

НАСТАВНО-НАУЧНОМ ВЕЋУ

Предмет: Оцена научне заснованости теме докторске дисертације кандидата Кристијана Жиже, мастер инжењера електротехнике и рачунарства, под насловом „Спречавање ексфилтрација података коришћењем DNS инфраструктуре“.

Одлуком бр. 75-31 од 16.01.2024. године, именовани смо за чланове Комисије за оцену научне заснованости теме докторске дисертације докторске дисертације кандидата Кристијана Жиже, под називом „Спречавање ексфилтрација података коришћењем DNS инфраструктуре“ (енг. *Prevention of Data Exfiltration Using DNS Infrastructure*).

На основу материјала приложеног уз Захтев кандидата, Комисија подноси следећи

ИЗВЕШТАЈ

1. Подаци о кандидату

1.1. Биографски подаци

Кристијан Жижа, мастер инж. електротехнике и рачунарства, рођен је у Глини, Хрватска, 3. септембра 1994. године. Основну школу „Илија Гарашанин“ завршио је 2009. године као ђак генерације и носилац Вукове дипломе. Средњу економску школу у Гроцкој завршио је 2013. године као носилац Вукове дипломе.

Основне студије на Електротехничком факултету уписао је школске 2013/2014. године, студијски програм Софтверско инжењерство. Дипломирао је 2017. године са просечном оценом 10.00. Дипломски рад на тему „Реализација MicroJava компајлера за Java виртуелну машину“ под менторством др Драгана Бојића одбранио је са оценом 10. Изабран је за најбољег студента генерације Електротехничког факултета која је дипломирала 2017. године. Током лета 2017. године учествовао је на летњем истраживачком пројекту на Рајс универзитету у Хјустону, САД.

Мастер академске студије на Електротехничком факултету уписао је школске 2017/2018, модул Софтверско инжењерство. Мастерирао је 2018. године са просечном оценом 10.00. Мастер рад на тему „Реализација генератора случајних MicroJava програма“ под менторством др Драгана Бојића одбранио је са оценом 10. Током лета 2018. био је на стручној пракси у компанији SAP у Валдорфу, Немачка.

Докторске академске студије на Електротехничком факултету у Београду уписао је школске 2018/2019, на модулу Софтверско инжењерство. До сада је остварио 120 ЕСПБ, односно положио све испите предвиђене студијским програмом са оценом 10. У току докторских студија објавио је један рад у међународном часопису са импакт фактором и три рада на домаћим конференцијама.

Од друге године студија радио је као студент-демонстратор на више предмета Катедре за рачунарску технику и информатику. Почев од децембра 2017. године запослен је на Електротехничком факултету Универзитета у Београду. У периоду од децембра 2017. до фебруара 2019. године био је изабран у звање сарадника у настави. Од марта 2019. запослен је у звању асистента на Катедри за рачунарску технику и информатику. Школске 2021/2022 био је на неплаћеном одсуству ради стручног усавршавања у Немачкој.

Учествовао је као предавач у програму преквалификација у области информационих технологија који је организовао Развојни програм Уједињених нација током 2021. и 2022. године.

1.2. Стечено научноистраживачко искуство

Кристијан Жижа је у свом истраживачком раду показао изузетно интересовање за област рачунарских мрежа, са посебним акцентом на нападе коришћењем DNS инфраструктуре.

Уписао је докторске академске студије школске 2018/2019. године на Електротехничком факултету Универзитета у Београду, на Модулу за Софтверско инјерство. Све испите предвиђеним овим студијским програмом је положио са просечном оценом 10,00 и остварио 120 ЕСПБ. Списак положених испита приказан је у табели која следи:

Назив предмета	Оцена	ЕСПБ	Датум полагања испита
(13Д111МИ) Медицинска информатика	10	9	29.09.2020.
(13Д111СТ) Софтверска техника	10	9	29.09.2020.
(13Д091УНР) Увод у научни рад	10	9	15.07.2020.
(13Д081СФ) Специјалне функције	10	9	16.01.2020.
(13Д081ФАП) Функционална анализа и примене	10	9	16.01.2020.
(13Д111АПС) Архитектуре за подршку софтверским системима	10	9	22.09.2019.
(13Д111ОПП) Одабрана поглавља из програмских преводаца	10	9	20.09.2019.
(13Д111СЗР) Сигурност и заштита рачунарских система	10	9	12.09.2019.
(13Д111ФЈА) Формални језици и аутомати	10	6	22.09.2019.
(19Д111СДМ) Софтверски дефинисане мреже	10	9	04.07.2019.

Кандидат је испунио све обавезе предвиђене наставним планом и програмом докторских студија: Студијски истраживачки рад I (15 ЕСПБ), Студијски истраживачки рад II (15 ЕСПБ) и Научно стручни рад (3 ЕСПБ).

Досадашњи резултати кандидата приказани су кроз више публикација на домаћим конференцијама као и једног рада у часопису са SCI листе. У наставку следи списак публикација:

Радови у часописима са SCI листе:

1. К. Жижа, П. Тадић, Р. Vuletić, **DNS exfiltration detection in the presence of adversarial attacks and modified exfiltrator behaviour**, INTERNATIONAL JOURNAL OF INFORMATION SECURITY, 2023, doi: 10.1007/s10207-023-00723-w. [M22]

Радови на домаћим конференцијама:

1. К. Жижа, Д. Милованчевић, М. Мишић, Ј. Протић, **Примена метода за анализу социјалних мрежа на моделирање линија градског превоза у Београду**, XXIV

Скуп ТРЕНДОВИ РАЗВОЈА, pp. 102-105, Универзитет у Новом Саду, Факултет техничких наука, Копаоник, Фебруар, 2018. [M63]

2. Ј. Ђукућ, К. Жижа, М. Пунт, **Систем за аутоматско генерисање, скенирање и прегледање тестова**, 62. Конференција ЕТРАН, Зборник радова, Палић, Јун, 2018. [M63]
3. К. Жижа, Д. Бојић, **Генератор случајних Mikrojava програма**, 26. Конференција ЈУ ИНФО, pp. 132-136, Друштво за информационе системе и рачунарске мреже, Копаоник, Март, 2020. [M63]

1.3. Оцена подобности кандидата за рад на предложеној теми

Дана 24.01.2024. године, кандидат Кристијан Жижа је на Електротехничком факултету Универзитета у Београду усмено полагао испит о подобности предложене теме докторске дисертације и кандидата (докторски испит), пред комисијом у саставу:

- ван. проф. др Жарко Станисављевић, доктор електротехничких наука, вандредни професор, Електротехнички факултет, Универзитет у Београду
- ред. проф. др Дејан Симић, доктор електротехничких наука, редовни професор, Факултет организационих наука, Универзитет у Београду
- ван. проф. др Горан Квашчев, доктор електротехничких наука, ванредни професор, Електротехнички факултет, Универзитет у Београду

На јавној усменој одбрани предложене теме Комисија је кандидата оценила оценом **задовољно**.

На основу резултата испита за оцену научне заснованости теме докторске дисертације, резултата у студирању на свим нивоима студија до сада са највишом оценом, објављеног научног рада у области теме докторске дисертације и оствареног искуства у раду на том истраживању, Комисија констатује да кандидат Кристијан Жижа поседује знање и истраживачко искуство који га квалификују за израду докторске дисертације под називом „Спречавање експилтрација података коришћењем DNS инфраструктуре“.

2. Предмет и циљ истраживања

DNS (енг. *Domain Name System*) је дистрибуирани систем који мапира симболичка имена рачунара и сервиса у IP (енг. *Internet Protocol*) адресе. Функционисање рачунарских мрежа и Интернета није могуће замислити без овог протокола, јер би без њега било потребно памтити и бележити IP адресе свих услуга, што би значајно отежало, ако не и онемогућило, коришћење Интернета. Имајући у виду фундаментални значај DNS протокола за лако и ефикасно коришћење Интернета, DNS захтеви и одговори пролазе кроз мрежне уређаје без икаквог филтрирања. Управо та особина овај протокол чини честом метаом нападача како би се искористио као платформа за извршавање различитих врста напада.

Предмет истраживања су напади у којима се DNS захтеви и одговори користе како би се кроз њих преносили подаци са заражених уређаја. Овај вид преноса података назива се DNS експилтрација. Комуникација успостављена у оба смера, која најчешће укључује енкапсулацију других мрежних протокола у DNS пакете, назива се DNS тунеловање. Међу познатим примерима до сада извршених напада помоћу DNS експилтрација и тунеловања су комуникациони канали великих ботнет мрежа и крађе информација о дебитним картицама, што додатно наглашава озбиљност ових безбедносних изазова и последица које могу проузроковати. Овакве врсте напада се и данас успешно извршавају и поред тога што су

одавно познате заједници. Томе сведоче бројни примери у којима је ексфилтрација детектована тек након одређеног времена, а претпоставка је и да велики број ексфилтрација пролази неопажено [1-4].

Механизми детекције DNS ексфилтрација су у последње време изазвали повећано интересовање истраживачке заједнице, те су тако предложене бројне методе за детекцију ове врсте напада, а највећи број њих је базиран на алгоритмима машинског учења [5-6]. Предложени класификатори најчешће одређују само да ли се ради о нападу или не (бинарна класификација), док се мањи број радова бави прецизнијом класификацијом појединих врста напада односно протокола који се преносе путем DNS [7-9]. Аутори су се приликом обучавања модела за детекцију најчешће одлучивали за одлике које су базирани на DNS захтеву (нпр. број лабела, дужина захтева, ентропија карактера итд.) [8, 10-13] или на статистичке одлике више узастопних пакета између једног уређаја и једног домена, (просечно време између упита, просечна величина пакета, јединственост захтева итд.) [7, 14-17]. Свега неколико радова комбинује и једну и другу групу одлика [18-20], а као изузетак појављује се и детекција заснована на статистици промашаја у DNS кешевима [21]. Значајан методолошки проблем у свим претходним радовима је то да су предложени механизми за детекцију тестирани у идеалним условима и на скуповима података који омогућавају висок ниво прецизности. Расположиви алати за ексфилтрацију који су коришћени за креирање скупова података, како би максимизирали проток, креирају DNS захтеве чији су домени значајно дужи од регуларних, расподела карактера у захтевима је јасно псеудослучајна као последица компресије и енкрипције и очигледно другачија од оне код регуларних захтева, а присутно је и константно и кратко време између узастопних захтева и слично. Такође, у досадашњим истраживањима нису узете у обзир методе које би нападачи могли да примене да заобиђу детекцију (енг. *adversarial attacks*), те и не чуди што се и поред свих предложених механизма за детекцију, ексфилтрације путем DNS протокола и даље често срећу.

Главни циљеви овог истраживања су: свеобухватна анализа рада постојећих механизма за детекцију DNS ексфилтрација, анализирање метода којима би нападачи покушали заобилажење детектора и генерално методологије нападача, проналажење границе у могућности детекције ове врсте напада у смислу величине и учестаности DNS упита, развој новог алата за ексфилтрацију који омогућава симулацију понашања нападача и начина заобилажења детекције, те на крају развој нове методологије и алата за детекцију DNS ексфилтрација који даје боље резултате у односу на постојећа решења комбинујући анализу DNS упита и временских карактеристика низова DNS захтева. Како би се остварила ефикасна и брза детекција у реалним условима, алат ће бити дизајниран за рад на програмабилним мрежним уређајима.

Значај истраживања огледа се у бољем разумевању потенцијалних стратегија нападача на заобилажењу детекције, границама могућности за детекцију DNS ексфилтрација, побољшању постојећих техника за детекцију DNS ексфилтрација, што би применом у реалним системима довело до брже детекције напада и спречавања нелегалног преношења информација. Систем ће бити развијен тако да се може на веома лак начин применити у постојећим системима заснованим на програмабилним мрежним уређајима.

3. Полазне хипотезе

Предложено истраживање полази од следећих хипотеза:

- Постојеће методе за детекцију DNS ексфилтрација, предложене у научној литератури, имају значајно нижу прецизност детекције када нападач активно покушава да заобиђе детекцију.
- Могуће је креирати механизме активног заобилажења детекције DNS ексфилтрације који постојеће методе за детекцију не могу детектовати.
- Технике машинског учења могу да постигну високе нивое прецизности детекције DNS ексфилтрација и у случајевима активног заобилажења детекције коришћењем различитих, међусобно супротстављених типова одлика.
- Постоје ограничења могућности детекције DNS ексфилтрације и начини ексфилтрације које није могуће детектовати.
- Могуће је имплементирати метод и алат за детекцију DNS ексфилтрације са могућношћу брзе детекције напада у реалном времену и у ситуацијама активних напада на ексфилтрацију.

4. Научне методе истраживања

Истраживање ће почети свеобухватном претрагом научне литературе у области DNS ексфилтрација и механизма детекције предложеним у њима. Посебан осврт ће бити направљен на анализу коришћених алата за ексфилтрацију и методологије формирања скупова података над којима су вршене класификације. Биће извршена анализа стратегија које могу нападачи да изврше са циљем заобилажења детекције, као и тачке у рачунарској мрежи на којима могу да се прикупе најквалитетније информације о ексфилтрацијама. За потребе развоја, тестирања и анализе прикупиће се скуп података који ће чинити реални DNS захтеви и ексфилтрације које ће се спровести постојећим алатима за ексфилтрацију. Скуп података ће бити прикупљен на DNS серверу који је у активној оперативној употреби како би се потпуно верно пренели сви параметри рада DNS сервера у реалном окружењу (нпр. времена трајања рекурзивних упита, оптерећења и слично), уз очување приватности података. Биће предложен и развијен нови алат за DNS ексфилтрацију који узима у обзир могуће стратегије заобилажења детекције, са циљем да се покаже да постојећи механизми за детекцију имају недостатке, односно да резултати пријављени у научним радовима до сада не одговарају ономе што може да се очекује у реалним условима са нападачама који активно покушавају да заобиђу детекцију. Потом ће се приступити изради класификатора заснованих на техникама машинског учења који ће омогућити прецизнију детекцију у условима непријатељских модификација напада. Биће извршена компаративна анализа перформанси детекције развијеног алата и постојећих решења. Тестирање рада алата ће се обавити и његовом применом у реалном систему имплементираном помоћу програмабилних мрежних уређаја. Експерименталним путем ће се утврдити перформансе и могућност коришћења оваквог алата на програмабилним мрежним уређајима у реалном времену.

5. Очекивани научни допринос

Очекивани научни доприноси дисертације су:

- Свеобухватни преглед научне литературе, механизма рада, механизма детекције DNS ексфилтрација и алата који врше ексфилтрацију.
- Формирање оригиналног скупа података DNS ексфилтрација и регуларних упита, формираних у реалним условима уз укључивање различитих варијанти стратегија ексфилтрације.
- Анализа могућности нових стратегија непријатељског напада и алата за ексфилтрацију података преко DNS протокола који постојећи механизми за детекцију не могу детектовати.

- Предлог скупа одлика и методе за детекцију DNS ексфилтрација која нуди већу прецизност у односу на постојећа решења укључујући и присуство непријатељских напада.
- Пројектовање и имплементација алата за детекцију DNS ексфилтрације на програмабилним мрежним уређајима са циљем остваривања максималних перформанси.
- Анализа могуће брзине детекције DNS ексфилтрације и односа брзине и прецизности детекције.
- Експериментална евалуација перформанси и ефикасности као супротстављених фактора новог алата на програмабилним мрежним уређајима.

6. План истраживања и структура рада

Планирано је да се истраживање састоји из следећих фаза:

- Прва фаза ће обухватити претрагу научне литературе у области DNS ексфилтрација, детекције истих, као и алата који су коришћени у формирању релевантних скупова података.
- У другој фази ће бити идентификоване мане постојећих решења и припремљена стратегија за прикупљање скупа података који ће се користити за анализу постојећих метода за детекцију ексфилтрација. Такође, биће предложен нови алат за DNS ексфилтрацију који укључује могућност конфигурације и анализе непријатељских напада на детекцију, а чија је сврха откривање слабости постојећих метода за детекцију и развој стратегије детекције отпорне на могућност избегавања напада. У овој фази ће бити прикупљен реалан и релевантан скуп података који укључује DNS ексфилтрације и регуларне DNS упите снимљене на серверу који је у оперативној употреби и опслужује десетине хиљада корисника свакодневно.
- У трећој фази, на основу спроведене анализе и прикупљеног скупа података биће предложен нови алгоритам за детекцију ексфилтрација. Ова фаза ће обухватити имплементацију алата за детекцију DNS ексфилтрација и анализу стратегија детекције. Коришћењем прикупљеног скупа података и новоразвијеног алата за DNS ексфилтрацију биће тестиран рад новог алата за детекцију. Извршиће се упоредна анализа са постојећим решењима.
- Четврта фаза ће обухватити експериментално утврђивање да ли се предложени алгоритам за детекцију DNS ексфилтрација може користити на програмабилним мрежним уређајима. Биће тестиране перформансе и прецизност таквог система у реалним условима.

Најрелевантнијих референце из отворене литературе у вези са тезом су:

- [1] New FrameworkPOS variant exfiltrates data via DNS requests (2014), G Data blog, <https://www.gdatasoftware.com/blog/2014/10/23942-new-frameworkpos-variant-exfiltrates-data-via-dns-requests> Accessed on November 27 2023
- [2] Krebs B.: Deconstructing the 2014 Sally Beauty Breach (2015), Krebs on Security, <https://krebsonsecurity.com/2015/05/deconstructing-the-2014-sally-beauty-breach/> Accessed on November 27 2023
- [3] Netlab blog, New Threat: B1txor20, A Linux Backdoor Using DNS Tunnel, https://blog.netlab.360.com/b1txor20-use-of-dns-tunneling_en/ Accessed on November 27 2023

- [4] Marinho, R.: Translating Saitama's DNS tunneling messages, SANS Infosec handlers diary, <https://isc.sans.edu/diary/Translating+Saitama%27s+DNS+tunneling+messages/28738> Accessed on November 27 2023
- [5] Sabir, B., Ullah, F., Babar, M.A., Gaire, R.: Machine learning for detecting data exfiltration. *ACM Comput. Surv.* 54(3), 1–47 (2021). <https://doi.org/10.1145/3442181>
- [6] Wang, Y., Zhou, A., Liao, S., Zheng, R., Hu, R., Zhang, L.: A comprehensive survey on DNS tunnel detection. *Comput. Netw.* 197, 108322 (2021). <https://doi.org/10.1016/j.comnet.2021.108322>
- [7] Bai, H., Liu, W., Liu, G., Dai, Y., Huang, S.: Application behavior identification in DNS tunnels based on spatial-temporal information. *IEEE Access* 9, 80639–80653 (2021). <https://doi.org/10.1109/ACCESS.2021.3085500>
- [8] Almusawi, A., Amintoosi, H.: DNS tunneling detection method based on multilabel support vector machine. *Security and Commun. Netw.* 2018, 1–9 (2018). <https://doi.org/10.1155/2018/6137098>
- [9] Homem, I., Papapetrou, P., Dosis, S.: Information-Entropy-Based DNS Tunnel Prediction pp. 127–140. https://doi.org/10.1007/978-3-319-99277-8_8 (2018)
- [10] Ahmed, J., Gharakheili, H.H., Raza, Q., Russell, C., Sivaraman, V.: Real-time detection of DNS exfiltration and tunneling from enterprise networks. *IFIP/IEEE Sympos. Integrat. Netw. Service Manag. (IM)* 2019, 649–653 (2019)
- [11] Tatang, D., Quinkert, F., Holz, T.: Below the radar: spotting DNS tunnels in newly observed hostnames in the wild. *APWG Sympos. Electron. Crime Res. (ECrime)* 2019, 1–15 (2019). <https://doi.org/10.1109/eCrime47957.2019.9037595>
- [12] Chen, S., Lang, B., Liu, H., Li, D., Gao, C.: DNS covert channel detection method using the LSTM model. *Comput. Secur.* 104, 102095 (2021). <https://doi.org/10.1016/j.cose.2020.102095>
- [13] Shafieian, S., Smith, D., Zulkernine, M.: Detecting DNS Tunneling Using Ensemble Learning (pp. 112–127). https://doi.org/10.1007/978-3-319-64701-2_9 (2017)
- [14] Zhan, M., Li, Y., Yu, G., Li, B., Wang, W.: Detecting DNS over HTTPS based data exfiltration. *Comput. Netw.* 209, 108919 (2022). <https://doi.org/10.1016/j.comnet.2022.108919>
- [15] Wang, S., Sun, L., Qin, S., Li, W., Liu, W.: KRTunnel: DNS channel detector for mobile devices. *Comput. Secur.* 120, 102818 (2022). <https://doi.org/10.1016/j.cose.2022.102818>
- [16] Aiello, M., Mongelli, M., Papaleo, G.: Basic classifiers for DNS tunneling detection. *Proceedings - International Symposium on Computers and Communications* 880–885, (2013). <https://doi.org/10.1109/ISCC.2013.6755060>
- [17] Steadman, J., Scott-Hayward, S.: DNSxP: Enhancing data exfiltration protection through data plane programmability. *Comput. Netw.* 195, 108174 (2021). <https://doi.org/10.1016/j.comnet.2021.108174>
- [18] Liu, J., Li, S., Zhang, Y., Xiao, J., Chang, P., Peng, C.: Detecting DNS tunnel through binary-classification based on behavior features. *Proceedings - 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 11th IEEE International Conference on Big Data Science and Engineering and 14th IEEE International Conference on Embedded Software and Systems*, 339–346. <https://doi.org/10.1109/Trustcom/BigDataSE/ICESSE.2017.256> (2017)
- [19] Paxson, V., Christodorescu, M., Javed, M., Rao, J., Sailer, R., Schales, D.L., Stoecklin, M., Thomas, K., Venema, W., Weaver, N.: Practical Comprehensive Bounds on Surreptitious Communication over DNS. *22nd USENIX Security Symposium (USENIX Security 13)*, 17–32. <https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/paxson> (2013)
- [20] Nadler, A., Aminov, A., Shabtai, A.: Detection of malicious and low throughput data exfiltration over the DNS protocol. *Comput. Secur.* 80, 36–53 (2019). <https://doi.org/10.1016/j.cose.2018.09.006>

- [21] Ishikura, N., Kondo, D., Vassiliades, V., Iordanov, I., Tode, H.: DNS tunneling detection by cache-property-aware features. IEEE Trans. Netw. Service Manag. 18(2), 1203–1217 (2021). <https://doi.org/10.1109/TNSM.2021.3078428>

7. Закључак и предлог

На основу приложене документације и стеченог целокупног утиска о теми докторске дисертације и досадашњег научног рада кандидата Кристијана Жижа, мастер инжењера електротехнике и рачунарства, Комисија је дошла до следећих закључака:

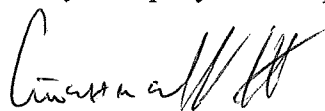
1. Кандидат испуњава све формалне и суштинске потребне услове прописане Законом о високом образовању, Статутом Универзитета у Београду и Статутом Електротехничког факултета Универзитета у Београду, за израду докторске дисертације.
2. Предложена тема **„Спречавање ексфилтрација података коришћењем DNS инфраструктуре”** јесте научно заснована, а резултати који ће проистећи израдом ове докторске дисертације представљаће значајан и оригиналан допринос међународној научној заједници. Тема припада ужој научној области Рачунарска техника и информатика.

На основу свега претходно изложеног, Комисија са задовољством предлаже Наставно-научном већу Електротехничког факултета Универзитета у Београду да кандидату Кристијану Жижи одобри израду докторске тезе под насловом **„Спречавање ексфилтрација података коришћењем DNS инфраструктуре”** (енг. *Prevention of Data Exfiltration Using DNS Infrastructure*), под менторством др Павла Вулетића, ванредног професора Електротехничког факултета Универзитета у Београду.

ЧЛАНОВИ КОМИСИЈЕ



др Павле Вулетић, ванредни професор
Универзитет у Београду – Електротехнички факултет



др Жарко Станисављевић, ванредни професор
Универзитет у Београду – Електротехнички факултет



др Дејан Симић, редовни професор
Универзитет у Београду – Факултет организационих наука



др Горан Квашчев, ванредни професор
Универзитет у Београду – Електротехнички факултет