Универзитет у Београду
Електротехнички факултет

НАСТАВНО-НАУЧНОМ ВЕЋУ

Предмет: Подобност теме и кандидата Мр **Yousef Abuadlla**, дипл. инж. за израду докторске дисертације

Одлуком на 765. Седници изборног и наставно-научног већа Електротехничког факултета Универзитета у Београду одржане. 03.09.2013. године и одлуком бр. 930/1 од 03.09.2013., именовани смо за чланове Комисије за оцену подобности теме и кандидата Мр **Yousef Abuadlla**, дипл. инж. за израду докторске дисертације и научне заснованости теме "Flow-Based Intrusion Detection System With Two Neural Network Stages" односно "Систем за детекцију упада заснован на токовима са две неуралне мреже"

На основу материјала приложеног уз захтев кандидата, Комисија подноси следећи

И З В Е Ш Т А Ј

1. Подаци о кандидату

1.1. Биографски подаци

Yousef Abuadlla рођен у месту Захра у Либији 1969. године. Након завршеног школовања до нивоа високе стручне спреме у Либији, наставља са успешном професионалном каријером. Влада Либије одлучује да стипендира његово даље школовање и 2001. године га шаље на магистарске студије на Универзитет у Београду, Електротехнички факултет. Ту завршава магистарске студије 06.10.2003. године. Наслов магистарске тезе је био:,,Avoiding Mutual Exclusion of Shared Data in Real-Time Operating Systems", односно "Избегавање међусобног искључивања за дељене податке у оперативним системима за рад у реалном времену" Након додатне успешне професионалне каријере, добија стипендију Либије за докторске студије на Универзитету у Београду, Електротехнички факултет. Yousef је међу најталентованијим стипендистима Владе Либије. Пред лето 2013. године, поднео је предлог теме докторске дисертације, а одлуком на 765. седници Изборног и наставно-научног већа Електротехничког факултета Универзитета у Београду одржане. 03.09.2013. године именована је Комисија за оцену подобности теме и кандидата.

1.2. Стечено научноистраживачко искуство

Магистарски рад "Избегавање међусобног искључивања за дељене податке у оперативним системима у реалном времену" припада области конкурентног и дистрибуираног програмирања. У тој области се проучавају поступци убрзавања комуникације између процеса који се паралелно извршавају. Након завршетка магистратуре, интерес кандидата се померио на област рачунарских мрежа које су инфраструктура за паралелно процесирање. Након успешног савладавања области мрежа и практичног рада на мрежним уређајима у мрежној академији при Рачунарском центру Универзитета у Београду (РЦУБ) створени су предуслови за рад на дисертацији. Сви до сада објављени радови су из области дисертације.

Објављени радови кандидата:

Међународни часописи:

1. Abuadlla Yousef, Goran Kvaščev, Slavko Gajin, Zoran Jovanovic: Flow-Based Anomaly Intrusion Detection System Using Two Stages Neural Network", Computer Science and Information Systems, ISSN: 1820-0214, Two-year impact factor (2012): 0.549, accepted for publication. M22
2. Abuadlla Yousef, Zoran Jovanovic: International Journal of Information Technology & Computer Science (IJITCS) : Issue : July / August 2012 : Internet Computing , Informatics in E-Business and applied Computing , ISSN (Online) : 2091-1610, Volume 4/Issue 2, | Pages : 46 - 52 | Publication Date : July / August 2012. M23

Међународне конференције:

Претходни рад из часописа је претходно објављен на конференцији

1. Abuadlla Yousef, Zoran Jovanovic: Flow-Based Anomaly Intrusion Detection System using Neural Network, International Conference on Internet Computing , Informatics in E-Business and applied Computing (ICIEACS 2012), Дубаи, 27-28 јул 2012., http://www.ijitcs.com/volume%204_No_2/Abuadlla+Yousef.pdf**.** M33

1.3. Оцена подобности кандидата за рад на предложеној теми

Кандидат је прошао процес усавршавања на Универзитету у Београду у току кога је достигао висок ниво предзнања неопходног за реализацију дисертације. Било је неопходно да се кандидат додатно обучи у практичном раду са мрежним уређајима, јер је то било потребно за реализацију дисертације. Како је за тему дисертације изабрана област у којој се научни резултати могу практично применити и потврдити, чињеница да је кандидат успешно обавио ту додатну обуку нас додатно уверава да може са успехом да заврши дисертацију. Кандидат већ има објављене радове из области тезе.

2. Предмет и циљ истраживања

Заштита рачунарских система и мрежа је једна од најзначајнијих области у информационо комуникационим технологијама, јер су данашњи системи рањиви. Убрзавање развоја друштва засновано на рачунарима је угрожено злонамерним нападима на рачунарске и мрежне инфраструктуре. Откривање упада и покушаја упада (напада) у рачунарске системе (intrusion detection) је кључан елемент у заштити рачунарски базираних система и сервиса заснованих на рачунарима.

Један приступ откривању упада је да се на сваком рачунару инсталирају процеси који прате системске позиве и покушавају да открију нерегуларно понашање других процеса. Други приступ је да се на неком делу мреже обједини откривање напада за све рачунаре на том делу мреже, тако што би се анализирали пакети намењени свим рачунарима на том делу мреже. Ово се назива мрежно заснованим системима за откривање упада, а софтвер којим се ради откривање се извршава на посебним машинама које учитавају пакете намењене свим рачунарима на брањеном делу мреже.

Први мрежно засновани системи за откривање упада су учитавали индивидуалне пакете и радили анализу користећи комплетне пакете. Учитавање пакета се радило са дељеног медијума мреже на коме су сви рачунари повезани на дељени медијум могли да читају пакете. Еволуција мрежа је довела до свођења броја рачунара на дељеном медијуму на минимум. Као последица, у ослушкивање саобраћаја у циљу откривања напада су се морали укључити мрежни уређаји. Истовремено је дошло до великог повећања брзине мрежа, па се анализа морала подићи на виши ниво од индивидуалних пакета који се учитавају.

За потребе надзора мрежа је у рутере уграђена могућност регистрације токова (flows). Токови укључују све пакете који имају исте изворне и одредишне адресе и имају још неке заједничке особине (нпр. протокол на слоју изнад ИП слоја, изворни и одредишни порт и тип сервиса и сл.). Токови су природан одраз интеракција између две софтверске компоненте дистрибуираног система, па се подизањем нивоа апстракције не губи много информација неопходних за детекцију упада. Како су у рутерима уграђене компоненте које региструју особине токова у току рада мреже, детекција упада помоћу токова се може остварити за мреже великог капацитета у реалном времену. Побољшање заштите рачунарских система и мрежа се значајно може поправити правовременим откривањем напада. Откривање тих напада се обавља помоћу система за откривање упада, а уколико се то ради на мрежном нивоу, основни правац је да се искористе подаци добијени из токова прикупљени од стране рутера.

Циљ тезе је да се развије систем који ће веома брзо моћи да открије нападе и да истовремено изврши класификацију напада, када се закључи да на мрежи постоји активност која одступа од нормалне. Тај систем треба да се заснива на неуралним мрежама. Већ су објављени радови везани за класификацију напада на основу токова, коришћењем неуралних мрежа, када се већ зна да постоји напад. Добијени резултати других аутора су обећавајући. Осим тога, неуралне мреже након тренинга веома брзо доносе закључке, што је неопходно код данашњих гигабитских мрежа. Међу методама за брзо откривање и класификацију напада, истраживања заснована на неуралним мрежама представљају један од главних праваца.

У истраживању ће се користити различите неуралне мреже у два степена. Први степен ће се користити за откривање нерегуларног понашања на мрежи, односно детекцију потенцијалног напада. Други степен ће се користити за класификацију типа напада. Током истраживања је потребно одредити који параметри добијени из записа токова са рутера треба да се искористе за откривање напада и класификацију. За први степен ће се тражити неурална мрежа која ће давати најбоље резултате у откривању токова који одступају од нормалног понашања. За други степен ће се испитати која неурална мрежа ће дати најбоље резултате у класификацији врсте напада.

Откривање и класификација напада помоћу неуралних мрежа је област која је изузетно актуелна и у последњој деценији се публикује велики број радова у научним часописима. За брзине данашњих рачунарских мрежа овај приступ је међу најперспективнијим. Убацивање два степена омогућава да се аутоматизовано селектују токови који су сумњиви са првим степеном и само они прослеђују до другог стрепена. На тај начин се растерећује други степен, али се истовремено детектује одступања од регуларног понашања на мрежи, чиме се потенцијално може помоћи у откривању потпуно нове врсте напада.

Очекује се да ће се на основу концепта са две неуралне мреже добити елементи комплетног система. Осим тога, испитивањем различитих врста неуралних мрежа ће се наћи оне које најбоље обављају посао за оба степена, па се очекују резултати који су бар у рангу најбољих из до сада објављених радова

Релевантни библиографски извори су многи радови објављени на међународним конференцијама и у научним часописима. У наставку је наведено неколико новијих радова из часописа.

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

V. Jyothsna, V. V. Rama Prasad, K. Munivara Prasad: A Review of Anomaly based Intrusion Detection Systems‘ International Journal of Computer Applications (0975 – 8887) Volume 28– No.7, August 2011.

[12] Xin Xu: Adaptive Intrusion Detection Based on Machine Learning: Feature Extraction, Classifier Constructionand Sequential Pattern Prediction,‘ International Journal of Web Services Practices, Vol.2, No.1-2 (2006), pp. 49-58.

Neethu B: Classification of Intrusion Detection Dataset using machine learning Approaches‘ International Journal of Electronics and Computer Science Engineering 1044 ISSN- 2277-1956, Volume 1, Issue 2, November 2012.

3. Полазне хипотезе

Полазне хипотезе су да рутери дају коректне записе за токове. Такође, пошто неуралне мреже морају да пролазе кроз поступак учења, користиће се обележени напади који су већ класификовани. Претпоставка је да су ти напади коректно класификовани (обележени). За то ће бити коришћен Darpa dataset са МИТ. Адреса на којој се налазе ти подаци је: http://www.ll.mit.edu/mission/communications/cyber/CSTcorpora/ideval/data/

Како велика већина аутора из области користи исти скуп података за процесе учења и испитивање добијених резултата, биће могуће прецизно упоредити добијене резултате са резултатима других аутора.

4. Научне методе истраживања

Развиће се софтвер којим се ради екстракција токова у случајевима када постоје обележени записи који садрже целокупне пакете (нпр. DARPA data set) и информацију о врсти напада. Одредиће се на основу особина напада који параметри токова треба да се доведу на улаз неуралних мрежа. Затим ће се пропуштати токови кроз неуралне мреже првог и другог нивоа и обезбедити њихово учење. Потом ће се пропуштати други обележени токови који нису коришћени за учење и испитати вероватноћа погађања, лажних аларма и сл. Тако ће се добити одговарајући статистички параметри. За испитане мреже ће се одредити која се понаша најбоље и резултати упоредити са релевантним резултатима из литературе.

5. <u>Очекивани научни допринос</u>

- Нови оригинални двостепени систем за детекцију упада коришћењем мрежног приступа, а реализован са неуралним мрежама.
- Откривање најбољих неуралних мрежа за сваки од степена система за детекцију напада.
- Висок степен класификације напада помоћу другог степена неуралне мреже у рангу најбољих објављених резултата или боље.

6. План истраживања и структура рада

После проучавања постојеће литературе ће се прикупити постојећи скупови токова или пакета са мрежа који имају обележене нападе. Са таквим подацима ће се тренирати различите неуралне мреже како би се открило које су врсте неуралних мрежа најпогодније за сваки од степена целог система за детекцију упада. Након тога ће се урадити додатна провера са познатим нападима на Академску мрежу, при чему ће токови за те нападе бити добијени помоћу система NetIS којим се врши надзор Академске мреже. На крају ће се упоредити резултати добијени помоћу развијеног система са до сада објављеним резултатима.

7. Закључак и предлог

На основу претходно изложеног, комисија је констатовала да предложена тема докторске дисертације, под називом "Flow-Based Intrusion Detection System With Two Neural Network Stages" односно "Систем за детекцију упада заснован на токовима са две неуралне мреже"**,** по предмету истраживања, циљевима и методологији има научну заснованост и одговара нивоу докторске дисертације. Предложена тема представља значајну област истраживања са теоријског и практичног становишта.

Комисија је констатовала да кандидат Мр **Yousef Abuadlla**, дипл. инж испуњава формалне услове и поседује све потребне квалификације за одобравање израде докторске дисертације на предложеној теми. У свом досадашњем истраживачком раду кандидат се бавио сродним областима и прошао додатну обуку потребну за израду дисертације у области рачунарских мрежа. Кандидат је већ објавио радове из области истраживања на предложеној дисертацији.
На основу изнетог, комисија за оцену испуњености услова кандидата и научне заснованости теме докторске дисертације предлаже Наставно-научном већу Електротехничкког факултета да кандидату Мр **Yousef Abuadlla** одобри израду дисертације под називом: **"Flow-Based Intrusion Detection System With Two Neural Network Stages"** односно **"Систем за детекцију упада заснован на токовима са две неуралне мреже".** Ужа научна област теме је Рачунарска техника и информатика. За ментора предлажемо проф. Зорана Јовановића.

У Београду 6.2.2014.

ЧЛАНОВИ КОМИСИЈЕ

_____
др Зоран Јовановић, редовни професор
Универзитет у Београду – Електротехнички факултет

_____
др Горан Квашчев, доцент
Универзитет у Београду – Електротехнички факултет

_____
др Душан Старчевић, редовни професор
Универзитет у Београду – Факултет организационих наука

_____
др Славко Гајин, доцент
Универзитет у Београду – Електротехнички факултет