Univerzita Komenského v Bratislave

Fakulta matematiky, fyziky a informatiky

Mikuláš Pataky

Autoreferát dizertačnej práce

Heterogénny bezpečnostný systém

na získanie akademického titulu philosophiae doctor

v odbore doktorandského štúdia:

9.2.1 Informatika

Miesto a dátum:

Bratislava 2017

(**2. strana autoreferátu**)

Dizertačná práca bola vypracovaná v dennej forme doktorandského štúdia

na Katedre aplikovanej informatiky

Predkladateľ: RNDr. Mikuláš Pataky
Katedra aplikovanej informatiky
Fakulta matematiky, fyziky a informatiky
Univerzita Komenského
Mlynská dolina
842 48 Bratislava

Školiteľ: doc. RNDr. Damas Gruska PhD.
Katedra aplikovanej informatiky
Fakulta matematiky, fyziky a informatiky
Univerzita Komenského
Mlynská dolina
842 48 Bratislava

9.2.1. Informatika, Informatika
.....
(študijný odbor) (názov študijného programu doktorandského štúdia)

Predseda odborovej komisie:
prof. RNDr. Rastislav Kráľovič, PhD.
Fakulta matematiky, fyziky a informatiky
Univerzita Komenského
Mlynská dolina
842 48 Bratislava

Úvod do problematiky

Počet používateľov internetu a lokálnych sietí narastá nelineárnym tempom každý deň. Dôsledkom tohto faktu je existencia množstva hrozieb, ktoré sa snažia o sprístupnenie súkromných alebo tajných informácií ako hesiel, dát alebo o poškodenie či zneužitie používateľa iným spôsobom. Terajšie generácie sieťových zariadení dovoľujú monitorovanie štruktúrovaného prehľadu prevádzky siete v reálnom čase. Informácie z takéhoto monitorovania poskytujú rôzne technológie. Najznámejšie a najviac rozšírené technológie tohto typu sú NetFlow od CISCO a sFlow od InMon. Obe umožňujú sledovať jednotlivé toky v sieťach.

Informácie poskytnuté z NetFlow alebo sFlow môžu byť použité aj na rozpoznanie sieťového útoku. Najfrekventovanejšie sieťové útoky môžeme podľa článku (viď.[25]) rozdeliť na tri hlavné skupiny:

Porušenie pravidiel súkromia – kompromitovanie dôverných informácií;

Pozmenenie informácie – kompromitovanie integrity dát;

Útoky vedúce k odmietnutiu servisu – DOS alebo DDOS útoky spôsobujú nedostupnosť alebo nespoľahlivosť sieťovej infraštruktúry, kompromitujú dostupnosť zdrojov.

Ochrana siete aj kvôli spomenutým útokom je viac než vítaná, ak má byť sieť dlhodobo v poriadku a má byť bezpečná. Problém ochrany siete vyžaduje monitorovanie reálne distribuovaných používateľov a komunikácií medzi nimi.

Podstata tejto práce tkvie v návrhu multiagentového heterogénneho systému na detekciu narušenia v sieti M-AHIDS (Multi-Agent Heterogenus Intrusion Detection System), ktorý je založený na analyzovaní informačných tokov vznikajúcich v sieťovej komunikácii. Podobné systémy bývajú výsledkom niekoľko ročnej tímovej práce. Avšak, my sa neobmedzíme iba na návrh, ale niektoré kľúčové komponenty implementujeme a dlhodobo odskúšame v praxi, čím overíme ich použiteľnosť.

Hlavným prínosom M-AHIDS je integrácia viacerých formalizmov informačných tokov a techník na detekciu anomality, nový typ detekčného agenta, mašinéria muti-agentnej temporálnej logiky, agrumentácie s hybridnou negociáciou a odhadom budúcich stavov pomocou regrasných metód. Každá detekčná technika je reprezentovaná vlastnosťami špecifického autonómneho detekčného agenta, ktorý analyzuje vymedzený typ informačného toku a každý agent determinuje dôveryhodnosť všetkých agregovaných spojení.

Pôvodnú inšpiráciu pre náš systém sme našli v projekte CAMNEP (viď.[141;143]). Na rozdiel od nášho systému sú všetky agenty v CAMNEP systéme separátnymi systémami na odhaľovanie narušenia a projekt CAMNEP sa snaží spojiť ich výsledky v jeden dôveryhodnejší výsledok. My sme sa rozhodli pre iný prístup k danej problematike.

Náš systém sa bude skladať z agentov, ktoré sú založené na analyzovaní informačného toku a sú tak jednoduché, ako je to len možné. Vyvinuli sme aj inovatívnu metódu odhaľovania narušenia, ktorá podľa našich najlepších znalostí nebola ešte nikým vytvorená ani navrhnutá. Túto metódu implementujeme do agenta s názvom *Web agent*. Web agent je schopný určiť dôveryhodnosť host-ov z informačných tokov vznikajúcich pri aktivite na webových stránkach. Táto metóda je založená na našom prvotnom projekte k tejto práci – De-anonymizovanie používateľa internetu (viď.[132–134]), ktorý bol vyše dvoch rokov nasadený na webových stránkach Univerzity Komenského v Bratislave a všetkých jej fakultách.

Okrem informácii pre analýzu Web agenta, systém sprostredkúva údaje o návštevách pre univerzitné Centrum Informačných Technológií (CIT) a umožňuje získanie prehľadu presného správania sa používateľov stránok. Tieto informácie môžu byť nesmierne cenné pre vývoj univerzitných stránok. Web agent patrí medzi signifikantné výhody nášho systému.

Jedným zo základných problémov v multiagentových systémoch je problém negociácie medzi jednotlivými agentmi. Tento problém nastáva v prípade, keď nejaké agenty majú opačné názory/výsledky o niečom. V našom prípade o dôveryhodnosti/neškodnosti konkrétneho sieťového spojenia. Tento problém sa pokúsime vyriešiť vyvinutím špeciálnej mašinérie multiagentovej temporálnej logiky (M-ATL) a argumentačného frameworku. Spojenie týchto techník implementujeme do *Logického agenta*, ktorý bude posledným stupňom v hierarchii rozhodovania a určí, či je dané spojenie časťou narušenia alebo nie. M-ATL nám umožní zbierať výsledky zo všetkých detekčných agentov z minulosti aj budúcnosti. Všetky minulé odhalenia narušenia budú pre M-ATL minulé stavy a pre výpočet budúcich stavov použijeme predikčné metódy časových radov z aktuálnych a minulých spojení.

V práci sme na niektorých miestach uprednostnili anglický originálny názov pred slovenským prekladom pre jednoznačnosť a zrozumiteľnosť textu.

Ciele práce

Práca si dáva niekoľko na seba nadväzujúcich cieľov:

- Spracovať, analyzovať a prezentovať problematiku systémov na detekciu narušenia so zameraním sa na sieťové typy takýchto systémov,
- spracovať, analyzovať a prezentovať problematiku formalizmov zaoberajúcich sa skrytými kanálmi v informačných tokoch,
- navrhnúť, implementovať a otestovať systém využívajúci skryté kanály pre odkrytie anonymity používateľa internetu,
- spracovať, analyzovať a prezentovať problematiku logických formalizmov využiteľných pri budovaní systému na detekciu narušenia,
- navrhnúť, implementovať a otestovať unikátny systém na detekciu narušenia s využitím poznatkov a analýz z predchádzajúcich cieľov.

Najdôležitejšie prínosy

Najdôležitejšie prínosy nášho výskumu prezentovaného v tejto práci sú: Integrácia niekoľkých diferentných techník založených na analyzovaní informačných tokov vhodných na odhaľovanie anomálií/narušení implementovaných v podobe agentov; Mašinéria multiagentovej temporálnej logiky; Odhad budúcich stavov pomocou regresných modelov; Hybridný spôsob negociácie tvorený argumentáciou a inšpiráciou biologických imunitných buniek; Nový inovatívny detekčný agent – Web agent, ktorý je schopný určiť dôveryhodnosť host-ov z ich aktivity na webových stránkach.

Organizácia práce

Práca je rozdelená do dvoch dielov s ôsmimi kapitolami nasledovne: Prvý diel je venovaný teoretickým východiskám a súčasným riešeniam, na ktorých sa naša práca zakladá, a je rozdelený do troch kapitol.

V prvej kapitole sa budeme venovať komplexnej analýze problému odhaľovania narušení v sieti, ktorý sa delí na viacero subproblémov. Zameriame sa najmä na sedem hlavných problémov, ktoré sa budú v tejto práci riešiť, a ktoré sú kľúčové pre správne riešenie IDS: **Problém narušenia v sieti**, **Problém umiestenia**, **Problém architektúry**, **Problém predspracovania**, **Problém detekcie**, **Problém reprezentovania** a **Problém zhody**. Všetky subproblémy popíšeme a načrtneme ich možné riešenie.

Druhá kapitola sa zaoberá širokým záberom teoretických prístupov, ktoré majú úzku súvislosť so systémami IDS. Niektoré z nich priamo využívame v našom systéme M-AHIDS, ktorý podrobne popíšeme v druhom diely, ostatné nás inšpirovali k našemu unikátnemu riešeniu. Táto kapitola tvorí základnú teoretickú bázu tejto práce a v následných častiach práce využívame poznatky v nej formulované. Nakoľko princíp bezpečnosti založenej na absencii či nízkej úrovni informačného toku je kľúčovým v našej práci, uvádzame tu rôzne jeho formulácie a formalizácie, a to i pre rôzne výpočtové modely. Ukazuje sa totiž, že techniky vyvinuté pre ten ktorý formalizmus a aplikáciu, môžu nájsť uplatnenie aj pre úplne inú aplikáciu a iný formalizmus. V úvode kapitoly uvedieme, prečo štandardné techniky ako kontrola prístupu, resp. šifrovanie, nedokážu uchovať úplnú dôvernosť informácií. V ďalších podkapitolách sa venujeme informačnému toku. Najprv uvedieme rôzne aspekty informačného toku pre imperatívne jazyky. Následne sa venujeme informačnému toku vo viacvláknových imperatívnych jazykoch, kde ukážeme aj riešenia tohto problému. Ďalej opíšeme výpočtové modely, v ktorých možno uvažovať s informačným tokom a dva príklady existujúcich riešení, v podobe programovacích a overovacích jazykov, úniku informácií cez nežiadúci informačný tok. Venujeme sa aj kvantifikácii informačného toku a možnostiam utajovania informácií v databáze. Tieto techniky využívame v našom deanonymizačnom projekte. Kapitola pokračuje časťou o multiagentovej paradigme a jej výhodami tohto umelointeligentného prístupu pri riešení IDS. Nasledujúce časti sa zaoberajú modálnymi logikami. Tu sme sa zamerali najmä na epistemické a temporálne logiky. V ďalšej časti sa už venujeme výstavbe formalizmu M-ATL, ktorý priamo zapracujeme do M-AHIDS. Na záver kapitoly opíšeme časové rady, ktorými riešime výpočet budúcich stavov.

V tretej kapitole práce predstavíme prístupy na detekciu narušenia, ich prednosti a nedostatky. V úvode kapitoly zmienime niekoľko dôležitých bodov z histórie IDS. Popíšeme technológie a postupy, ktoré sa používajú pri vývoji a implementácií takýchto systémov. Pokračujeme uvedením dôležitosti takýchto systémov, ako aj o možných hrozbách. Všeobecne popíšeme základné typy týchto systémov aj s konkrétnymi príkladmi. V nasledujúcich podkapitolách sa venujeme analýze siete a metódam tejto analýzy. Venujeme sa predovšetkým aktuálne využívaným technológiám a prístupom, ktoré sú pre prácu najzaujímavejšie. Ďalej podrobne popíšeme systém CAMNEP, kde načrtneme aj význam používaných agentov. V závere kapitoly uvedieme niekoľko ďalších inšpirujúcich projektov pre náš výskum.

Druhý diel sa venuje samotnému riešeniu systému na zachytávanie narušení v sieti a je rozdelený do piatich kapitol.

Štvrtá kapitola pojednáva o základných myšlienkach, na ktorých je náš M-AHIDS postavený. M-AHIDS je založený na analyzovaní informačných tokov vznikajúcich v sieťovej komunikácii. Hlavným prínosom M-AHIDS je integrácia viacerých formalizmov in-

formačných tokov a techník na detekciu anomality, nový typ detekčného agenta, mašinéria multi-agentnej temporálnej logiky, agrumentácie s hybridnou negociáciou a odhadom budúcich stavov pomocou regresných metód. Každá detekčná technika je reprezentovaná vlastnosťami špecifického autonómneho detekčného agenta, ktorý analyzuje vymedzený typ informačného toku a každý agent determinuje dôveryhodnosť všetkých agregovaných spojení.

V piatej kapitole sa budeme venovať návrhu nášho systému M-AHIDS na odhaľovanie narušení v sieti. Navyše, neostávame len pri návrhu, ale niektoré kľúčové komponenty sme implementovali a dlhodobo vyskúšali v praxi, čím sme overili ich použiteľnosť. Úplná implementácia komplexného systému na odhaľovanie narušenia v sieti, ktorým podľa návrhu M-AHIDS je, by bola výsledkom niekoľkoročnej tímovej práce. Podobné kapacity sme k dispozícii nemali a z tohto dôvodu sme implementovali len niektoré kľúčové časti navrhnutého systému M-AHIDS. M-AHIDS je multiagentový heterogénny systém na odhaľovanie narušení (viď.[135]). Podstata systému je založená na niekoľkých nezávislých detekčných metódach, ktoré hľadajú medzi jednotlivými komunikačnými spojeniami skryté informačné toky. Odhalené informačné toky nám umožňujú určiť, či je nejaké spojenie súčasťou narušenia alebo nie. V prvej časti kapitoly sa budeme venovať architektúre systému, kde rozoberieme základný návrh jednotlivých častí, ako aj technológie a procesy, ktoré v systéme M-AHIDS používame. V druhej časti sa venujeme anonymite používateľa v internete a de-anonymizačným technikám, ktoré využívame v našom *Web agente*.

Šiesta kapitola sa venuje jednotlivým agentom, ktoré tvoria jadro M-AHIDS. Naše agenty sme vyvinuli a budovali ako jednoduché autonómne entity, v ktorých je implementovaná niektorá metóda pre detekciu narušenia zo vznikajúcich informačných tokov. Ani jeden agent nie je samostatný IDS. Výsledný agent pre konečné určenie narušenia – logický agent, využíva logickú mašinériu temporálnej logiky s argumentačným frameworkom. Snažili sme sa vyvinúť agenty, ktoré pokrývajú svojimi analýzami čo najširšiu množinu rôznych informačných tokov, ktoré vznikajú pri sieťovej komunikácii. Pri tvorbe agentov sme využili aj prehľadový článok, v ktorom autori (viď.[179]) spracovali 55 štúdií o detekčných agentov. Nakoľko neuvádzajú ich presné výsledky a ani pôvodné články nemajú jednotnú metriku miery úspešnosti, nevedeli sme vybrať všeobecne najlepšie, ale pokúsili sme vytvoriť naše agenty tak, aby zahŕňali detekciu pre čo možno najviac hrozieb. V ďalších častiach tejto kapitoly podrobne opíšeme jednotlivé agenty, ktoré v M-AHIDS využívame, ako aj základné princípy, na ktorých sú postavené dva najvýznamnejšie agenty: *Web agent* a *Logický agent*.

Predposledná kapitola sa zaoberá technickými detailami implementácie a testovania M-AHIDS. Na začiatku kapitoly popíšeme, v akom prostredí a na akých technológiách je M-AHIDS postavený. Rozoberieme aj implementačnú štruktúru riešenia do siedmich projektov. Ďalej sa v kapitole venujeme experimentom, ktorými sme M-AHIDS podrobili. Vo všeobecnosti vieme naše experimenty rozdeliť podľa spracovávaných dát do dvoch skupín: Online a Offline. Online experiment tvorí nasadenie M-AHIDS na katedrovej sieti, kde zisťuje narušenia z dát poskytovaných sFlow. Druhý typ experimentov – Offline bol vykonaný na dvoch benchmarkoch: DARPA dataset a KDD99 cup dataset. Záver kapitoly patrí úpravám M-AHIDS pre jednotlivé benchmarky.

V poslednej ôsmej predstavíme dosiahnuté výsledky z našich projektov: De-anonymizácia používateľov v internete a nášho systému na odhaľovanie narušení v sieti M-AHIDS. Následne tu pre plynulosť čitateľnosti textu ostatných častí práce uvádzame rozsiahlejšie výsledky z týchto projektov.

Závery a výsledky

Predkladaná práca sa zaoberá návrhom a implementáciou systému na odhaľovanie narušení v sieti a problémami s tým spojenými. Nakoľko kompletná implementácia navrhnutého komplexného systému M-AHIDS by bola výsledkom niekoľkoročnej tímovej práce, venovali sme sa predovšetkým návrhu systému. Avšak, neobmedzili sme sa iba naň a niektoré kľúčové komponenty sme implementovali a vyskúšali dlhodobo v praxi, čím sme overili ich použiteľnosť.

Najvýznamnejšími časťami pri tvorbe systému bolo preskúmanie viacerých aspektov bezpečnosti založených na informačných tokoch, riešenie negociácie v multiagentovom systéme a vytvorenie vlastnej detekčnej metódy v podobe Web agenta.

Na začiatku práce sme sa podrobne venovali analýze komplexného problému odhaľovania narušení v sieti. Tento problém sme rozdelili do siedmych hlavných podproblémov: Problém narušenia v sieti, Problém umiestenia, Problém architektúry, Problém predspracovania, Problém detekcie, Problém reprezentovania a Problém zhody. Pri analýze sme vychádzali zo všeobecných poznatkov o vývoji systému, ako aj z existujúcich riešení systémov na odhaľovanie narušení. V každom probléme sme uviedli dôležité vlastnosti, ktoré musí spĺňať riešenie daného problému. Výsledkom analýzy je súbor podmienok, ktoré musia použité metódy a celkové riešenie spĺňať.

Ďalej sme prehľadne uviedli problematiku informačného toku. Zaviedli sme súvisiace pojmy a ich význam pre bezpečnosť. Na rozdiel od explicitného informačného toku, ktorý priamo prenáša informácie, a teda nespôsobuje pre svoju ľahkú detekciu problémy v bezpečnosti systémov, spôsobujú implicitné informačné toky, ktoré vyzrádzajú privátne informácie, ťažšie problémy pre detekciu.

V práci sme rozčlenili informačné toky do viacerých kategórií podľa ich druhu, pričom sme sa venovali aj informačným tokom spôsobeným viacvláknovými programami. Popísali sme rôzne prístupy, ktoré riešia tento problém. Pomocou informačných tokov sme zisťovali možné narušenia v sieti, pričom sme vyhodnocovali široké spektrum metód a techník za účelom zabezpečenia dostatku relevantných poznatkov.

Ďalšou nevyhnutnou súčasťou východiskovej bázy boli možnosti merania informačných tokov. Tieto metriky majú značný význam v systémoch, ktoré z podstaty svojej funkčnosti musia povoliť nežiaduci informačný tok. Tieto metriky a spôsoby na utajovanie údajov v databázach sme využívali v nami vytvorenom de-anonymizačnom projekte, v ktorom zisťujeme, okrem iného, utajenosť prehliadačov v internete.

V nasledujúcej časti práce sme zhrnuli a predstavili význam neklasických logík, ktoré nám pri riešení nášho výskumu boli nápomocné. Zamerali sme sa najmä na modálnu logiku a jej deriváty – temporálnu a epistemickú logiku. Tieto logiky spolu umožňujú usudzovať nad znalosťami aj s využitím časového priestoru. Uviedli sme dva konkrétne príklady využitia logík. Ďalej sme popísali možnosti riešenia negociácie v multiagentovom systéme.

Porovnávaním viacerých možností modálnych logík sme dospeli k záveru, že pre naše využitie a splnenie podmienok analýzy je najvhodnejšia paradigma temporálnej logiky, a to pre presnejšie a univerzálnejšie detekovanie narušenia bezpečnosti v heterogénnom bezpečnostnom systéme. Získané znalosti sme využili pre vytvorenie špeciálneho multiagentového temporálneho formalizmu M-ATL a argumentačného framework-u, ktoré boli použité v logickom agente nášho M-AHIDS.

V nadväznosti na východiskové teoretické vymedzenie tejto práce sme preskúmavali možnosti systémov na detekciu narušenia v sieti. Uviedli sme základné typy takýchto sys-

témov spolu s ich predstaviteľmi. Zistili sme, že pre efektívny prístup k tejto problematike je multiagentový systém vhodným riešením z dôvodu využitia viacerých detekčných techník v jednom systéme, čo bolo potvrdené aj viacerými z uvedených systémov, ktoré boli navrhnuté a implementované v multiagentovej paradigme.

Podrobnejšie sme sa zamerali na komplexný multiagentový systém pre detekciu škodlivej komunikácie – CAMNEP. Základom tohto systému sú rôzne detekčné techniky v podobe agentov. Každý z nich reaguje na iné podnety, a tak ovplyvňuje celkový trust model komunikácie. Týmto spôsobom je možné dosiahnuť relevantné výsledky, ktoré uľahčujú spravovanie siete.

V tomto systéme sa využívajú ako agenty samostatné detekčné systémy, ktoré budujú model dôvery sieťového toku. Pomocou tohto modelu sa potom následne rozhodne, ktoré sieťové toky sú narušenia a ktoré nie. Podľa našich poznatkov nevyužívajú logické mechanizmy medzi jednotlivými agentmi. Uvedený systém tvoril základnú ideu pre vývoj agentov v našom projekte M-AHIDS, avšak líšime sa v dvoch zásadných veciach:

1. Naše agenty sú jednoduché autonómne entity, v ktorých je implementovaná niektorá metóda pre detekciu narušenia zo vznikajúcich informačných tokov. Žiadny agent nie je schopný vykonávať samostatne úlohy IDS, ako je tomu v projekte CAMNEP.

2. Výsledný agent pre konečné určenie narušenia - Logický agent - využíva logickú mašinériu temporálnej logiky s argumentačným frameworkom, na rozdiel od budovania modelu dôveryhodnosti.

Po preskúmaní vyššie uvedených formalizmov sme navrhli a implementovali systém na odhaľovanie narušenia v sieti. Najvýznamnejšími prínosmi nášho multiagentového systému M-AHIDS sú:

- Integrácia šiestich typov techník pre zisťovanie narušenia v sieti pomocou informačných tokov. Každá technika je reprezentovaná jedným alebo viacerými agentmi.

- Inovatívny Web agent, ktorý je schopný rozpoznať dôveryhodného hosta z aktivity na webových stránkach univerzity. Tento agent je založený na našom prvotnom projekte ohľadne bezpečnosti, ktorý bol nepretržite nasadený na všetkých stránkach Univerzity Komenského dlhšie ako jeden rok a osem mesiacov.

- Spolu 15 detekčných agentov. Každý v samostatnom vlákne.

- Mašinéria multiagentovej temporálnej logiky.

- Hybridná negociácia agentov s argumentáciou a váhami dôvery inšpirované biologickým imunitným systémom.

Následne, ako sme systém natrénovali a otestovali, M-AHIDS považoval iba 3 percentá škodlivých spojení za normálne spojenia a dosiahli sme 36,40 percentnú mieru úspešnosti vo false positives v škodlivých spojeniach. Tento výsledok môže byť pre nás uspokojivý, nakoľko projekt CAMNEP[143] má pri 1 percentnom false negatives 40 percent false positives. S ostatnými projektami sme náš systém nevedeli porovnať na online dátach, nakoľko buď ich autori vo svojich článkoch neuvádzajú presné miery úspešnosti alebo používajú úplne inú metriku merania, ktorú sme nevedeli v našom systéme napodobniť.

Nakoľko ale porovnanie na online dátach, ktoré sú vždy iné, nie je úplne vierohodné, podrobili sme M-AHIDS aj testom na benchmarkoch DARPA a KDD99. Aj v týchto

testoch náš systém uspel na úrovni, ktorú môžeme považovať za uspokojivú. M-AHIDS dosiahol v meraných mierach úspešnosti na DARPA benchmarku: Detection Rate = 93,1; False Positive = 8,8; Accurancy = 92,3. Na KDD99 dátovej mnoažine Detection Rate = 91,9; False Positive = 9,1; Accurancy = 91,1. Pričom IDS systémy na KDD99 dátovej množine dosahujú výsledky Detection Rate: 83% - 98%; False Positive: 1% - 20%; Accurancy: 85% - 97%.

Výsledky nášho výskumu o de-anonymizácii poukazujú na to, že ľubovoľná web stránka môže (s pomerne dobrou presnosťou) identifikovať prehliadač používateľa internetu, resp. v niektorých prípadoch zistiť jeho históriu. Náš systém dokázal počas jednoročného nasadenia jednoznačne identifikovať 2/3 prehliadačov. V porovnaní s inými podobnými projektami (viď [49] a [198]), sme dosiahli menšiu úspešnosť. Tento fakt môže byť spôsobený nasadením systému v akademickej sfére, kde sa nachádza pomerne veľa zhodných počítačov. Ďalším dôvodom môže byť, že uvedené projekty zobrazujú výsledky spred niekoľkých rokov a dnes si vývojári prehliadačov dávajú ešte viac záležať na rýchlej a častej aktualizácii, ktorá môže ovplyvňovať naše výsledky.

Účinnosť takéhoto systému môže závisieť aj od konkrétnej web stránky, pre akých používateľov s akými prehliadačmi je zaujímavá. Ak stránka zaujme používateľov s ojedinelými prehliadačmi, či so špeciálnymi rozšíreniami, je vysoká pravdepodobnosť veľmi dobrej účinnosti systému.

Takéto identifikovanie prehliadača sa dá následne jednoducho prepojiť aj s ďalšími informáciami, ktoré na internete poskytujeme. Napríklad prepojenie prehliadača a sociálnej siete či e-mailového účtu by umožňovalo zistenie komplexných informácií o danom používateľovi internetu, od jeho osobných údajov až po jeho aktivity v internete.

V závere práce sme zhrnuli najvýznamnejšie výsledky a uviedli najrozsiahlejšie rezultáty našich projektov.

Vybrané čiastočne výsledky práce boli už publikované. Predpokladáme, že po získaní ďalších dát a skúseností, po nutnom dlhodobejšom nasadení a testovaní a po prípadnom dolaďovaní systému, budeme publikovať ďalšie výsledky a skúsenosti.

Literatúra

[1] M. K. A. V. Jones, A. Lomuscio and W. Penczek. Parametric computation tree logic with knowledge. In *Concurrency, Specification and Programming (CS&P 2011)*, pages 286–300, Pułtusk, Poland, 2011. Proceedings of the international workshop CS&P 2011.

[2] A. Abbasi, J. Wetzels, W. Bokslag, E. Zambon, and S. Etalle. On emulation-based network intrusion detection systems. In A. Stavrou, H. Bos, and G. Portokalidis, editors, *Research in Attacks, Intrusions and Defenses*, volume 8688 of *Lecture Notes in Computer Science*, pages 384–404. Springer International Publishing, 2014.

[3] E. Ábrahám and C. Palamidessi, editors. *Formal Techniques for Distributed Objects, Components, and Systems - 34th IFIP WG 6.1 International Conference, FORTE 2014, Held as Part of the 9th International Federated Conference on Distributed Computing Techniques, DisCoTec 2014, Berlin, Germany, June 3-5, 2014. Proceedings*, volume 8461 of *Lecture Notes in Computer Science*. Springer, 2014.

[4] W. L. Al-Yaseen, Z. A. Othman, and M. Z. A. Nazri. Real-time intrusion detection system using multi-agent system. *IAENG International Journal of Computer Science*, 43(1):80–90, 2016.

[5] Alexa. The top 500 sites on the web @ONLINE. `http://www.alexa.com/topsites/global`, Sept. 2012.

[6] M. S. Alvim, M. E. Andrés, and C. Palamidessi. Entropy and attack models in information flow - (invited talk). In C. S. Calude and V. Sassone, editors, *IFIP TCS*, volume 323 of *IFIP Advances in Information and Communication Technology*, pages 53–54. Springer, 2010.

[7] J. P. Anderson. Computer security threat monitoring and surveillance. Technical report, James P. Anderson Co., Fort Washington, Pennsylvania, 1980.

[8] R. Anderson and R. Needham. Programming satan's computer. In *in Computer Science Today*, pages 426–440. Springer-Verlag, 1995.

[9] L. Andrej. Multiagentové systémy. Katedra Aplikovanej Informatiky, Fakulta Matematiky, Fyziky a Informatiky, Univerzita Komenského. Bratislava.

[10] M. Arnao, C. Smutz, A. Zollman, A. Richardson, and E. Hutchins. Laika boss: Scalable file-centric malware analysis and intrusion detection system. *Lockheed Martin Corporation*, 2015.

[11] A. S. Ashoor and P. S. Gore. Importance of intrusion detection system (ids). *International Journal of Scientific & Engineering Research*, 2011.

[12] Awio. Global web stats @ONLINE. `http://www.w3counter.com/globalstats.php`, Aug. 2012.

[13] M. Balliu, M. Dam, and G. Le Guernic. Epistemic temporal logic for information flow security, 2011.

[14] J. Barnes. *High Integrity Software: The SPARK Approach to Safety and Security*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2003.

[15] G. Barthe, T. Rezk, R. Russo, and A. Sabelfeld. Security of multithreaded programs by compilation. In *In Proc. 12th European Symposium on Research in Computer Security*, pages 2–18. Springer-Verlag, 2007.

[16] K. Bartos and M. Rehak. Distributed self-organized collaboration of autonomous ids sensors. In *Dependable Networks and Services*, pages 113–117, Heidelberg, 2012. Springer.

[17] K. Bartos and M. Rehak. Trust-based solution for robust self-configuration of distributed intrusion detection systems. In *In Proceedings of the 20th European Conference on Artificial Intelligence (ECAI)*, pages 121–126. IOS Press, 2012.

[18] J. G. Bazan, M. Szpyrka, A. Szczur, L. Dydo, and H. Wojtowicz. Classifiers for behavioral patterns identification induced from huge temporal data. In *Proceedings of the 23th International Workshop on Concurrency, Specification and Programming, Chemnitz, Germany,*

September 29 - October 1, 2014., pages 22–33, 2014.

[19] N. Benyettou, A. Benyettou, V. Rodin, and S. Y. Berrouiguet. The multi-agents immune system for network intrusions detection (MAISID). *Oriental Journal Of Computer Science & Technology*, 6(4):383–390, December 2013.

[20] P. Besnard and A. Hunter. *Elements of Argumentation*. The MIT Press, 2008.

[21] N. C. Bianchi and G. Lugosi. On prediction of individual sequences. Economics Working Papers 324, Department of Economics and Business, Universitat Pompeu Fabra, July 1998.

[22] P. e. a. Blackburn. *Handbook of Modal Logic, Volume 3 (Studies in Logic and Practical Reasoning)*. Elsevier Science, 2006.

[23] J. Boubeta-Puig, G. Ortiz, and I. Medina-Bulo. Medit4cep. *Know.-Based Syst.*, 89(C):97–112, Nov. 2015.

[24] K. Boudaoud and Z. Guessoum. A multi-agents system for network security management. In *SMARTNET 2000, 6th IFIP Conference on Intelligence in Networks, September 18-22, 2000, Vienna, Austria*, Vienna, AUSTRIA, 09 2000.

[25] K. Boudaoud, H. Labiod, Z. Guessoum, and R. Boutaba. Network security management with intelligent agents. In *NOMS 2000, IEEE/IFIP Network Operations and Management Symposium, 08-14 avril 2000, Honolulu, Hawaii*, Honolulu, UNITED STATES, 04 2000.

[26] I. Boureanu, M. Cohen, and A. Lomuscio. Automatic verification of temporal-epistemic properties of cryptographic protocols. *Journal of Applied Non-Classical Logics*, pages 463–487, 2009.

[27] P. Braun, J. Brzostowski, G. Kersten, J. Kim, R. Kowalczyk, S. Strecker, and R. Vahidov. e-negotiation systems and software agents: Methods, models, and applications. In *Intelligent Decision-making Support Systems*, Decision Engineering, pages 271–300. Springer London, 2006.

[28] J. W. Bryans, M. Koutny, and P. Y. A. Ryan. Modelling opacity using petri nets. *Electron. Notes Theor. Comput. Sci.*, 121:101–115, February 2005.

[29] A. Burns, B. Dobbing, and T. Vardanega. Guide for the use of the ada ravenscar profile in high integrity systems. *Ada Lett.*, XXIV:1–74, June 2004.

[30] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. *ACM TRANSACTIONS ON COMPUTER SYSTEMS*, 8:18–36, 1990.

[31] I. Butun, I.-H. Ra, and R. Sankar. An intrusion detection system based on multi-level clustering for hierarchical wireless sensor networks. *Sensors*, 15(11):28960, 2015.

[32] A. Campan, T. M. Truta, and N. Cooper. P-sensitive k-anonymity with generalization constraints. *Trans. Data Privacy*, 3(2):65–89, Aug. 2010.

[33] O. Can and O. K. Sahingoz. A survey of intrusion detection systems in wireless sensor networks. In *Modeling, Simulation, and Applied Optimization (ICMSAO), 2015 6th International Conference on*, pages 1–6. IEEE, 2015.

[34] V. Ciriani, S. D. C. di Vimercati, S. Foresti, and P. Samarati. *k*-anonymity. In *Secure Data Management in Decentralized Systems*, pages 323–353. Springer US, 2007.

[35] D. Clark, S. Hunt, and P. Malacaria. A static analysis for quantifying information flow in a simple imperative language. *J. Comput. Secur.*, 15(3):321–371, Aug. 2007.

[36] M. R. Clarkson, A. C. Myers, and F. B. Schneider. Quantifying information flow with beliefs. *J. Comput. Secur.*, 17(5):655–701, Oct. 2009.

[37] M. R. Clarkson and F. B. Schneider. Quantification of integrity. In *Proceedings of the 23rd IEEE Computer Security Foundations Symposium, CSF 2010, Edinburgh, United Kingdom, July 17-19, 2010*, pages 28–43. IEEE Computer Society, 2010.

[38] M. Cohen, M. Dam, A. Lomuscio, and F. Russo. Abstraction in model checking multi-agent systems. In *Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems - Volume 2*, AAMAS '09, pages 945–952, Richland, SC, 2009.

International Foundation for Autonomous Agents and Multiagent Systems.

[39] J. Crampton and C. Morisset. Ptacl: A language for attribute-based access control in open systems. *CoRR*, abs/1111.5767, 2011.

[40] M. Cresswell and G. Hughes. *A New Introduction to Modal Logic*. Routledge, London, 1996.

[41] P. Das and R. Niyogi. A temporal logic based approach to multi-agent intrusion detection and prevention. In *International Journal of Communication Network & Security*, volume 1, pages 53–61, 2011.

[42] F. Dechesne, S. Orzan, and Y. Wang. Refinement of kripke models for dynamics. In *Proceedings of the 5th international colloquium on Theoretical Aspects of Computing*, pages 111–125, Berlin, Heidelberg, 2008. Springer-Verlag.

[43] F. Dechesne and Y. Wang. To know or not to know: epistemic approaches to security protocol verification. *Synthese*, 177:51–76, 2010. 10.1007/s11229-010-9765-8.

[44] S. Delaune, S. Kremer, and M. D. Ryan. Verifying privacy-type properties of electronic voting protocols. *Journal of Computer Security*, 17(4):435–487, July 2009.

[45] R. A. DeMillo, N. A. Lynch, and M. J. Merritt. Cryptographic protocols. In *Proceedings of the fourteenth annual ACM symposium on Theory of computing*, STOC '82, pages 383–400, New York, NY, USA, 1982. ACM.

[46] H. V. Ditmarsch. The russian cards problem: a case study in cryptography with public announcements. Technical report, Department of Computer Science, University of Otago, 2002.

[47] H. V. Ditmarsch, W. van der Hoek, and B. Kooi. Playing cards with hintikka - an introduction to dynamic epistemic logic, 2004.

[48] P. M. Dung. On the acceptability of arguments and its fundamental role in nonmonotonic reasoning, logic programming and n-person games. *Artif. Intell.*, 77(2):321–357, Sept. 1995.

[49] P. Eckersley. How unique is your web browser? In *Proceedings of the 10th international conference on Privacy enhancing technologies*, PETS'10, pages 1–18, Berlin, Heidelberg, 2010. Springer-Verlag.

[50] s. ELET. Absolútny rebríček @ONLINE. `http://naj.sk/Rebricek/2012/09/`, Sept. 2012.

[51] L. Ertöz, E. Eilertson, A. Lazarevic, P. N. Tan, V. Kumar, J. Srivastava, and P. Dokas. *MINDS - Minnesota Intrusion Detection System*, chapter 3, page 21. MIT Press, 2004.

[52] R. Fagin and J. Y. Halpern. Reasoning about knowledge and probability: preliminary report. In *Proc. Second Conference on Theoretical Aspects of Reasoning about Knowledge*, pages 277–293. Morgan Kaufmann, 1988.

[53] R. Fagin, J. Y. Halpern, Y. Moses, and M. Y. Vardi. *Reasoning about Knowledge*. MIT Press, 1995.

[54] P. Faratin. *Automated Service Negotiation Between Autonomous Computational Agents*. PhD thesis, University of London, Queen Mary and Westfield College, Department of Electronic Engineering, 2000.

[55] S. S. Fatima, M. Wooldridge, and N. R. Jennings. Multi-issue negotiation under time constraints. In *Proceedings of the First International Joint Conference on Autonomous Agents and Multiagent Systems: Part 1*, AAMAS '02, pages 143–150, New York, NY, USA, 2002. ACM.

[56] M. Feder, N. Merhav, and M. Gutman. Correction to 'universal prediction of individual sequences' (jul 92 1258-1270). *IEEE Transactions on Information Theory*, 40(1):285, 1994.

[57] E. W. T. Ferreira, A. A. Shinoda, V. E. N. Ruy De Oliveira, and N. V. D. S. Araújo. A methodology for building a dataset to assess intrusion detection systems in wireless networks. *WSEAS TRANSACTIONS on COMMUNICATIONS*, 14(16):113–120, 2015.

[58] R. Focardi and R. Gorrieri. Classification of security properties (part i: Information flow).

Revised versions of lectures given during the IFIP WG 17 International School on Foundations of Security Analysis and Design on Foundations of Security Analysis and Design Tutorial Lectures, 2171:331–396, 2001.

[59] R. Focardi, R. Gorrieri, and F. Martinelli. Information flow analysis in a discrete-time process algebra. In *Computer Security FoundationWorkshop*, pages 170–184, July 2000.

[60] R. Focardi, R. Gorrieri, and F. Martinelli. Real-time information flow analysis. *IEEE Journal on Selected Areas in Communications*, 21(1):20–35, 2003.

[61] R. Focardi, R. Gorrieri, and F. Martinelli. Classification of security properties (part ii: Network security). *Methods*, 2946(September):139–185, 2004.

[62] S. Frau, R. Gorrieri, and C. Ferigato. Formal aspects in security and trust. In P. Degano, J. Guttman, and F. Martinelli, editors, *Formal Aspects in Security and Trust*, chapter Petri Net Security Checker: Structural Non-interference at Work, pages 210–225. Springer-Verlag, Berlin, Heidelberg, 2009.

[63] J. Fu, H. G. Tanner, and J. Heinz. Concurrent multi-agent systems with temporal logic objectives: game theoretic analysis and planning through negotiation. *IET Control Theory Applications*, 9(3):465–474, 2015.

[64] R. Gad, M. Kappes, J. Boubeta-Puig, and I. Medina-Bulo. Employing the CEP paradigm for network analysis and surveillance. In *Proceedings of The Ninth Advanced International Conference on Telecommunications*, page 204–210, Rome, Italy, 2013. IARIA, IARIA.

[65] A. Galton. Temporal logic. In E. N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Stanford University, fall 2008 edition, 2008.

[66] S. Ganapathy, P. Vijayakumar, Y. Palanichamy, and A. Kannan. An intelligent crf based feature selection for effective intrusion detection. *Int. Arab J. Inf. Technol.*, 13(1):44–50, 2016.

[67] J. Garson. Modal logic. In E. N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Stanford University, winter 2009 edition, 2009.

[68] B. Gedik and L. Liu. Protecting location privacy with personalized k-anonymity: Architecture and algorithms. *IEEE Transactions on Mobile Computing*, 7(1):1–18, 2008.

[69] H. Gemal. Browserspy.dk @ONLINE. `http://browserspy.dk/`, Sept. 2012.

[70] M. R. Genesereth and N. J. Nilsson. *Logical foundations of artificial intelligence*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 1987.

[71] E. Gerds. Browser plugin detection with plugindetect @ONLINE. `http://www.pinlady.net/PluginDetect/`, Sept. 2012.

[72] Google. The 1000 most-visited sites on the web @ONLINE. `http://www.google.com/adplanner/static/top1000/`, Sept. 2012.

[73] D. P. Gruska. Network information flow. *Fundam. Inf.*, 72:167–180, April 2006.

[74] D. P. Gruska. Observation based system security. *Fundam. Inform.*, 79(3-4):335–346, 2007.

[75] D. P. Gruska. Process algebra contexts and security properties. *Fundam. Inform.*, 102(1):63–76, 2010.

[76] D. P. Gruska. Informational analysis of security and integrity. *Fundam. Inform.*, 120(3-4):295–309, 2012.

[77] D. P. Gruska and A. Maggiolo-Schettini. Process algebras for network communication. *Fundam. Inf.*, 45:359–378, January 2001.

[78] J. Y. Halpern. Using reasoning about knowledge to analyze distributed systems. *Annual Reviews of Computer Science*, 2:37–68, 1987.

[79] J. Y. Halpern and R. Fagin. Modelling knowledge and action in distributed systems. *Distributed Computing*, 3:159–179, 1988.

[80] J. Y. Halpern and Y. Moses. Knowledge and common knowledge in a distributed envi-

ronment. In *Proceedings of the third annual ACM symposium on Principles of distributed computing*, PODC '84, pages 50–61, New York, NY, USA, 1984. ACM.

[81] J. Y. Halpern and Y. Moses. A guide to the modal logics of knowledge and belief: preliminary draft. In *Proceedings of the 9th international joint conference on Artificial intelligence - Volume 1*, pages 480–490, San Francisco, CA, USA, 1985. Morgan Kaufmann Publishers Inc.

[82] J. Y. Halpern and M. Y. Vardi. *Model checking vs. theorem proving: a manifesto*, pages 151–176. Academic Press Professional, Inc., San Diego, CA, USA, 1991.

[83] V. Hendricks and J. Symons. Epistemic logic. In E. N. Zalta, editor, *The Stanford Encyclopedia of Philosophy*. Stanford University, spring 2009 edition, 2009.

[84] J. Hintikka. *Knowledge and Belief: An Introduction to the Logic of the Two Notions*. Cornell University Press, 1962.

[85] M. Huisman and H.-C. Blondeel. Model-checking secure information flow for multi-threaded programs. In S. Mödersheim and C. Palamadessi, editors, *Proceedings of the Joint Workshop on Theory of Security and Applications, TOSCA 2011, Saarbruecken, Germany*, volume 6993 of *Lecture Notes in Computer Science*, pages 148–165, Berlin, March 2011. Springer Verlag.

[86] M. Huth and M. Ryan. *Logic in Computer Science: Modelling and Reasoning about Systems*. Cambridge University Press, New York, NY, USA, 2004.

[87] inMon. sFlowTool. `http://www.inmon.com/technology/sflowTools.php`.

[88] M. J.-J. *Modal Logics for Intelligent Agents*. Utrecht University, Institute of Information and Computing Sciences, Intelligent Systems Group, P.O. Box 80.089, 3508 TB Utrecht, The Netherlands, 2004.

[89] W. Jamroga. A temporal logic for stochastic multi-agent systems. In *Intelligent Agents and Multi-Agent Systems, 11th Pacific Rim International Conference on Multi-Agents, PRIMA 2008, Hanoi, Vietnam, December 15-16, 2008. Proceedings*, pages 239–250, 2008.

[90] A. Janc and L. Olejnik. Feasibility and real-world implications of web browser history detection, 2010.

[91] J. P. John, F. Yu, Y. Xie, M. Abadi, and A. Krishnamurthy. Searching the searchers with searchaudit. In *Proceedings of the 19th USENIX conference on Security*, USENIX Security'10, pages 9–9, Berkeley, CA, USA, 2010. USENIX Association.

[92] J. P. John, F. Yu, Y. Xie, A. Krishnamurthy, and M. Abadi. deseo: combating search-result poisoning. In *Proceedings of the 20th USENIX conference on Security*, SEC'11, pages 20–20, Berkeley, CA, USA, 2011. USENIX Association.

[93] J. P. John, F. Yu, Y. Xie, A. Krishnamurthy, and M. Abadi. Heat-seeking honeypots: design and experience. In *Proceedings of the 20th international conference on World wide web*, WWW '11, pages 207–216, New York, NY, USA, 2011. ACM.

[94] M. Kacprzak, M. Dziubinski, and K. Budzynska. Strategies in dialogues: A game-theoretic approach. In *Computational Models of Argument - Proceedings of COMMA 2014, Atholl Palace Hotel, Scottish Highlands, UK, September 9-12, 2014*, volume 266 of *Frontiers in Artificial Intelligence and Applications*, pages 333–344. IOS Press, 2014.

[95] K. Knorr. Multilevel security and information flow in petri net workflows. Technical report, In: Proceedings of the 9th International Conference on Telecommunication Systems - Modeling and Analysis, Special Session on Security Aspects of Telecommunication Systems, 2001.

[96] K. Konolige. A deductive model of belief. In *Proceedings of the Eighth international joint conference on Artificial intelligence - Volume 1*, pages 377–381, San Francisco, CA, USA, 1983. Morgan Kaufmann Publishers Inc.

[97] M. Korayem and D. J. Crandall. De-anonymizing users across heterogeneous social computing platforms. *The 7th international aaai conference on weblogs and social media (ICWSM*

2013), 2013.

[98] S. Kramer. *Logical Concepts in Cryptography*. PhD thesis, ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE, 2007.

[99] S. Kraus, K. Sycara, and A. Evenchik. Reaching agreements through argumentation: a logical model and implementation. *Artificial Intelligence*, 104(1–2):1 – 69, 1998.

[100] S. A. Kripke. Semantical analysis of modal logic i. normal propositional calculi. *Zeitschrift fur mathematische Logik und Grundlagen der Mathematik*, 9:67–96, 1963.

[101] S. A. Kripke. Semantical considerations on modal logic. *Acta Philosophica Fennica*, 16:83–94, 1963.

[102] A. Lakhina, M. Crovella, and C. Diot. Diagnosing network-wide traffic anomalies. *SIGCOMM Comput. Commun. Rev.*, 34:219–230, Aug. 2004.

[103] A. Lakhina, M. Crovella, and C. Diot. Mining anomalies using traffic feature distributions. *SIGCOMM Comput. Commun. Rev.*, 35:217–228, August 2005.

[104] B. W. Lampson. A note on the confinement problem. *Commun. ACM*, 16:613–615, October 1973.

[105] N. D. Lane, J. Xie, T. Moscibroda, and F. Zhao. On the feasibility of user de-anonymization from shared mobile sensor data. In *Proceedings of the Third International Workshop on Sensing Applications on Mobile Phones*, PhoneSense '12, pages 3:1–3:5, New York, NY, USA, 2012. ACM.

[106] P. Lasek and K. Lasek. Relative constraints as features. In L. Popova-Zeugmann, editor, *Proceedings of the 23th International Workshop on Concurrency, Specification and Programming, Chemnitz, Germany, September 29 - October 1, 2014.*, volume 1269 of *CEUR Workshop Proceedings*, pages 121–125. CEUR-WS.org, 2014.

[107] W. Lee and S. J. Stolfo. A framework for constructing features and models for intrusion detection systems. *ACM Trans. Inf. Syst. Secur.*, 3(4):227–261, Nov. 2000.

[108] W. Lee, S. J. Stolfo, and K. W. Mok. A data mining framework for building intrusion detection models. In *1999 IEEE Symposium on Security and Privacy, Oakland, California, USA, May 9-12, 1999*, pages 120–132, 1999.

[109] X. Leroy, D. Doligez, A. Frisch, J. Garrigue, D. Rémy, and J. Vouillon. The objective caml system release 3.12 documentation and user's manual, 2010.

[110] N. Li and T. Li. t-closeness: Privacy beyond k-anonymity and ?-diversity. In *In Proc. of IEEE 23rd Int'l Conf. on Data Engineering (ICDE'07*, 2007.

[111] R. Lippmann, J. W. Haines, D. J. Fried, J. Korba, and K. Das. The 1999 darpa off-line intrusion detection evaluation. *Comput. Netw.*, 34(4):579–595, Oct. 2000.

[112] R. P. Lippmann, D. J. Fried, I. Graf, J. W. Haines, K. R. Kendall, D. McClung, D. Weber, S. E. Webster, D. Wyschogrod, R. K. Cunningham, and M. A. Zissman. Evaluating intrusion detection systems: The 1998 darpa off-line intrusion detection evaluation. *discex*, 2:1012, 2000.

[113] A. Lomuscio and F. Raimondi. Mcmas: A model checker for multi-agent systems. In *Proceedings of TACAS 2006*, pages 450–454. Springer Verlag, 2006.

[114] G. Lowe. Quantifying information flow. In *Proceedings of the 15th IEEE Workshop on Computer Security Foundations*, CSFW '02, pages 18–, Washington, DC, USA, 2002. IEEE Computer Society.

[115] X. Luo, P. Zhou, E. W. W. Chan, R. K. C. Chang, and W. Lee. A combinatorial approach to network covert communications with applications in web leaks. In *Proceedings of the 2011 IEEE/IFIP 41st International Conference on Dependable Systems&Networks*, DSN '11, pages 474–485, Washington, DC, USA, 2011. IEEE Computer Society.

[116] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam. L-diversity: Privacy beyond k-anonymity. *ACM Trans. Knowl. Discov. Data*, 1(1), Mar. 2007.

[117] L. A. Maglaras. A novel distributed intrusion detection system for vehicular ad hoc networks. *International Journal of Advanced Computer Science and Applications (IJACSA)*, 6(4):101–106, 2015.

[118] B. Mahapatra and S. Patnaik. Self learning intrusion detection system for cross layer analysis in manets. *International Journal of Computer Science and Information Security (IJCSIS)*, 14(9):97–103, September 2016.

[119] F. Majorczyk, E. Totel, and L. Me. Experiments on cots diversity as an intrusion detection and tolerance mechanism. In *Workshop on Recent Advances on Intrusion-Tolerant Systems (WRAITS)*, March 2007.

[120] S. P. Marsh. Formalising trust as a computational concept. Technical report, Department of Computing Science and Mathematics, University of Stirling, 1994.

[121] J. Mccarthy and P. J. Hayes. Some philosophical problems from the standpoint of artificial intelligence. In *Machine Intelligence*, pages 463–502. Edinburgh University Press, 1969.

[122] J.-J. C. Meyer and W. van der Hoek. *Epistemic Logic for AI and Computer Science (Cambridge Tracts in Theoretical Computer Science)*. Cambridge University Press, 1995.

[123] J. K. Millen. Covert channel capacity. In *Proceedings of the IEEE Symposium on Security and Privacy*, page 7. IEEE Press, 1987.

[124] L. Mohammadpour, M. Hussain, A. Aryanfar, V. M. Raee, and F. Sattar. Evaluating performance of intrusion detection system using support vector machines : Review. *International Journal of Security and Its Applications (IJSIA)*, 9(9):225–234, 2015.

[125] A. C. Myers. Jflow: practical mostly-static information flow control. In *Proceedings of the 26th ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, POPL '99, pages 228–241, New York, NY, USA, 1999. ACM.

[126] A. A. Nasr, M. M. Ezz, and M. Z. Abdulmaged. An intrusion detection and prevention system based on automatic learning of traffic anomalies. *International Journal of Computer Network and Information Security(IJCNIS)*, 8(1):53–60, 2016.

[127] Netcraft. Most visited web sites @ONLINE. `http://toolbar.netcraft.com/stats/topsites?c=&submit=Refresh`, Sept. 2012.

[128] J. Newsome and D. Song. Dynamic Taint Analysis for Automatic Detection, Analysis, and Signature Generation of Exploits on Commodity Software. In *Proceedings of the Network and Distributed System Security Symposium (NDSS 2005)*, 2005.

[129] E. OSTERTAGOVÁ. Modelovanie ČasovÝch radov. *The 13th International Scientific Conference: Trends and Innovative Approaches in Business Processes "2010"*, 2010.

[130] A. Özgür and H. Erdem. A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015. *PeerJ PrePrints*, 4:e1954, 2016.

[131] S. Parsons and P. Giorgini. An approach to using degrees of belief in bdi agents. In B. Bouchon-Meunier, R. Yager, and L. Zadeh, editors, *Information, Uncertainty and Fusion*, volume 516 of *The Springer International Series in Engineering and Computer Science*, pages 81–92. Springer US, 2000.

[132] M. Pataky. Anonymita používateľa v internete. In *ITAT 2013: Information Technologies—Applications and Theory Proceedings*, pages 18–23. CreateSpace Independent Publishing Platform, 2013.

[133] M. Pataky. The anonymity of the internet user. In *Proceedings of the Scientific Conference of Technology and Innovation Processes 2013*, pages 35–41, Hradec Králové, CZ, 2013. MAGNANIMITAS.

[134] M. Pataky. De-anonymization of an internet user based on his web browser. In *CER Comparative European Research 2014 Proceedings*, pages 125–128, London, 2014. Sciemcee Publishing.

[135] M. Pataky and D. P. Gruska. Multi-agent heterogeneous intrusion detection system. In

Proceedings of the 23th International Workshop on Concurrency, Specification and Programming, Chemnitz, Germany, September 29 - October 1, 2014., pages 184–195, 2014.

[136] M. Pataky and D. P. Gruska. Analysing of M-AHIDS with future states on DARPA and KDD99 benchmarks. In *Proceedings of the 25th International Workshop on Concurrency, Specification and Programming, Rostock, Germany, September 28-30, 2016.*, pages 153–164, 2016.

[137] J. Patel and M. K. Panchal. Effective intrusion detection system using data mining technique. *Journal of Emerging Technologies and Innovative Research (JETIR)*, 2(6):1869–1878, Jun 2015.

[138] Y. qian Zhang and L. wan Chan. Forenet: Fourier recurrent networks for time series prediction. In *In Proceedings of International Conference on Neural Information Processing, ICONIP 2000, Korea*, 2000.

[139] I. Rahwan, S. Ramchurn, N. R. Jennings, P. McBurney, S. Parsons, and L. Sonenberg. Argumentation-based negotiation. *The Knowledge Engineering Review*, 18(4):343–375, 2003.

[140] M. Rehak, M. Grill, and J. Stiborek. On the value of coordination in distributed self-adaptation of intrusion detection system. In *Proceedings Web Intelligence and Intelligent Agent Technology WI-IAT11*, pages 196–203, Los Alamitos, CA, 2011. IEEE Computer Soc.

[141] M. Rehak, M. Pechoucek, K. Bartos, M. Grill, P. Celeda, and V. Krmicek. Camnep: An intrusion detection system for high-speed networks. *Progress in Informatics*, 5(5):65–74, March 2008.

[142] M. Rehak, M. Pechoucek, P. Celeda, V. Krmicek, M. Grill, and K. Bartos. Multi-agent approach to network intrusion detection (demo paper). In M. Padgham, Parkes and Parsons, editors, *Proc. of 7th Int. Conf. on Autonomous Agents and Multiagent Systems (AAMAS 2008)*. IFAMAS, 2008.

[143] M. Rehák, M. Pechoucek, M. Grill, J. Stiborek, K. Bartoš, and P. Celeda. Adaptive multiagent system for network traffic monitoring. *IEEE Intelligent Systems*, 24(3):16–25, 2009.

[144] M. Rehák and M. Pěchouček. Trust modeling with context representation and generalized identities. In *Proceedings of the 11th international workshop on Cooperative Information Agents XI*, CIA '07, pages 298–312, Berlin, Heidelberg, 2007. Springer-Verlag.

[145] R. U. Rehman. *Intrusion Detection Systems with Snort: Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID.* Prentice Hall PTR, Upper Saddle River, New Jersey 07458, USA, 2003.

[146] I. Roy, S. T. V. Setty, A. Kilzer, V. Shmatikov, and E. Witchel. Airavat: security and privacy for mapreduce. In *Proceedings of the 7th USENIX conference on Networked systems design and implementation*, NSDI'10, pages 20–20, Berkeley, CA, USA, 2010. USENIX Association.

[147] A. Russo and A. Sabelfeld. Securing interaction between threads and the scheduler in the presence of synchronization. In *IN PROC. IEEE COMPUTER SECURITY FOUNDATIONS WORKSHOP*, pages 177–189. IEEE Computer Society, 2006.

[148] A. Russo, A. Sabelfeld, and K. Li. Implicit flows in malicious and nonmalicious code, 2009.

[149] P. Ryan and S. Schneider. *The modelling and analysis of security protocols: the csp approach.* Addison-Wesley Professional, first edition, 2000.

[150] V. V. Rybakov. Linear temporal logic $\mathrm{ltk}_{\mathrm{k}}$ extended by multi-agent logic k_{n} with interacting agents. *J. Log. Comput.*, 19(6):989–1017, 2009.

[151] A. Sabelfeld and A. C. Myers. Language-based information-flow security. *IEEE Journal on Selected Areas in Communications*, 21:15, 2003.

[152] A. Sabelfeld and D. Sands. Probabilistic noninterference for multi-threaded programs. In

Proceedings of the 13th IEEE workshop on Computer Security Foundations, pages 200–214, Washington, DC, USA, 2000. IEEE Computer Society.

[153] S. M. Sajjad and M. Yousaf. Netmids: Neighbor node trust management based anomaly intrusion detection system for wireless sensor networks. *International Journal of Computer Science and Information Security (IJCSIS)*, 14(7), July 2016.

[154] M. Salem. Mining techniques in network security to enhance intrusion detection systems. *International Journal of Network Security & Its Applications*, 4(6):51–66, nov 2012.

[155] T. Sandholm. Algorithm for optimal winner determination in combinatorial auctions. *Artificial Intelligence*, 135(1–2):1 – 54, 2002.

[156] K. Scarfone and P. Mell. Guide to intrusion detection and prevention systems (idps) recommendations of the national institute of standards and technology. *Nist Special Publication*, 800(94):94, 2007.

[157] J. Sedlák. Hlavně nenápadne. *Computer*, 18(17/11):32–34, Sept. 2011.

[158] sFlow.org. Traffic monitoring using sflow, 2003.

[159] C. Sierra, N. R. Jennings, P. Noriega, and S. Parsons. A framework for argumentation-based negotiation. In *Proceedings of the 4th International Workshop on Agent Theories, Architectures, and Languages (ATAL-97), volume 1365 of LNAI*, pages 177–192. Springer-Verlag, 1998.

[160] V. Simonet. The Flow Caml System (version 1.00): Documentation and user's manual. Technical Report 0282, INRIA, 2003.

[161] G. Smith and D. Volpano. Secure information flow in a multi-threaded imperative language. In *Proceedings of the 25th ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, POPL '98, pages 355–364, New York, NY, USA, 1998. ACM.

[162] G. Smith and D. M. Volpano. Confinement properties for multi-threaded programs. *Electr. Notes Theor. Comput. Sci.*, 20:132–142, 1999.

[163] A. Sridharan and T. Ye. Tracking port scanners on the ip backbone. In *Proceedings of the 2007 workshop on Large scale attack defense*, LSAD '07, pages 137–144, New York, NY, USA, 2007. ACM.

[164] M. Srivatsa and M. Hicks. Deanonymizing mobility traces: using social network as a side-channel. In *Proceedings of the 2012 ACM conference on Computer and communications security*, CCS '12, pages 628–637, New York, NY, USA, 2012. ACM.

[165] I. W. Stats. Internet usage statistics @ONLINE. `http://www.internetworldstats.com/stats.htm/`, 2011.

[166] R. Sterritt and M. Hinchey. Biologically-inspired concepts for autonomic self-protection in multiagent systems. In M. Barley, H. Mouratidis, A. Unruh, D. Spears, P. Scerri, and F. Massacci, editors, *Safety and Security in Multiagent Systems*, volume 4324 of *Lecture Notes in Computer Science*, pages 330–341. Springer Berlin Heidelberg, 2009.

[167] A. S. Steve Bono, Michael Brotzman, S. Small, and K. Watkins. Ban logic reading guide, October 2004.

[168] S. J. Stolfo, W. Fan, W. Lee, A. Prodromidis, , and P. K. Chan. Cost-based modeling for fraud and intrusion detection: Results from the jam project. *discex*, 2:1130, 2000.

[169] R. Sun and C. L. Giles. Sequence learning: From recognition and prediction to sequential decision making. *IEEE Intelligent Systems*, 16(4):67–70, 2001.

[170] L. Sweeney. Achieving k-anonymity privacy protection using generalization and suppression. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, 10(5):571–588, Oct. 2002.

[171] L. Sweeney. k-anonymity: a model for protecting privacy. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, 10(5):557–570, Oct. 2002.

[172] C. system. Cisco ios netflow, 2011.

[173] P. Syverson and I. Cervesato. The logic of authentication protocols. In *Foundations of Security Analysis and Design, LNCS 2171*, pages 63–136. Springer-Verlag, 2001.

[174] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani. A detailed analysis of the kdd cup 99 data set. In *Proceedings of the Second IEEE International Conference on Computational Intelligence for Security and Defense Applications*, CISDA'09, pages 53–58, Piscataway, NJ, USA, 2009. IEEE Press.

[175] R. Tewatia and A. Mishra. Introduction to intrusion detection system: Review. *International Journal of Scientific & Technology Research*, 4(5), May 2015.

[176] C. Tofallis. A better measure of relative prediction accuracy for model selection and model estimation. *JORS*, 66(8):1352–1362, 2015.

[177] M. Toulouse, B. Q. Minh, and P. Curtis. A consensus based network intrusion detection system. *CoRR*, abs/1505.05288, 2015.

[178] T. M. Truta and B. Vinay. Privacy protection: p-sensitive k-anonymity property. In *In Proc. of 22nd IEEE Int'l Conf. on Data Engineering Workshops*, page 94. IEEE Computer Society, 2006.

[179] C.-F. Tsai, Y.-F. Hsu, C.-Y. Lin, and W.-Y. Lin. Intrusion detection by machine learning: A review. *Expert Systems with Applications*, 36(10):11994 – 12000, 2009.

[180] N. Ugtakhbayar, B. Usukhbayar, and J. Nyamjav. An approach to detect tcp/ip based attack. *International Journal of Computer Science and Network Security*, 16(4):37–40, April 2016.

[181] J. van Benthem, J. Gerbrandy, and E. Pacuit. Merging frameworks for interaction: Del and etl. In *Proceedings of the 11th conference on Theoretical aspects of rationality and knowledge*, TARK '07, pages 72–81, New York, NY, USA, 2007. ACM.

[182] H. van Ditmarsch. The russian cards problem. *Studia Logica*, 75:31–62, 2003. 10.1023/A:1026168632319.

[183] J. Van Eijck. Demo—a demo of epistemic modelling. *Interactive Logic Selected Papers from the 7th Augustus de Morgan Workshop London*, page 303, 2007.

[184] O. Vaněk, Z. Yin, M. Jain, B. Bošanský, M. Tambe, and M. Pěchouček. Game-theoretic resource allocation for malicious packet detection in computer networks. In *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems - Volume 2*, AAMAS '12, pages 905–912, Richland, SC, 2012. International Foundation for Autonomous Agents and Multiagent Systems.

[185] Y. Venema, L. G. (ed, B. Guide, P. Logic, and B. Publishers. Temporal logic. In *The Blackwell Guide to Philosophical Logic. Blackwell Philosophy Guides (2001.* Basil Blackwell Publishers, 1998.

[186] S. Vijayarani and M. S. S. Intrusion detection system – a study. *International Journal of Security, Privacy and Trust Management (IJSPTM)*, 4(1), February 2015.

[187] D. Volpano, C. Irvine, and G. Smith. A sound type system for secure flow analysis. *J. Comput. Secur.*, 4:167–187, January 1996.

[188] W3Schools. Browser statistics @ONLINE. `http://www.w3schools.com/browsers/browsers_stats.asp`, Aug. 2012.

[189] Y. Wahba, E. ElSalamouny, and G. ElTaweel. Improving the performance of multi-class intrusion detection systems using feature reduction. *International Journal of Computer Science Issues IJCSI*, 3, May 2015.

[190] M. P. Websites. Most popular websites on the internet @ONLINE. `http://mostpopularwebsites.net/`, Sept. 2012.

[191] S. Whalen, N. Boggs, and S. J. Stolfo. Model aggregation for distributed content anomaly detection. In *Proceedings of the 2014 Workshop on Artificial Intelligent and Security Workshop*, AISec '14, pages 61–71, New York, NY, USA, 2014. ACM.

[192] B. W.-S. Wojciech Penczek and A. Zbrzezny. Towards sat-based bmc for ltlk over interleaved interpreted systems. In *Concurrency, Specification and Programming (CS&P 2011)*, pages 565–576, Pułtusk, Poland, 2011. Proceedings of the international workshop CS&P 2011.

[193] G. Wondracek, T. Holz, E. Kirda, and C. Kruegel. A practical attack to de-anonymize social network users. In *Proceedings of the 2010 IEEE Symposium on Security and Privacy*, SP '10, pages 223–238, Washington, DC, USA, 2010. IEEE Computer Society.

[194] M. J. Wooldridge. *The logical modelling of computational multi-agent systems*. PhD thesis, University of Manchester, UK, 1992.

[195] M. Woolridge and M. J. Wooldridge. *Introduction to Multiagent Systems*. John Wiley & Sons, Inc., New York, NY, USA, 2001.

[196] Y. Xie, F. Yu, and M. Abadi. De-anonymizing the internet using unreliable ids. *SIGCOMM Comput. Commun. Rev.*, 39(4):75–86, Aug. 2009.

[197] K. Xu, Z.-L. Zhang, and S. Bhattacharyya. Reducing unwanted traffic in a backbone network. In *Proceedings of the Steps to Reducing Unwanted Traffic on the Internet on Steps to Reducing Unwanted Traffic on the Internet Workshop*, pages 2–2, Berkeley, CA, USA, 2005. USENIX Association.

[198] T.-F. Yen, Y. Xie, F. Yu, R. P. Yu, and M. Abadi. Host Fingerprinting and Tracking on the Web: Privacy and Security Implications. In *Proceedings of the 19th Annual Network & Distributed System Security Symposium*, Feb. 2012.

[199] E. N. Zalta. Basic concepts in modal logic.

[200] A. Zbrzezny. A new translation from ectl* to sat. In *Concurrency, Specification and Programming (CS&P2011)*, pages 589–600, Pułtusk, Poland, 2011. Proceedings of the international workshop CS&P 2011.

[201] S. Zhai, C. Hu, and Z. Weiming. Multiagent distributed intrusion detection system model based on bp neural network. *International Journal of Information and Network Security (IJINS)*, 3(3), 2014.

[202] Y. Zhang. *Prediction of Financial Time Series with Hidden Markov Models [microform]*. Thesis (M.A.Sc.)–Simon Fraser University, 2005.

[203] C. z.s.p.o. Family of combo cards, 2011.

[204] R. Zuech, T. M. Khoshgoftaar, and R. Wald. Intrusion detection and big heterogeneous data: a survey. *Journal of Big Data*, 2(1):1–41, 2015.

Relevantné publikované práce

AFC Publikované príspevky na zahraničných vedeckých konferenciách Pataky, Mikuláš 100%: *De-anonymization of an internet user based on his web browser* In: CER Comparative European Research 2014: Proceedings. - London : Sciemcee Publishing, 2014. - S. 125-128. - ISBN 978-0-9928772-0-0
[CER 2014 : Comparative European Research : International Scientific Conference for Ph.D. students of EU countries. 1st, London, 17.-21.3.2014]

Pataky, Mikuláš 80% a Gruska, Damas 20%: *Multi-agent heterogeneous intrusion detection system* In: Proceedings of the 23th International Workshop on Concurrency, Specification and Programming 2014. - Chemnitz, Germany: Informatik-Bericht Nr. 245, 2014. - S. 184-195. - ISSN: 0863 - 095X
[CS&P'2014 : Concurrency, Specification and Programming : 23th International Workshop on Concurrency, Specification and Programming 2014. Chemnitz, Germany, 29.9. - 1.10.2014.]

Pataky, Mikuláš 80% a Gruska, Damas 20%: *Analysing of M-AHIDS with future states on DARPA and KDD99* In: Proceedings of the 25th International Workshop on Concurrency, Specification and Programming 2016. - Rostock, Germany: Informatik-Bericht Nr. 247, 2014. - S. 153-164. - ISSN: 0863 - 095X
[CS&P'2016 : Concurrency, Specification and Programming : 25th International Workshop on Concurrency, Specification and Programming 2016. Rostock, Germany, 28. - 30.9.2016.]

AFD Publikované príspevky na domácich vedeckých konferenciách Pataky, Mikuláš 100%: *Anonymita používateľa na internete* In: ITAT 2013 : Information Technologies Applications and Theory : Proceedings [elektronický zdroj]. - [North Charleston] : CreateSpace Independent Publishing Platform, 2013. - S. 18-23 [USB kľúč]. - ISBN 978-1490952000
[ITAT 2013 : Information Technologies Applications and Theory : Conference. 13th, Donovaly, 11.-15.9.2013]

AFH Abstrakty príspevkov z domácich vedeckých konferencií Pataky, Mikuláš 100%: *Anonymita užívatel a v internete* In: Študentská vedecká konferencia FMFI UK, Bratislava 2013 : Zborník príspevkov. - Bratislava : Fakulta matematiky, fyziky a informatiky UK, 2013. - S. 287. - ISBN 978-80-8147-009-7
[Študentská vedecká konferencia FMFI UK 2013. Bratislava, 23.4.2013]

BEE Odborné práce v zahraničných zborníkoch Pataky, Mikuláš 100%: *The anonymity of the internet user* In: Technológia Europea 2013. - Hradec Králové : Magnanimitas, 2013. - S. 35-41. - ISBN 978-80-87952-01-6
[Technológia Europea 2013 : mezinárodní vědecká konference k problematice technologických a inovačních procesů. 3., Hradec Králové, 16.-20.12.213]

Granty

UK/241/2014 Grant UK (Grant pre doktorandov a mladých vedeckých pracovníkov UK) *Bezpečnostný systém založený na formálnom prístupe* (2014)

VEGA 1/1333/12 *Knowledge representation for ambient intelligence* (2012 - 2015), člen riešiteľského kolektívu

Summary

This thesis is dedicated to the heterogeneous security system for detection of the network intrusions and it consists of solving of two problems: the problem of detection of a network intrusion, and the problem of making a singular result in multi-agent system. Basic common features of the detection methods, which solve the first established problem, are the different information flows implicitly arising in a network communication. The network connections, which have high probability of a network intrusion, are detected using the methods based on the information flow. In this connection, we are using the data acquired from our project of de-anonymization of internet user, which is deployed on all web pages of the Comenius University in Bratislava and its faculties from December 2012 to January 2015. This thesis also solves the problem of the negotiation in the multiagent system, with special multiagent temporal formalism (M-ATL) and argumentation framework based on M-ATL with inspiration from biological immune system. Results of this thesis are the proposal and partial implementation of the complex multiagent heterogeneous system for intrusion detection M-AHIDS.