dr hab. inż. Piotr Zwierzykowski, prof. PP

Politechnika Poznańska
Wydział Informatyki i Telekomunikacji,
Instytut Sieci Teleinformatycznych

29 czerwiec 2022 r.

RECENZJA ROZPRAWY DOKTORSKIEJ

przygotowana dla Rady Naukowej Dyscypliny Informatyka Techniczna i Telekomunikacja Wydziału Elektroniki i Technik Informacyjnych Politechniki Warszawskiej

Tytuł rozprawy:	Badanie przydatności technologii Software-Defined Networking do wykrywania i przeciwdziałania zagrożeniom w sieciach teleinformatycznych
Autor rozprawy:	**mgr inż. Marcin Gregorczyk**
Promotorzy:	dr hab. inż. Wojciech Mazurczyk, prof. PW
Dziedzina:	nauki inżynieryjno-techniczne
Dyscyplina:	informatyka techniczna i telekomunikacja

1. Jakie zagadnienie naukowe/badawcze jest rozpatrywane w pracy (cel i teza rozprawy) i czy zostało ono dostatecznie jasno sformułowane przez Autora?

Rozprawa doktorska dotyczy problematyki zapewnienia bezpieczeństwa sieci korzystając z technologii SDN. Podjęty przez Doktoranta problem jest problemem aktualnym i ważnym, zarówno pod względem teoretycznym, jak i praktycznym. Mgr inż. Marcin Gregorczyk przyjął w rozprawie następującą tezę: *„Możliwe jest stworzenie efektywnych metod zabezpieczeń z wykorzystaniem technologii Software-Defined Networking w celu skutecznego wykrywania i zapobiegania atakom sieciowym"*.

W celu wykazania tezy rozprawy Kandydat sformułował szereg logicznie uporządkowanych zadań, które kolejno omówił w artykułach stanowiących integralną części rozprawy doktorskiej. Zadania dotyczyły:

- opracowania, zaimplementowania i oceny systemu detekcji złośliwego oprogramowania typu ransomware, opartego na technologii SDN wykorzystującego analizę ruchu HTTP;
- opracowania algorytmu wykrywania skanowania portów;
- opracowania oraz oceny efektywności systemu detekcji i powstrzymywania ataków, który korzysta z technologii SDN;
- opracowania metody detekcji pasywnego podsłuchu w sieci z użyciem SDN, która wykorzystuje uczenie maszynowe do analizy ruchu warstwy aplikacji;
- zaproponowania, oceny efektywności i propozycji obrony przez atakiem na architekturę technologii SDN w oparciu o autorski atak *fingerprinting*.

Poszczególne zdania badawcze dotyczyły problemów występujących w różnych warstwach modelu TCP/IP, obejmując wszystkie warstwy modelu. Można więc przyjąć, że swoim zakresem objęły wszystkie potencjalne poziomy na których mogą wystąpić zagrożenia bezpieczeństwa sieci.

W mojej opinii cel i teza rozprawy zostały przez Autora dostatecznie jasno i precyzyjnie sformułowane.

2. Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł, w tym literatury światowej, stanu wiedzy i zastosowań w przemyśle?

Początkowe dwa rozdziały rozprawy Doktorant poświęcił przeglądowi dostępnych źródeł. W rozdziale drugim Kandydat przedstawił klasyfikację taktyk i technik ataków prowadzoną przez MITRE ATT&CK oraz odniósł do nich taktyki i techniki którym odpowiadają zadania badawcze zdefiniowane w ramach rozprawy. W rozdziale tym znalazło się również uzasadnienie wyboru taktyk i technik wybranych do oceny podatności SDN na cyberataki. Rozdział trzeci Autor poświęcił przedstawieniu aplikacji podnoszących bezpieczeństwo SDN oraz omówieniu stanu wiedzy dotyczącemu zagrożeń bezpieczeństwa w środowiskach SDN. Doktorant opisał w nim m.in. innymi wektory ataków na sieci SDN oraz propozycje własnej klasyfikacji ataków na środowisko SDN nawiązującą do warstwowego modelu sieci TCP/IP. Przedstawione klasyfikacje stanowiły przyczynek do dyskusji nad atakami na aplikacje i technologię SDN. W rozdziale tym zawarto przegląd publikacji dotyczących bezpieczeństwa aplikacji w sieciach SDN oraz publikacji związanych z bezpieczeństwem samej technologii SDN. Przegląd obejmuje kilkadziesiąt pozycji literaturowych i stanowi dobry przykład analizy źródeł literaturowych zagadnień bezpieczeństwa sieci SDN.

Uważam, że analizę źródeł, przegląd wiedzy i zastosowań przeprowadzono w rozprawie w sposób właściwy.

3. Czy Autor rozwiązał postawione zagadnienia, czy użył właściwej do tego metody i czy przyjęte założenia są uzasadnione?

Doktorant konsekwentnie realizował zadania badawcze, których celem było wykazanie prawdziwości przyjętej w rozprawie tezy. W tym celu wykorzystał trzy publikacje w czasopismach i jedną publikację konferencyjną, których był współautorem oraz umieścił je w kolejnych rozdziałach rozprawy. Taką postać mają rozdziały od czwartego do siódmego, odpowiadające kolejnym zdaniom badawczym zdefiniowanym w ramach rozprawy.

W rozdziale czwartym Kandydat przedstawił detekcję zagrożeń typu ransomware na podstawie analizy charakterystyki ruchu HTTP. W rozprawie wykazano, że możliwa jest detekcja oprogramowania crypto ransomware poprzez analizę wymiany sekwencji komunikatów protokołu HTTP. Badania opisane w tym rozdziale dotyczą programów CryptoWall i Locky, które były jednymi z najbardziej znanych programów crypto ransomware w momencie prowadzenia badań. Uzyskane wyniki potwierdziły możliwość i użyteczność wykorzystania SDN do prowadzenia takich analiz. Warto podkreślić, że analizy te były rezultatem działań prototypowego systemu detekcji uruchomionego w rzeczywistym systemie sieciowym. Na podstawie przedstawionych przez Doktoranta wyników można stwierdzić, że system detekcji umożliwiał wykrywanie programów CryptoWall i Locky z 97 % skutecznością.

Uważam, że Autor prawidłowo wykonał pierwsze zadanie badawcze, przyjmując poprawne założenia i używając do tego właściwej metody.

Rozdział piąty rozprawy zawiera opis nowych sposobów przeciwdziałania skanowaniu portów (TCP SYN Scan) oraz atakowi DHCP Starviation będącego przykładem ataku DoS. W rozdziale tym przedstawiono wyniki uzyskane w sieci testowej. Na podstawie danych dostarczonych przez Doktoranta można stwierdzić, że zaproponowany w tym rozdziale mechanizm przeciwdziałania skanowaniu portów charakteryzuje się 99% skutecznością. Natomiast metoda zapewniająca ochronę przez atakiem DHCP Starviation okazała się skuteczna w 100% przeprowadzonych prób ataków. Metody te zostały zaimplementowane w narzędziu *Integrated Security Framework*, które powstało w wyniku realizacji projektu „Internet of Radio Light" programu Horyzont 2020, w którym uczestniczył Autor rozprawy. Zakres przedstawionych przez Doktoranta w tym rozdziale badań odpowiada drugiemu i trzeciemu zadaniu badawczemu.

Uważam, że Autor prawidłowo wykonał drugie i trzeci zadanie badawcze, przyjmując poprawne założenia i używając do tego właściwej metody.

W rozdziale szóstym Doktorant przedstawił metodę wykrywania podsłuchu sieciowego na podstawie analizy metryk ruch, która została również zaimplementowana w narzędziu *Integrated Security Framework*. Zaproponowana metoda wykorzystuje techniki uczenia maszynowego do analizy ruchu protokołów ICMP oraz HTTP. Wyniki przedstawione przez Autora wskazują na 99% skuteczność metody. Zakres opisanych przez Kandydata w tym rozdziale badań odpowiada czwartemu zadaniu badawczemu zdefiniowanemu w ramach rozprawy.

Uważam, że Autor prawidłowo wykonał czwarte zadanie badawcze, przyjmując poprawne założenia i używając do tego właściwej metody.

Rozdział siódmy opisuje szacowanie poufnych parametrów tablicy przepływów w przełączniku SDN. Celem tego rozdziału było opisanie metod zabezpieczenia przed nowymi podatnościami, które pojawiały się wraz z wprowadzeniem SDN. Zilustrowano to na przykładzie ataku przepełnienia tablicy przepływów w przełączniku. Warunkiem powodzenia takiego ataku jest znajomość wielkości i zajętości tablicy przepływów przełącznika SDN. W rozdziale tym przedstawiono autorską technikę ataku opartą na aktywnym fingerprintingu wzbogaconą o algorytmy wykrywania skoków i zmian poziomów oraz porównano ją z metodą znaną z literatury przedmiotu. Uzyskane wyniki wskazują na znacznie większą skuteczność metody zaproponowanej przez Doktoranta przy określaniu rozmiaru i zajętości tablicy SDN (ponad 99%). Rozdział przedstawia również nowe metody ochrony przed takim atakiem. Zakres przedstawionych przez Kandydata w tym rozdziale badań odpowiada piątemu zadaniu badawczemu zdefiniowanemu w ramach rozprawy.

Uważam, że Autor prawidłowo wykonał piąte zadanie badawcze, przyjmując poprawne założenia i używając do tego właściwej metody.

4. **Na czym polega oryginalność rozprawy, co stanowi samodzielny i oryginalny dorobek Autora, jaka jest pozycja rozprawy w stosunku do stanu wiedzy i poziomu techniki reprezentowanych przez literaturę światową?**

Za najbardziej istotne i oryginalne wyniki Autora uważam:

- wykorzystanie analizy ruchu HTTP, przeprowadzonej w oparciu o środowisko SDN, do wykrycia złośliwego oprogramowania crypto ransomware typu CryptoWall i Locky,
- opracowanie metody detekcji pasywnego podsłuchu w sieci za pomocą nowatorskiej metody opartej na uczeniu maszynowym,
- analizę efektywności i opracowanie ulepszonego ataku typu active fingerprinting na przełącznik SDN oraz zaproponowanie sposobów obrony przed tym atakiem.

Po zapoznaniu się z treścią pracy oraz z oświadczeniami Doktoranta i współautorów prac stanowiących integralną część rozprawy uważam, że prezentowane w rozprawie wyniki związanie ze zdefiniowanymi przez Kandydata zadaniami badawczymi, stanowią samodzielny i oryginalny dorobek Autora.

Bezpośrednio w odniesieniu do rozważanych w rozprawie rozwiązań oraz prezentowanych wyników badań trudno jest sformułować poważniejsze zastrzeżenia merytoryczne. Doktorant od kilku lat z powodzeniem zajmuje się problematyką bezpieczeństwa środowisk SDN. Wiele wyników przedstawionych w rozprawie zostało opublikowanych w publikacjach, w których podlegały analizie i ocenie, a niektóre stanowią również integralną część pracy.

Rozprawę oceniam jednoznacznie pozytywnie, jednak podczas jej lektury nasunęły mi się pewne wątpliwości dotyczące sposobu opisu realizacji poszczególnych zadań badawczych. Skłoniło mnie to, to sformułowania następujących pytań:

- *Czy i w jakim zakresie rozważne w rozprawie taktyki i techniki ataków oraz proponowane metody im przeciwdziałania są odpowiednio dobrane do oceny zagrożeń SDN? Czy równie dobrze można dobrać inny zbiór taktyk i technik i znaleźć odpowiednie metody ochrony SDN? Dlaczego te a nie inne techniki i taktyki wybrano do udowodnienia tezy rozprawy?*
- *W jak dużym stopniu sposób detekcji crypto ransomware zaproponowany w pracy jest zależny od rodzajów analizowanych programów wykorzystywanych do ataku? Czy obecnie popularne programy crypto ransomware również mogą zostać wykryte i ewentualnie z jaką skutecznością? Czy podobna analizę można przeprowadzić w oparciu o coraz bardziej popularny protokół https?*
- *Czy zaproponowana w rozprawie metoda wykrywania skanowania portów i zabezpieczania przed skanowaniem oraz metoda ochrony przed atakiem DHCP Starviation, będą mogły być również wykorzystane przy sieci opartej na protokole IPv6?*

Bez wątpienia dużą zaletą rozprawy jest przedstawienie zadań badawczych poprzez przeprowadzanie eksperymentów w rzeczywistych środowiskach testowych. Uważam jednak, że bardzo dobrym uzupełnieniem tych badań byłby eksperymenty symulacyjne. W niektórych miejscach (np. w rozdziale 5) Doktorant powołuje się na

wyniki symulacyjne. Nie znalazło to jednak swojego szerszego omówienia w ramach pracy. *Dlaczego w rozprawie tak mało miejsca poświecono uogólnieniom, które mogłyby wynikać z badań symulacyjnych?*

Praca zawiera pewną liczbę błędów językowych, których można by uniknąć przy bardziej wnikliwej redakcji. Nie znalazłem natomiast w rozprawie błędów merytorycznych, a drobne zastrzeżenia lub wątpliwości, o których pisałem powyżej dotyczą raczej strony redakcyjnej pracy, lub mają charakter polemiczny i nie mogą mieć wpływu na ostateczną pozytywną ocenę pracy. Uważam, że recenzowana rozprawa zawiera wiele oryginalnych wyników i wnosi wartościowy wkład w rozwój informatyki technicznej i telekomunikacji.

Obszerna literatura przytoczona w pracy (spis publikacji zawiera 155 pozycji) świadczy o rozległej wiedzy i orientacji Autora w dziedzinie, którą uprawia. Zamieszczone pozycje z ostatnich lat (około 40% cytowanych prac zostało opublikowane po 2018 roku) potwierdzają, że Kandydat nie zajmuje się tematyką wyczerpaną, lecz przeciwnie, jest ona aktualna i inspirująca badawczo. O kompetencji Kandydata świadczą również zawarte w rozprawie 4 prace, w tym trzy artykuły w opublikowane czasopismach międzynarodowych *„IEEE ACCESS"* (IF=4,076; 100 pkt.), *„Computers & Electrical Engineering"* (IF=2,335; 70 pkt.) oraz *„Security and Communication Networks"* (IF=1,306; 40 pkt.).

5. Czy Autor wskazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników (zwięzłość, jasność, poprawność redakcyjna rozprawy)?

Cel, zakres, podstawy metodologiczne, rezultaty osiągnięte w rezultacie badań i sformułowane wnioski zostały przedstawione w rozprawie wystraczająco jasno i precyzyjnie. Kandydat wykazał, że skutecznie opanował logikę komponentów stosowanych w środowisku SDN i potrafi ją wykorzystać w badaniach eksperymentalnych. Posiada również dużą wiedzę dotyczącą technicznych i implementacyjnych aspektów zagadnień bezpieczeństwa środowiska SDN. Autor jasno przedstawił swój wkład do dziedziny badań, w której mieści się rozprawa. Strona redakcyjna i terminologiczna rozprawy nie budzą większych zastrzeżeń.

6. Jaka jest przydatność rozprawy dla nauk inżynieryjno-technicznych?

Obecnie środowiska SDN są coraz częściej wykorzystywane w codziennej działalności wielu firm i organizacji na świecie. Powszechne wykorzystanie SDN w środowiskach chmurowych i związki z technologią 5G powodują, że jej popularność od wielu lat konsekwentnie rośnie. Od wielu lat w ośrodkach naukowo-badawczych i akademickich prowadzone są badania, których celem jest zwiększenie wydajności i skalowalności środowisk SDN. Badania te obejmują zarówno aspekty implementacyjne, jak i teoretyczne. Podejmowane w rozprawie problemy badawcze których celem było wykorzystanie środowiska SDN do zapewnienia bezpieczeństwa sieci oraz rozważania dotyczące bezpieczeństwa samego środowiska SDN bardzo dobrze wpisują się w ten nurt badań, bezpośrednio lub je uzupełniając.

Można zatem stwierdzić, że tematyka badań podejmowanych w rozprawie bardzo dobrze wpisuje w międzynarodowy nurt badań teoretycznych i aplikacyjnych prowadzonych w dziedzinie uprawianej przez Autora.

O praktycznym znaczeniu osiągnięć Doktoranta może świadczyć wykorzystanie środowisk eksperymentalnych do przeprowadzania badań prowadzonych w ramach poszczególnych zadań badawczych objętych tematyką rozprawy. Wyniki uzyskiwane w tych badaniach wskazują na dużą skuteczność uzyskanych rozwiązań, o czym świadczą przytoczone przez Kandydata dane:

- 97% skuteczność wykrywania ransomware CryptoWall oraz Locky;
- 99% skuteczność detekcji skanowania TCP SYN,
- 100% wykrywalność próby ataku DHCP Starvation,
- 99% skuteczność detekcji podsłuchu sieciowego z wykorzystaniem sniffera,
- 99% skuteczności szacowania dwóch poufnych parametrów tablicy przepływów w przełączniku SDN.

Warto również wspomnieć o narzędziu *Integrated Security Framework* opracowanym w ramach projektu „Internet of Radio Light " w którym uczestniczył Doktorant. Narzędzie to miało zapewnić bezpieczeństwo sieci testowej zabudowanej w oparciu o technologię 5G. Zaimplementowano w nim rozwiązania będące również zadaniami badawczymi w rozprawie: tj. nowe sposoby przeciwdziałania skanowaniu portów i atakowi DoS oraz wykrywanie podsłuchu sieciowego na podstawie analizy metryk ruchu.

Proponowane przez Kandydata rozwiązania mogą wpłynąć na wzrost popularności środowisk SDN w stosunkowo nowym obszarze zastosowań jakim jest wykorzystywane SDN jako elementu zabezpieczenia sieci. Natomiast rozważania dotyczące zwiększenia bezpieczeństwa samych systemów SDN mają moim zdaniem jeszcze większy potencjał implementacyjny z uwagi na szeroki obszar zastosowań tych systemów. Pozwala to na stwierdzenie, że rozprawa może mieć istotny wpływ na poprawę bezpieczeństwa sieci 5G oraz środowisk i aplikacji uruchomionych w chmurze, a tym samym przyczyni się do zwiększenia możliwości wykorzystania środowisk chmurowych, które są istotnym elementem wspomagającym pracę wielu obszarów gospodarki.

7. Czy rozprawa spełnia wymagania stawiane rozprawom doktorskim przez obowiązujące przepisy?

Biorąc pod uwagę wnioski zaprezentowane w poprzednich punktach i wymagania podane w Artykule 13 Ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz stopniach i tytule w zakresie sztuki (z późniejszymi zmianami) uważam, że **rozprawa doktorska** mgr inż. Marcina Gregorczyka pt. *„Badanie przydatności technologii Software-Defined Networking do wykrywania i przeciwdziałania zagrożeniom w sieciach teleinformatycznych"* **zawiera oryginalne rozwiązania problemu naukowego** oraz dowodzi, że **Kandydat posiada ogólną wiedzę teoretyczną** w dyscyplinie informatyka techniczna i telekomunikacja i **posiada umiejętność samodzielnego prowadzenia pracy naukowej.**

Uważam, że **rozprawa spełnia wymagania ustawy** i **wnoszę o dopuszczenie rozprawy doktorskiej** Pana mgr inż. Marcina Gregorczyka pt. *„Badanie przydatności technologii Software-Defined Networking do wykrywania i przeciwdziałania zagrożeniom w sieciach teleinformatycznych"* **do publicznej obrony**.