Wrocław, 27 czerwca 2022

Prof. dr hab. inż. Krzysztof Walkowiak
Wydział Informatyki i Telekomunikacji
Politechnika Wrocławska

RECENZJA ROZPRAWY DOKTORSKIEJ
DLA RADY DYSCYPLINY INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA
POLITECHNIKI WARSZAWSKIEJ

Autor rozprawy doktorskiej: mgr inż. Marcin Gregorczyk
Tytuł rozprawy doktorskiej: *„Badanie przydatności technologii Software-Defined Networking do wykrywania i przeciwdziałania zagrożeniom w sieciach teleinformatycznych”*
Promotor: dr hab. inż. Wojciech Mazurczyk, prof. uczelni

1. Zakres i charakter rozprawy

Recenzowana rozprawa doktorska mgr inż. Marcina Gregorczyka dotyczy zagadnień związanych z bezpieczeństwem sieci teleinformatycznych, w szczególności rozprawa koncentruje się na problematyce wykrywania i przeciwdziałania wybranym zagrożeniom w sieciach teleinformatycznych z wykorzystaniem technologii SDN (ang. *Software-Defined Networking*). Tematyka cyberbezpieczeństwa jest obecnie bardzo aktualnym i ważnym obszarem badawczym. Wynika to głównie z nieustannie rosnącego znaczenia różnych rozwiązań informatycznych oferowanych za pomocą sieci teleinformatycznych w praktycznie w każdym aspekcie ludzkiej aktywności. Dodatkowo w ostatnich latach obserwowany jest duży wzrost liczby różnych zagrożeń i ataków na systemy informatyczne mające związek z działaniami przestępczymi, także w sferze konfliktów międzynarodowych. Technologia SDN to stosunkowo nowa koncepcja polegająca na oddzieleniu płaszczyzny zarządzania siecią (ang. *control plane*) od płaszczyzny przesyłania pakietów (ang. *data plane*) i stworzeniu programowalnej infrastruktury, która jest odrębna od urządzeń fizycznych. SDN umożliwia stosowanie w sieci tzw. kontrolera sieciowego, który jest odpowiedzialny za podejmowanie decyzji dotyczących sposoby przesyłania i kontrolowania danych, także w zakresie wybieranych tras rutingu. Umożliwia to łatwe wprowadzenie do sieci nowych algorytmów i metod, także w zakresie cyberbezpieczeństwa. Kolejną zaletą technologii SDN jest szerokie wsparcie dla mechanizmów wirtualizacji, tzn. kontrolery SDN nie muszą być dedykowanymi urządzeniami sieciowymi, lecz mogą być realizowane jako oprogramowanie uruchamiane w środowisku wirtualnym, co umożliwia wykorzystywanie wydajności, skali i dostępności zasobów chmury obliczeniowej i pamięci masowej. Główne zalety SDN to możliwość lepszej optymalizacji zasobów

sieciowych, wysoka skalowalność dzięki stosowaniu mechanizmów wirtualizacji i możliwość szybkiej adaptacji sieci do zmieniających się: warunków, ruchu, potrzeb biznesowych oraz aplikacji. Technologia SDN zyskała popularność na przestrzeni ostatnich kilkunastu lat głównie w zastosowaniach chmurowych. Jednak zalety SDN mogą być także wykorzystane dla celów podniesienie bezpieczeństwa sieci teleinformatycznych, co zostało pokazane w recenzowanej rozprawie.

Recenzowana rozprawa doktorska jest przedstawiona jako cykl czterech artykułów naukowych:

- Gregorczyk Marcin, Mazurczyk Wojciech: "*Inferring Flow Table State through Active Fingerprinting in SDN Environments: A Practical Approach"*, Proceedings of the 18th International Conference on Security and Cryptography / De Capitani di Vimercati Sabrina, Samarati Pierangela (red.), 2021, SCITEPRESS – Science and Technology Publications.
- Gregorczyk Marcin, ˙Zórawski Piotr, Nowakowski Piotr, Cabaj Krzysztof, Mazurczyk Wojciech: "*Sniffing Detection Based on Network Traffic Probing and Machine Learning"*, IEEE Access, vol. 8, 2020.
- Cabaj Krzysztof, Gregorczyk Marcin, Mazurczyk Wojciech, Nowakowski Piotr, Żórawski Piotr: "*Network Threats Mitigation Using Software-Defined Networking for the 5G Internet of Radio Light System"*, Security and Communication Networks, Wiley, 2019.
- Cabaj Krzysztof, Gregorczyk Marcin, Mazurczyk Wojciech, "*Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics"*, Computers & Electrical Engineering, vol. 66, 2018.

Należy podkreślić, że wybrana tematyka rozprawy jest aktualnym obszarem badań poszerzającym dotychczas realizowane prace w zakresie cyberbezpieczeństwa. Warto również zauważyć, że publikacje wchodzące w skład rozprawy zostały opublikowane w renomowanych czasopismach i w materiałach dobrej konferencji naukowej oraz uzyskały znaczny oddźwięk w środowisku naukowym potwierdzony dużą liczbą cytowań.

2. Zawartość rozprawy

Rozprawa składa się z 8 rozdziałów. Pierwszy rozdział to wprowadzenie przedstawiające motywację tematu rozprawy, tezę rozprawy oraz opis podstawowych zagadnień związanych z tematyką rozprawy doktorskiej. Rozdział 2 opisuje najważniejsze zagadnienia dotyczące technologii SDN, jej oraz wybrane cyberzagrożenia, które zostały poddane analizę w dalszej części rozprawy. W rozdziale 3 Doktorant przedstawił przegląd literaturowy dotyczący obszarów badawczych poruszanych w rozprawie. Rozdział 4 przedstawia problem detekcji zagrożeń typu ransomware na podstawie analizy charakterystyki ruchu HTTP i składa się z publikacji *„Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics"* opublikowanej w czasopiśmie Computers & Electrical Engineering. Rozdział 5 dotyczy problemu detekcji i mitygacja ataków sieciowych TCP SYN Scan oraz DHCP Starvation i zawiera publikację "*Network Threats Mitigation*

Using Software-Defined Networking for the 5G Internet of Radio Light System" opublikowaną w czasopiśmie Security and Communication Networks. Rozdział 6 koncentruje się na problemie wykrywanie podsłuchu sieciowego na podstawie analizy metryk ruchu i przedstawia publikację "*Sniffing Detection Based on Network Traffic Probing and Machine Learning"*, która ukazał się w czasopiśmie IEEE Access. Rozdział 7 dotyczy problemu szacowanie poufnych parametrów tablicy przepływów w przełączniku SDN i zawiera publikację "*Inferring Flow Table State through Active Fingerprinting in SDN Environments: A Practical Approach"*, która ukazała sie w materiałach konferencji 18th International Conference on Security and Cryptography. Ostatni rozdział zawiera podsumowanie rozprawy.

W mojej ocenie struktura rozprawy doktorskiej jest prawidłowa. Doktorant w logiczny i przejrzysty sposób przedstawił kolejne zagadnienia, co ułatwia lekturę i analizę zawartości rozprawy. Ponadto, pragnę podkreślić wysoką jakość rozprawy pod kątem językowym, stylistycznym i edycyjnym.

3. Poprawność i oryginalność postawionej tezy

Teza pracy jest sformułowana w następujący sposób: „*Możliwe jest stworzenie efektywnych metod zabezpieczeń z wykorzystaniem technologii Software-Defined Networking w celu skutecznego wykrywania i zapobiegania atakom sieciowym.*" W mojej opinii teza pracy jest sformułowana poprawnie. Doktorant na podstawie przeglądu literaturowego i własnej wiedzy prawidłowo określił zakres swojej rozprawy, koncentrując się na istotnych aspektach związanych ze współczesnymi problemami bezpieczeństwa sieci teleinformatycznych.

Teza rozprawy został osiągnięty w rozprawie doktorskiej poprzez:

- Opracowanie, zaimplementowanie i zbadanie systemu detekcji złośliwego oprogramowania typu ransomware, opartego na technologii SDN wykorzystującego analizę ruchu HTTP oraz porównanie charakterystyk dwóch rodzin ransomware: Locky oraz CryptoWall.
- Opracowane i zbadanie nowatorskiego, zoptymalizowanego algorytmu wykrywania skanowania portów.
- Opracowane i zbadanie systemu detekcji oraz mitygacji wykorzystującego technologią SDN dla zagrożeń typu Denial of Service (DoS).
- Opracowanie nowatorskiej metody detekcji pasywnego podsłuchu w sieci opartej na uczeniu maszynowym oraz ruchu warstwy aplikacji stosu TCP/IP.
- Zbadanie efektywności ulepszonego ataku typu fingerprinting na architekturę technologii SDN oraz opracowanie sposobów obrony przed nimi.

Według mojej opinii mgr inż. Marcin Gregorczyk rozwiązał postawiony problem naukowy stosując prawidłowe metody badawcze.

4. Analiza źródeł (w tym literatury światowej i stanu techniki) świadcząca o dostatecznej wiedzy autora w danej dyscyplinie naukowej

Rozprawa doktorska mgr inż. Marcina Gregorczyka dotyczy aktualnych zagadnień związanych z bezpieczeństwem sieci teleinformatycznych. Doktorant przeprowadził dokładny przegląd literaturowy. Lista pozycji bibliograficznych umieszczona w rozprawie zawiera 155 publikacji naukowych. Wśród nich znajdują się najważniejsze prace związane z tematyką poruszaną w rozprawie, w szczególności z: technologią SDN, cyberzagrożeniami, aplikacjami i systemami podnoszącymi bezpieczeństwo w sieciach SDN. Przedstawiony przegląd literaturowy stanowi dobre wprowadzenie do dalszej części rozprawy prezentującej oryginalne koncepcje Doktoranta. Ponadto, każdy z artykułów wchodzących w skład rozprawy zawiera dokładny przegląd literatury dotyczącej tematyki danego artykułu. Moim zdaniem, Doktorant posiada odpowiednią wiedzę i znajomość współczesnej literatury z zakresu związanego z tematyka rozprawy.

5. Pozycja rozprawy w stosunku do stanu wiedzy i stanu techniki reprezentowanych przez literaturę światową

Tematyka rozprawy doktorskiej jest związana z aktualnie rozwijanymi kierunkami badań w zakresie cyberbezpieczeństwa. Zagadnienia dotyczące podniesienia bezpieczeństwa działania sieci teleinformatycznych z wykorzystaniem technologii SDN są bardzo ważnym tematem badawczym. Wynika to z jednej strony z nieustannego wzrostu liczby różnego rodzaju cyberzagrożeń, a z drugiej strony z rosnącej popularności stosowania technologii SDN nie tylko w obszarze chmur obliczeniowych, ale także w sieciach operatorów telekomunikacyjnych.

Rozważane w rozprawie cyberzagrożenia są aktualne i przeciwdziałanie tym zagrożeniom stanowi wyzwanie dla bardzo wielu instytucji i przedsiębiorstw. Doktorant w prawidłowy sposób określił zakres tematyczny rozprawy i następnie zaproponował właściwe metody rozwiązania postawionych problemów stosując rozwiązania zgodne z aktualnym stanem wiedzy i techniki reprezentowanym w światowej literaturze. Na szczególne podkreślenie zasługuje zastosowanie metod uczenia maszynowego oraz bardzo obszerne badania eksperymentalne wykorzystujące rzeczywiste dane oraz przeprowadzone z zastosowaniem zaawansowanego sprzętu komputerowego (w tym dwa serwery najwyższej klasy Enterprise, tj. IBM POWER AC822 oraz AC922 wypożyczone z firmy IBM Polska). Wymagało to bardzo dużej wiedzy i doświadczenia Doktoranta w zakresie: użycia różnych technik podnoszenia cyberbezpieczeństwa, metod uczenia maszynowego, technologii SDN, umiejętności technicznych w zakresie programowania oraz konfiguracji systemów komputerowych.

Należy podkreślić, że wyniki przedstawione w rozprawie zostały zrealizowane w ramach projektu EU Horizon 2020 *„IoRL (Internet of Radio Light)”*, w którego realizacji brało udział wiele renomowanych ośrodków naukowych.

6. Znaczenie uzyskanych wyników dla danej dyscypliny naukowej

Jako najważniejsze oryginalne osiągnięcia rozprawy doktorskiej mgr inż. Marcina Gregorczyka w dyscyplinie informatyka techniczna i telekomunikacja należy wymienić:

- Dokładną analizę technologii SDN pod kątem możliwości wykorzystania tej technologii do przeciwdziałania cyberzagrożeniom.
- Zastosowanie różnych funkcjonalności technologii SDN w celu przeciwdziałania wybranym cyberzagrożeniom, w szczególności:
    - Opracowanie, zaimplementowanie i zbadanie systemu detekcji złośliwego oprogramowania typu ransomware wykorzystującego analizę ruchu HTTP oraz porównanie charakterystyk dwóch rodzin ransomware: Locky oraz CryptoWall.
    - Opracowane i zbadanie nowatorskiego, zoptymalizowanego algorytmu wykrywania ataku dotyczącego skanowania portów.
    - Opracowane i zbadanie systemu detekcji oraz mitygacji dla zagrożeń typu DoS.
    - Opracowanie nowatorskiej metody detekcji pasywnego podsłuchu w sieci opartej na uczeniu maszynowym oraz ruchu warstwy aplikacji stosu TCP/IP.
    - Zbadanie efektywności ulepszonego ataku typu fingerprinting na architekturę technologii SDN oraz opracowanie sposobów obrony przed nimi.
- Przeprowadzenie szerokich badań eksperymentalnych wykorzystujących rzeczywiste dane oraz zaawansowany sprzęt komputerowy.

Należy podkreślić, że opracowane koncepcje oraz uzyskane wyniki mają duże znaczenia praktyczne. Doktorant zdefiniował i następnie rozwiązał realne i aktualne problemy badawcze związany z bezpieczeństwem sieci teleinformatycznych wykorzystując możliwości nowoczesnej technologii SDN oraz stosując wiele różnych narzędzi badawczych, w tym metody uczenia maszynowego.

7. Główne wady rozprawy, słabe stron wraz z krytycznymi uwagami szczegółowymi

Uwagi natury ogólnej:

- Przedłożona rozpraw jest spójnym tematycznie zbiorem czterech artykułów opublikowanych w czasopismach naukowych. Wszystkie artykuły są wieloautorskie, w tym: jeden artykuł ma dwóch autorów, jeden artykuł ma trzech autorów i dwa artykuły mają pięciu autorów. Niestety w rozprawie doktorskiej Doktorant nie podaje, które elementy tych artykułów są jego autorstwa. Co prawda oprócz rozprawy otrzymałem oświadczenia współautorów publikacji pokazujące procentowy udział poszczególnych autorów w przygotowaniu artykułów oraz zwięzły opis wkładu poszczególnych autorów do publikacji. Jednak moim zdaniem Doktorant powinien w samej rozprawie dokładnie opisać, które elementy poszczególnych artykułów są jego autorstwa. Jako podstawa do nadania stopnia doktora są przedstawione publikacje zawierającej także elementy opracowane przez innych autorów. W przypadku rozprawy doktorskiej przygotowanej jako monografia, wszystkie elementy niebędące wprost autorstwa doktoranta muszą być opatrzone

odpowiednim odwołaniem do literatury, więc Doktorant powinien w rozprawie będącej serią publikacji zastosować podobne podejście.

- W rozprawie brakuje szerszej próby generalizacji uzyskanych wyników. Rozważane są konkretne zagrożenia związane z cyberbezpieczeństwem, dla których Doktorant opracował metody przeciwdziałania. Jednak moim zdaniem brakuje szerszego spojrzenia na poszczególne zagrożenia i próby zaproponowania bardziej generalnych metod, mogących być także stosowanych do podobnych zagrożeń.

Uwagi natury polemicznej:

- Rozprawa doktorska jest mocno związana z technologią SDN, która jest ważnym elementem proponowanych rozwiązań. Moim zdaniem warto byłoby przedstawić dodatkowe informacje wskazujące czy zaproponowane w rozprawie rozwiązania są możliwe do stosowania także w przypadku kiedy rozważany system teleinformatyczny nie używa technologii SDN.

8. Konkluzja

Recenzowana rozprawa stanowi oryginalne rozwiązanie jednoznacznie sformułowanego zagadnienia naukowego. Autor rozprawy mgr inż. Marcin Gregorczyk w przekonujący sposób wykazał umiejętność samodzielnego prowadzenia badań naukowych, a także ich prawidłowej i wnikliwej interpretacji. Wymienione powyżej uwagi ogólne, polemiczne oraz szczegółowe nie mają znaczącego wpływu na pozytywną ocenę rozprawy. W związku z powyższym uważam, iż przedstawiona mi do recenzji rozprawa doktorska mgr inż. Marcina Gregorczyka spełnia wymogi zawarte w Ustawie dnia 3 lipca 2018 r. Przepisy wprowadzające ustawę – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2018 r, nr 1669) oraz w Ustawie o stopniach naukowych i tytule naukowym z dnia 14 marca 2003 roku (Dz. U. z 2003 r., nr 65, poz. 595 z późniejszymi zmianami) i wnoszę o dopuszczenie jej do publicznej obrony.