiant stebėti kompiuterių tinklų veikimą, modeliuoti duomenų srautus. Vėliau šie duomenys buvo sėkmingai panaudoti kompiuterių tinklų saugumui užtikrinti.

2.4.2 Tiesioginė duomenų paketų analizė

Bet apžvelgtų tinklo srauto analizės technologijų galima ir tiesioginė tinklo duomenų paketų analizė. Tokios technologijos kaip tcpdump ir libpcap[2] biblioteka leidžia tinkle esančiam specialiam įrenginiui nuskaityti visus į šio įrenginio tinklo sąsajas pasiekiančius duomenų paketus. Siekiant didesnio efekto, toks įrenginys jungiamas prie tinklo įrenginio palaikančio tinklo prievado veidrodžio (angl. Port mirroring) technologiją. Šio sprendimo dėka sudaromos sąlygos paketus skaitančiam įrenginiui nuskaityti visus per tinklo įrenginį, prie kurio prisijungta, keliaujančius kompiuterių tinklo duomenų paketus. Principinė tokio sprendimo schema pateikiama 2 paveikslėlyje.

[2] Nuoroda: http://www.tcpdump.org/



2 pav. Principinė tinklo srauto nuskaitymo schema.

Gautų tinklo duomenų konvertavimas į tinklo srautų duomenis galimas programinės įrangos pagalba. Viena tokių – Argus[3].

Pagal statistinių duomenų klasifikavimą, tinklo srauto duomenų objektus sudaro skaitiniai (angl. Numerical data), kategoriniai (angl. Categorical data) parametrai, jie yra sekos duomenys (angl. Sequence data), turintys laiko žymes (angl. Time series).

2.5 Įsiskverbimai į kompiuterių tinklus

Remiantis NIST organizacijos apibrėžimu - kibernetine ataka yra laikoma ataka per kibernetinę erdvę, išnaudojant organizacijų kibernetinę erdvę su tikslu sutrikdyti, išjungti, sunaikinti ar neleistinai kontroliuoti aplinką ir infrastruktūrą; sugadinti organizacijos duomenis; pavogti organizacijos informaciją (Kissel, 2013). Kibernetinės atakos dažniausiai yra vykdomos nuosekliai (Brewer, 2017):

1 etapas: **Žvalgyba** (angl. Reconnaissance) – Šio etapo metu nustatinėjami potencialūs atakos objektai, kuriuos išnaudojus būtų pasiekti išsikelti tikslai. Nustačius naudojamas apsaugos sistemas, susipažinus su infrastruktūra, parenkami atitinkamos atakos priemonės.

2 etapas: **Pirminis įsilaužimas** (angl. Initial compromise) – Šio etapo metu atakuojantys įveikia naudojamas apsaugos sistemas ir patenka į kompiuterio tinklo vidų per įsilaužtą įrenginį ar naudotojo paskyrą.

[3] Nuoroda: https://qosient.com/argus/

3 etapas: **Vadovavimas ir valdymas** (angl. Command & control) – kompromituotas įrenginys naudojamas kaip taškas, į kurį nusikaltėliai atsisiunčia papildomus įrankius (dažniausiai nuotolinės prieigos programas (angl. remote-access Trojan).

4 etapas: **Horizontalus judėjimas** (angl. Lateral movement) – Sukūrus ne vieną prieigos kanalą nusikaltėliai siekia užvaldyti daugiau įrenginių. Kadangi nusikaltėliai veikia vidinių naudotojų vardu – jų veiklą yra sudėtinga aptikti.

5 etapas: **Taikinių užvaldymas** (angl. Target attainment) – Šiuo etapo metu nusikaltėliai jau tu užvaldę daug tinklo įrenginių, pilnai žino tinklo infrastruktūrą, gali užvaldyti didžiąją dalį įrenginių.

6 etapas: **Duomenų ištraukimas, sistemų sugadinimas ir sutrikdymas** (angl. Exfiltration, corruption, and disruption) – Tai paskutinis etapas, kurio metu žala įmonės veiklai didėja eksponentiškai ir priklauso nuo nusikaltėlių turėtų tikslų.

Visų minėtų etapų metu nusikaltėliai gali naudoti įvairius kibernetinių atakų metodus ir įrankius. Žemiau pateikiami tik keli galimi:

- Viso tinklo skenavimas (angl. Scanning) siekiant pažinti infrastruktūrą.
- Tinklo įrenginių prievadų skenavimas (angl. Port scanning) siekiant nustatyti įrenginių teikiamas paslaugas, naudojamas programas.
- Tinklo srautų nukreipimas per apgaulingus DNS (angl. Domain Name Service) serverius riekiant nuskaityti tinklo srautų duomenis.

Renkant tinklo srautų duomenis, kiekviena tokios veiklos komunikacijos pėdsakai įregistruojama tinklo srautų duomenų registre ir tampa objektu tolimesnei analizei.

2.6 Dirbtinio intelekto metodai

2.6.1 Kompiuterių tinklo veiklos požymiai

Dirbtinio intelekto metodai kompiuterių tinklo apsaugoje pasitelkiami tada, kai nepakanka taisyklėmis paremtų saugos sprendimų (Moore, 2017). Tai realizuojama aptinkant anomalijas kompiuterių tinklų veikloje analizuojant įvairius veiklos šablonus:

- 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 skenavimo stebėjimas.
- Atsisakymo aptarnauti ir Paskirstyto atsisakymo aptarnauti atakų (angl. Distributed denial of service) aptikimas.
- Robotizuotų kompiuterių tinklų (angl. Botnet) plitimo aptikimas.

2.6.2 Anomalijos

Kompiuterių tinklų veikloje anksčiau dar nematytų duomenų struktūrų aptikimas (angl. Novelty detection), leidžia išskirti anomalijas. Anomalijomis (angl. Anomaly) yra laikomos struktūros, šablonai duomenyse, kurie neatitinka tiksliai apibrėžtų normalaus elgesio sąvokų (Chandola, Banerjee, & Kumar, 2009).

Pagrindinės anomalijų kategorijos (Chandola, Banerjee, & Kumar, 2009):

- Taško anomalijos (angl. Point anomalies), kaip vienas duomenų objektas laikomas anomalija lyginant su visais kitais objektais.
- Kontekstinės anomalijos (angl. Contextual anomalies):
  - Kontekstiniai požymiai.
  - Elgsenos požymiai.
- Rinkinio anomalija (angl. Collective anomaly). Kai susijusių duomenų egzempliorių rinkinys yra anomalus viso duomenų rinkinio atžvilgiu.

2.6.3 Metodai naudojami anomalijų aptikimui

Esminiai anomalijų aptikimo metodai (Chandola, Banerjee, & Kumar, 2009):

- Paremti klasifikavimu (angl. Classification-based).
- Paremti artimiausių kaimynų (angl. Nearest neighbor-based).
- Paremti klasterizavimu (angl. Clustering-based).
- Paremti statistika (angl. Statistical based).

Anomalijų aptikimo metodai veikia trimis veiksenomis:

- Prižiūrimas anomalijos aptikimas (angl. Supervised Anomaly Detection). Metodas remiasi duomenų žymėmis, kai duomenys pateikiami kartu su normalios ir anomalios klasės žymėmis. Visi nežymėti duomenys yra lyginami su žinomomis klasės ir priskiriami vienai jų. Problemos: (1) anomalios klasės egzempliorių dažniausiai būna mažiau nei normalios veiklos klasės; (2) Tikslių ir reprezentatyvių žymių gavyba yra sudėtinga, kartais tam naudojami dirbtiniai anomalijų generavimo metodai.
- Pusiau prižiūrimas anomalijos aptikimas (angl. Semi supervised Anomaly Detection). Metodas remiasi tik vienos iš klasių pateikimu, dažniausiai normalios veiklos klase

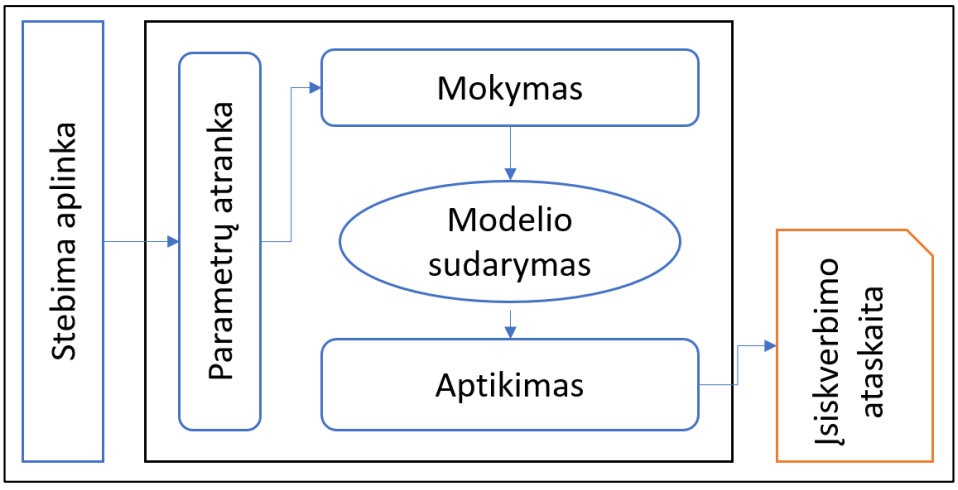
pažymėtus duomenis. Taip atpažinimo metodai vertina duomenis pagal normalios veiklos požymius. Šis metodas plačiau naudojamas, nei prižiūrimo aptikimo metodas.

- Neprižiūrimas anomalijos aptikimas (angl. Unsupervised Anomaly Detection). Šiam metodui nereikia iš anksto sužymėtų mokymo duomenų. Šios kategorijos metodai paremti prielaida, kad didžioji duomenų dalis yra iš normalios veiklos ir tik keletas egzempliorių yra anomalūs. Esant skirtingai situacijai – šios kategorijos anomalijų atpažinimo metodai generuoja daug klaidingai teigiamų (angl. False positive) rezultatų.

Prižiūrimo ir pusiau prižiūrimo anomalijų aptikimo dirbtinio intelekto metodų sužymėtų mokymo duomenų gavyba yra vienas didesnių iššūkių.

Mokymui galima pasinaudoti viešai internete prieinamais sužymėtais tinklo srautų duomenis iš „CTU-13“ duomenų rinkinio (Zunino, Grill, Stiborek, & Garcia, 2014). Rinkinį viešai publikuoja Čekijos respublikos technikos universitetas (CTU). Taip pat CTU universitetas publikuoja ir kitus panašius duomenų rinkinius, kuriuose surinkta kompiuterių tinklų normalios komunikacijos, foninės ir kenkėjiškos veiklos komunikacijos pavyzdžiai.

Apibendrinta principinė anomalijomis pagrįstos įsiskverbimo aptikimo sistemos (angl. Anomaly based Network Intrutiom Detection System, A-NIDS) pagal Garcia Teodoroa (Garcıa Teodoroa, Dıaz Verdejoa, & G. Macia Fernandeza, 2009) schema pateikiama 3 paveikslėlyje.



3 pav. Principinė anomalijomis pagrįstos įsiskverbimo aptikimo sistemos schema

Šiame modelyje:

- Stebima aplinka siunčia duomenis į A-NIDS.
- Atrenkami duomenų parametrai naudojami analizei ir mokymui.
- Sudaromi anomalijų aptikimo algoritmų normalios ir anomalios veiklos modeliai.
- Vykdomas anomalijų aptikimas.
- Generuojama anomalijos / įsiskverbimo į kompiuterių tinklus atskaita.

Sistemoje be statistika paremtų (angl. Statistical based) ir žiniomis paremtų (angl. Knowledge based) taikomi šie dirbtinio intelekto metodais paremtos A-NIDS schemos:

Bajeso tinklai (angl. Bayesian networks). Šis 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.

Tipiškai dirbtinio intelekto metodai anomalijas kompiuterių tinkluose vertina taip:

- Balais (angl. Scores). Vertinimo metodai priskiria kiekvienam duomenų egzemplioriui įvertinimą tam tikroje skalėje. Tokiu atveju analitikas gali pasirinkti ir gyliau tirti tik tam tikrą balą turinčius egzempliorius, arba nustatyti rėžio (angl. cut off) ribą, kurią peržengus egzemplioriai automatiškai laikomi anomaliais.
- Žymėmis (angl. Labels). Šios kategorijos metodai klasifikuoja testinius duomenis jiems priskirdami vieną iš dviejų žymių: (1) normalūs; (2) anomalūs.

3. Rezultatai ir išvados

Šiame tyrime buvo išanalizuoti pagrindiniai kompiuterių tinklo srautų duomenys, jų gavybos būdai ir sprendimai. Siekiant gauti kompiuterių tinklo duomenis gali pasinaudoti jau sukurtomis technologijomis kai 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 bus siaurinamas akcentuojantis į kibernetinės atakos horizontalus judėjimas (angl. Lateral movement) etapą, siekiant aptikti jau esamą pirminį įsilaužimą ir nusikaltėlių veiksmus kompiuterių tinkle.

4. Literatūra.

1. Berk, V. (2014 m. 02 06 d.). *The NetFlow / sFlow® / CFlow / JFlow Flow Dilemma*. (FlowTrack) Paimta 2017 m. 09 15 d. iš FlowTrack: https://www.flowtraq.com/the-netflowsflowcflowjflow-flow-dilemma/
2. Brewer, R. (2017 m. 03 06 d.). *The six stages of a cyber attack lifecycle*. Paimta 2017 m. 08 11 d. iš Helpnetsecurity: https://www.helpnetsecurity.com/2017/03/06/cyber-attack-lifecycle/
3. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *41*(3).
4. Cisco. (2006 m. 06 19 d.). *Cisco IOS Flexible NetFlow Technology Q&A*. (Cisco) Paimta 2017 m. 09 05 d. iš Cisco: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/flexible-netflow/prod_qas0900aecd804be091.html
5. Cisco. (2012). Introduction to Cisco IOS® NetFlow.
6. Garcıa Teodoroa, P., Dıaz Verdejoa, J., & G. Macia Fernandeza, E. V. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. *computers & security*, 18-28.
7. HUAWEI. (2012). *NetStream (Integrated) Technology White Paper* (T. 01). HUAWEI TECHNOLOGIES CO., LTD.
8. Juniper. (2011). *Juniper flow monitoring*. Juniper Networks, Inc.
9. KAM. (2017). *2016 metų Nacionalinio kibernetinio saugumo būklės ataskaita.* Vilnius: KAM.
10. Kissel, R. L. (2013). *Glossary of Key Information Security Terms*. NIST.
11. Kumar. (2005). Parallel and distributed computing for cybersecurity. *6*.
12. Moore, K. (2017 m. 01 03 d.). *Artificial Intelligence to the Rescue: The Race Against Cyber Crime is Lost Without AI*. Nuskaityta iš sparkcognition: https://sparkcognition.com/2017/01/race-cyber-crime-lost-without-ai/
13. Murphy, J. (2014 m. 04 30 d.). *Configuring Flexible NetFlow Export on Cisco Routers*. (FlowTrack) Paimta 2017 m. 09 15 d. iš FlowTrack: https://www.flowtraq.com/configuring-flexible-netflow-export-cisco-routers/
14. Murphy, J. (2014 m. 07 10 d.). *Configuring J-Flow Export on Juniper SRX-Series Routers*. (FlowTraq) Paimta 2017 m. 09 15 d. iš FlowTraq: https://www.flowtraq.com/configuring-j-flow-export-juniper-srx-series-routers/
15. sFlow. (2003). *Traffic Monitoring using sFlow*. sFlow.org.
16. VSD. (2017). *Grėsmių nacionaliniam saugumui vertinimas.* Vilnius: VSD. Paimta 2017 m. 02 15 d. iš Lietuvos Respublikos valstybės saugumo departamentas: http://www.vsd.lt/Page.aspx?pageID=269
17. Zunino, A., Grill, M., Stiborek, H., & Garcia, S. (2014). An empirical comparison of botnet detection methods. *Computers and Security Journal*(45), p. 100-123.