Wrocław 18.08.2023r.

Dr hab. inż. Grzegorz Kołaczek, prof. uczelni
Katedra Informatyk i Inżynierii Systemów
Wydział Informatyki i Telekomunikacji
Politechnika Wrocławska
ul. Wybrzeże Wyspiańskiego 27
50-370 Wrocław

Recenzja rozprawy doktorskiej

Autor:

mgr inż. Wojciech Niewolski

Tytuł:

„System adaptacji poziomu bezpieczeństwa do potrzeb usług realizowanych w nowych architekturach sieciowych"

Promotor:

Prof. dr hab. Zbigniew Kotulski,
Politechnika Warszawska

Niniejsza opinia została przygotowana na prośbę dr hab. inż. Jarosława Arabasa, prof. uczelni, Przewodniczącego Rady Dyscypliny Informatyka Techniczna i Telekomunikacja z dnia 20.06.2023r.

1. Problem badawczy i jego znaczenie

Recenzowana rozprawa jest związana z problematyką zapewnienia bezpieczeństwa złożonym, dynamicznym systemom informatycznym. W szczególności rezultaty rozprawy dotyczą zagadnień zautomatyzowanego, adaptacyjnego zapewniania bezpieczeństwa usług. Autor rozprawy skupia się na możliwości dostosowania metody ochrony do typu zagrożenia i charakterystyki serwisu z jednoczesnym uwzględnieniem polityki ochrony zdefiniowanej przez właściciela aplikacji.

Analiza literatury przedmiotu oraz aktualnych przedsięwzięć o charakterze wdrożeniowym potwierdza istotność wybranej przez autora rozprawy problematyki badawczej. W szczególności wzrost złożoności systemów, ich heterogeniczność oraz dynamika rozwoju, z drugiej zaś strony różnorodność wymagań definiowanych przez użytkowników, przy jednoczesnym wzroście zarówno liczby zagrożeń, jak i też oczekiwań dotyczących bezpieczeństwa usług informatycznych sprawia, że uzyskane w ramach przedłożonej rozprawy rezultaty mają znaczący wpływ na rozwój badań w obszarze bezpieczeństwa w dyscyplinie naukowej informatyka techniczna i telekomunikacja.

2. Kompozycja rozprawy

Recenzowana rozprawa liczy 260 stron. Została ona podzielona na siedem rozdziałów oraz zawiera trzy załączniki. W pracy zamieszczono również spis rysunków, spis tabel i skrótów oraz bibliografię złożoną z 276 pozycji literaturowych.

Układ i zawartość rozdziałów merytorycznych jest zasadniczo poprawna. W pierwszym rozdziale w sposób syntetyczny przedstawiony jest cel badań oraz sformułowana jest główna teza badawcza rozprawy. Ponadto wymienione są główne rezultaty naukowe rozprawy oraz scharakteryzowana została struktura dalszej części rozprawy.

Drugi rozdział zawiera wprowadzenie do zagadnień związanych z usługami chmurowymi w kontekście sieci nowej generacji w tym sieci 5G. W pierwszej części rozdziału omówione są różne modele i architektury świadczenia usług chmurowych. Następnie przedstawione są możliwości realizacji dostępu mobilnego do środowisk chmurowych, a w kolejnej części rozdziału zaprezentowane są koncepcje integracji systemu 5G i MEC (Multi-access Edge Computing) oraz scharakteryzowane są nowe potrzeby i trendy usług wertykalnych.

Kolejny rozdział dotyczy zagrożeń i ochrony usług w środowisku MEC. W tym rozdziale omówione są zagadnienia związane z oceną zagrożeń i zarządzaniem ryzykiem, metodami zapobiegania zagrożeniom w środowisku MEC oraz dokonano przeglądu literatury w zakresie systemów do automatycznej ochrony.

Rozdział czwarty przedstawia projekt systemu adaptacji bezpieczeństwa, na który składa się analiza istniejących metod monitorowania aplikacji chmurowych oraz opis proponowanej architektury systemu monitoringu. W tym rozdziale również przedstawiona jest dyskusja nad możliwością ograniczenia zapotrzebowania na energię elektryczną detektora zdarzeń bezpieczeństwa oraz przedstawiono architekturę i sposób implementacji interfejsu sterowania dla zaproponowanego systemu bezpieczeństwa.

Kolejny rozdział zawiera wyniki przeprowadzonych badań nad skutecznością detekcji i klasyfikacji incydentów dla projektowanego systemu wraz z charakterystyką działań prowadzących do optymalizacji jego działania.

Rozdział szósty koncentruje się nad efektywnością procesu orkiestracji w środowiskach przetwarzania Edge Computing. Również w tym rozdziale zawarto rozważania dotyczące problemów w implementacji polityki bezpieczeństwa w systemach informatycznych.

Końcowy rozdział zawiera syntetyczne podsumowania otrzymanych rezultatów oraz charakterystykę możliwych prac związanych z dalszym rozwojem zaproponowanego w rozprawie rozwiązania.

3. Oryginalne osiągnięcia

Do szczególnych oryginalnych elementów rozprawy należy zaliczyć:

- zaprojektowanie architektury referencyjnej Multi Access Edge Computing (MEC) dającej możliwość integracji z różnorodnymi metodami dostępu oraz dokonanie przykładowej implementacji i testów rozwiązania w zgodzie z zaproponowanymi wytycznymi projektowymi
- opracowanie interoperacyjnego i przenaszalnego systemu monitorowania na potrzeby gromadzenia danych charakteryzujących aktualny poziom bezpieczeństwa aplikacji
- opracowanie metody detekcji anomalii z uwzględnieniem wymagań dotyczących ograniczenia zapotrzebowania na konsumpcję energii elektrycznej
- opracowanie i implementację dynamicznego modelu polityki bezpieczeństwa wraz z interpretatorem umożliwiającym konfigurowalny i zautomatyzowany proces detekcji oraz reakcji, uwzględniający dane kontekstowe
- zaprojektowanie i implementację metody ochrony dostępu, dla aplikacji uruchamianych w MEC (MEC Enabler) wraz funkcją umożliwiającą anonimizację wybranych połączeń
- implementację demonstratora systemu AraMIS umożliwiającego dopasowanie poziomu bezpieczeństwa, zależnie od typu zagrożenia, charakterystyki serwisu, jak i polityki ochrony zdefiniowanej przez właściciela aplikacji

Dorobek publikacyjny autora wskazany jako związany z przedłożoną rozprawą składa się z dziewięciu publikacji, w tym w IEEE Access (IF=3,9 oraz 100 pkt. na liście MEiN). Dorobek publikacyjny świadczy o tym, iż przedstawione w rozprawie wyniki prac badawczych zostały również pozytywnie zweryfikowane podczas procesu recenzyjnego oraz także poddane dyskusji w trakcie wystąpień na konferencjach.

Powyższe osiągnięcia należy uznać za oryginalne i znaczące dla dyscypliny naukowej informatyka techniczna i telekomunikacja. Na tej podstawie Recenzent opiera swoją ogólną pozytywną ocenę rozprawy. Osiągnięcia te stanowią równocześnie potwierdzenie postawionej przez Autora głównej tezy pracy, czyli pokazują, iż możliwe jest zbudowanie systemu dynamicznej adaptacji poziomu bezpieczeństwa do potrzeb usług realizowanych w nowych architekturach sieciowych.

4. Uwagi krytyczne

Przedłożona do recenzji rozprawa jest pod względem merytorycznym i redakcyjnym w przeważającej części napisana poprawnie. W ocenie Recenzenta Autor nie ustrzegł się jednak również pewnych błędów, niedociągnięć i nieścisłości. Poniżej zostały zamieszczone najważniejsze uwagi krytyczne do treści, jak i formy pracy.

a. Uwagi natury ogólnej

1. Analiza literatury. W rozprawie analiza literatury pojawia się w kilku miejscach. W opinii recenzenta korzystniejsze dla rozprawy i dla jej czytelności byłoby dokonanie takiej analizy w jednym miejscu i w sposób metodyczny (np. przy zastosowaniu metody systematycznego przeglądu literatury). Dałoby to możliwość bardziej precyzyjnego i spójnego przedstawienia prezentowanego problemu na tle aktualnych osiągnięć naukowych.
2. Granularność modułów. Autor rozprawy rozpatruje oddzielnie moduł wykrywania anomalii i moduł klasyfikacji zdarzeń. W opinii recenzenta zasadne byłoby rozważenie możliwości integracji tych dwóch modułów w jeden, w celu zapewnienia większej wydajności i efektywności systemu zarządzania bezpieczeństwem.
    i. Czy możliwość klasyfikacji zdarzenie jako np. atak typu „brute force" nie jest wystarczającą informacją dla całego systemu zarządzania bezpieczeństwem, np. umożliwiającą podjęcie skutecznej reakcji?
    ii. Czy istnieją anomalie, które nie będą sklasyfikowane na późniejszym etapie i jaki to może mieć wpływ na działanie systemu zarządzania bezpieczeństwem?
    iii. Jak rozdzielenie tych funkcji wpływa np. na ograniczenie zapotrzebowania na energię.
3. Narzędzia w implementacji. W przedstawionej implementacji opracowanej architektury systemu zarządzania bezpieczeństwem wykorzystano wybrane narzędzia (np. OpenVSwitch, Suricata, itd.). W opinii recenzenta wybór ten jest arbitralny. Warto byłoby rozważyć opracowanie metody wyboru narzędzi, np. w oparciu o bardziej ogólne ale również konkretne wymagania dotyczące np. możliwości eksportu informacji dotyczącej monitorowanego obiektu w formacie json, możliwości generowania zdarzeń z zadanym odstępem czasu, itp.
    i. Czy dokonany wybór ma/może mieć wpływ na interoperacyjność, przenaszalność i efektywność zaimplementowanego rozwiązania?.
4. Wektor danych. Wykorzystywane w pracy algorytmy uczenia maszynowego korzystają ze zbioru danych określonego na 240/100 wyselekcjonowanych cech opisujących system. Jaki był oryginalny rozmiar wektora cech? Dlaczego zdecydowano się na wykorzystanie takiego szerokiego wektora cech skoro w świetle wyników z rozdziału 4 znaczna ich liczba nie jest znacząca informacyjnie? Czy oprócz

przedstawionej w rozprawie metody selekcji cech autor rozważał możliwości wykorzystania metod ekstrakcji cech? Czy były prowadzone analizy reprezentatywności analizowanego zbioru danych dla tak szerokiego wektora cech?

5. Diagramy. Jednym z istotnych elementów pracy jest projekt złożonego systemu. Czy w trakcie projektu były wykorzystywane metody modelowania np. z wykorzystaniem diagramów UML, BPMN, lub innych?
6. Anomalie. W rozdziale 5 przedstawiono test skuteczności działania algorytmów detekcji i klasyfikacji. W tym celu zasymulowane zostały wybrane scenariusze ataków, przy czym proporcja stanu normalnego do anomalnego (ataku) wyniosła 144/60. Jak taka proporcja ma się do potencjalnie możliwych do wystąpienia sytuacji w środowisku rzeczywistym i jaki to może mieć wpływ na poprawną interpretację wyników eksperymentu?
7. Precyzja języka.
    i. Autor rozprawy posługuje się wieloma terminami bez określenia precyzyjnego i właściwego dla nich kontekstu (np. optymalizacja), bądź stosuje zamiennie terminy o różnym znaczeniu (np. funkcja i funkcjonalność, adaptacja do polityki bezpieczeństwa oraz adaptacja bezpieczeństwa i adaptacja komponentów bezpieczeństwa, metody i mechanizmy oraz systemy), lub w przekonaniu recenzenta, w nie do końca właściwej formie (np. przenośny vs przenaszalny, adaptacja danych wejściowych). Również nie udało się ustrzec Autorowi pewnych niezręczności językowych (np. „ocena parametrów przy pomocy twierdzenia Shannon”). Niektóre z powyższych błędów mogą niekorzystnie wpływać na czytelność i możliwość poprawnej interpretacji treści rozprawy.
    ii. W pracy zabrakło jasnego zdefiniowania kluczowych dla rozprawy terminów takich jak adaptacja poziomu bezpieczeństwa, dynamiczna adaptacja, wydajność, skuteczność, automatyzacja (np. w taki sposób jak to zostało zrobione w pkt. 5.4)
8. Dostępność kodu źródłowego. Obecnie powszechnie stosowaną praktyką jest udostępnianie kodu, zwłaszcza kodu związanego z realizowaną pracą badawczą. Autor mógł udostępnić wytworzony kod, np. w postaci ogólnodostępnego repozytorium. Stanowić mogłoby to dodatkową cenną możliwość upowszechnienia i rozwoju przeprowadzonych prac badawczych.

b. Uwagi natury szczegółowej

1. Rysunki i tabele w rozdziale 2 posiadają niewłaściwą numerację.
2. Sposób prezentacji elementów graficznych w wielu miejscach wersji drukowanej rozprawy jest nieczytelny, a przez to również ogranicza możliwość analizy i interpretacji.

3. Niektóre dane prezentowane w rozprawie pozostawione bez szerszego komentarza mogą mieć charakter kontrowersyjny/dyskusyjny (np. dane w Tabeli 1.3 – mały wpływ ataków typu „data breach” w sektorze „healthcare”).
4. Nie jest jasne dla Recenzenta jak należy interpretować dane w kolumnie „Okres aktywności” w Tabeli 4.9. i co jest podstawą do takich, a nie innych wartości występujących w tej kolumnie.
5. Autor nie ustrzegł się błędów językowych i interpunkcyjnych.

5. Konkluzja

Zgodnie z zapisami ustawy „Prawo o szkolnictwie wyższym i nauce” (art. 187.1) z dnia 20 lipca 2018 r. ocenie podlega, czy rozprawa doktorska prezentuje ogólną wiedzę teoretyczną kandydata w dyscyplinie, umiejętność samodzielnego prowadzenia pracy naukowej oraz czy rozprawa doktorska stanowi oryginalne rozwiązanie problemu naukowego, oryginalne rozwiązanie w zakresie zastosowania wyników własnych badań naukowych w sferze gospodarczej lub społecznej.

Doktorant wykazał się w recenzowanej rozprawie obszerną wiedzą z zakresu poruszanej tematyki bezpieczeństwa systemów informatycznych i telekomunikacyjnych. Autor rozprawy w wyniku studiów literaturowych poprawnie zidentyfikował istotne problemy badawcze, a na tej podstawie sformułował tezę pracy oraz opracował scenariusze badawcze i przedstawił, w jaki sposób zostały one przeprowadzone w ramach podjętych prac. Pozwala to na stwierdzenie faktu spełnienia wymogów ustawy przez mgr. inż. Wojciecha Niewolskiego w dyscyplinie Informatyka Techniczna i Telekomunikacja.

Recenzowana rozprawa przedstawia ponadto oryginalne rozwiązanie problemu z zakresu adaptacyjnych metod gwarantowania wymaganego poziomu bezpieczeństwa systemom i usługom informatycznym. Ponadto autor rozprawy przedstawił sposób zastosowania wyników przeprowadzonych badań naukowych w sektorze telekomunikacyjnym gospodarki, a przez to przedłożona rozprawa również wypełnia wymagania ustawy w zakresie umiejętności prowadzenia samodzielnej pracy naukowej.

Biorąc powyższe pod uwagę stwierdzam, że praca mgr. inż. Wojciecha Niewolskiego pt. „System adaptacji poziomu bezpieczeństwa do potrzeb usług realizowanych w nowych architekturach sieciowych” spełnia wszystkie wymagania stawiane rozprawom doktorskim w świetle stosownej ustawy. Wnoszę o jej przyjęcie i dopuszczenie do jej publicznej obrony.

Grzegorz Kołaczek