POLITECHNIKA GDAŃSKA
WYDZIAŁ ELEKTRONIKI, TELEKOMUNIKACJI I INFORMATYKI

Gdańsk, 14.08.2023 r.

Dr hab. inż. Jacek Rak, prof. PG
Wydział Elektroniki, Telekomunikacji i Informatyki
Politechnika Gdańska

Recenzja rozprawy doktorskiej

Tytuł: System adaptacji poziomu bezpieczeństwa do potrzeb usług realizowanych w nowych architekturach sieciowych

Autor: Mgr inż. Wojciech Niewolski

Rozprawa doktorska mgra inż. Wojciecha Niewolskiego dotyczy problemu budowy systemu bezpieczeństwa, którego właściwości i zasady funkcjonowania są dopasowane adekwatnie do potrzeb świadczonych usług oraz architektur sieciowych, w ramach których te usługi funkcjonują (postulat adaptacji). Rozpatrywany problem jest niewątpliwie ważny i aktualny z uwagi na szereg zmieniających się dynamicznie uwarunkowań dotyczących m.in. ewolucji klas usług, różnorodności charakterystyk architektur (wykorzystujących np. strategie Cloud Computing, Edge Computing, Multi Access Edge Computing), jak i postępujących dalszych zmian tychże architektur. Niemniej istotną w tym zakresie jest dynamika zmian charakterystyk samych ataków sprawiająca, że opracowane metody zaradcze w zakresie detekcji, klasyfikacji i przeciwdziałania atakom, z biegiem czasu tracą na znaczeniu. Niewątpliwie słuszny jest zatem kierunek badań niniejszej rozprawy dotyczący konstrukcji systemu adaptacji poziomu bezpieczeństwa do konkretnych (zmiennych w czasie) uwarunkowań.

Oceniana rozprawa doktorska ukazuje autorskie rezultaty w rozpatrywanym obszarze, w tym w szczególności w zakresie: (1) projektu systemu bezpieczeństwa oferującego dopasowanie poziomu bezpieczeństwa do charakterystyk zagrożenia, cech architektury sieci oraz wymagań wynikających z założonej polityki ochrony; (2) analizy skuteczności zrealizowanego systemu.

Rak

Oceniana rozprawa doktorska została napisana w języku polskim i składa się z siedmiu rozdziałów numerowanych oraz kilku części nienumerowanych, w tym wykazu literatury, skrótów, tabel, rysunków oraz trzech załączników. Jej struktura jest ogólnie poprawna i odpowiada zwyczajowym wymaganiom stawianym rozprawom doktorskim. Jednocześnie należy zaznaczyć, że oceniana rozprawa doktorska jest także wynikiem realizacji tzw. „doktoratu wdrożeniowego", a więc dotyczącego realnych badawczych problemów praktycznych (w tym przypadku związanych z działalnością firmy Orange).

1. Jaki jest problem naukowy, cel i teza rozprawy oraz czy zostały one trafnie i jasno sformułowane?

Problemem naukowym ocenianej rozprawy jest opracowanie mechanizmu dopasowania poziomu bezpieczeństwa adekwatnie do charakterystyk świadczonych usług sieciowych, właściwości architektury systemu oferującego te usługi, jak i przyjętej polityki bezpieczeństwa.

Sformułowaną w tym kontekście na stronie 8 tezę rozprawy mówiącą o ***możliwości zbudowania systemu dynamicznej adaptacji poziomu bezpieczeństwa do potrzeb usług realizowanych w nowych architekturach sieciowych*** należy uznać za postawioną jednoznacznie i właściwie, a trud jej wykazania jako adekwatny dla tez rozpraw doktorskich.

Celem pracy jest więc próba opracowania systemu bezpieczeństwa spełniającego powyższe wymagania, a więc którego właściwości mogłyby dowieść prawdziwości postawionej tezy.

Aby zrealizować postawiony cel badawczy i wykazać tezę rozprawy, Doktorant wykonał pięć głównych zadań badawczych dotyczących:

(1) projektu i implementacji referencyjnej architektury referencyjnej Multi Access Edge Computing,
(2) realizacji uniwersalnego systemu pozyskiwania danych w zakresie oceny poziomu bezpieczeństwa aplikacji,
(3) opracowania modelu detektora anomalii przy wykorzystaniu ML/VAE,
(4) realizacji dynamicznego modelu polityki bezpieczeństwa uwzględniającego dane kontekstowe,
(5) projektu i implementacji systemu ochrony dostępu dedykowanego aplikacjom uruchomionych w MEC, jak i anonimizacji części połączeń

oraz trzy zadania pomocnicze w zakresie:

(a) analizy danych przy wykorzystaniu technik AI/ML,
(b) konstrukcji systemu generowania oraz uruchamiania modeli detektorów i klasyfikatorów,
(c) analizy skuteczności i wydajności autorskich komponentów

ukazane na stronach 8 i 9 rozprawy.

Zakres tychże zadań nie budzi moich zastrzeżeń i jest moim zdaniem adekwatny w stosunku do postawionej tezy.

2. Na czym polega oryginalny dorobek Autora i jakie jest znaczenie poznawcze lub przydatność praktyczna dla nauki bądź techniki?

Do oryginalnego dorobku Autora niniejszej rozprawy doktorskiej można moim zdaniem zaliczyć następujące rezultaty:

1) dyskusję w zakresie właściwości modeli i architektur świadczenia usług chmurowych wraz z charakterystyką dominujących scenariuszy dostępu do usług rozproszonych, jak i charakterystyką możliwych schematów integracji tychże architektur z sieciami mobilnymi (w szczególności realizacja dostępu mobilnego do środowisk chmurowych oraz integracja systemu 5G i MEC) ukazane w rozdziale 2 rozprawy,

2) szczegółowy opis zagrożeń w obszarze bezpieczeństwa (w tym w szczególności ich kilkustronicowa szczegółowa klasyfikacja w tabeli 3.1) w kontekście architektur obecnie wykorzystywanych systemów wraz z klasyfikacją cyberataków ukazane w rozdziale 3,

3) rozszerzenie rozdziału 3 rozprawy o przedstawienie i analizę właściwości mechanizmów zarządzania ryzykiem incydentów cyberbezpieczeństwa wraz z opisem metod zapobiegania tymże zagrożeniom w środowisku MEC (tabela 3.4), jak i przegląd oraz analiza właściwości systemów automatycznej ochrony przed cyberatakami,

4) propozycję adaptacyjnego systemu bezpieczeństwa AraMIS szczegółowo opisaną w rozdziale 4. W szczególności na uwagę zasługuje zawarty w nim opis systemu przenośnego monitoringu, autorska propozycja modelu sieci neuronowej opracowanego przez Doktoranta w celu opracowania detektora anomalii, jak i szczegółowy opis implementacji interfejsu do sterowania systemem AraMIS,

5) analizę właściwości systemu AraMIS przedstawioną w rozdziale 5 rozprawy, w tym w szczególności szczegółowy opis scenariuszy testów, opis metod używanych do analizy wyników, oraz szczegółową analizę wyników uzyskanych w przygotowanym przez Doktoranta w tym celu środowisku eksperymentalnym dotyczących skuteczności proponowanego rozwiązania w zakresie detekcji oraz klasyfikacji cyberataków w zestawieniu z wynikami systemów referencyjnych. Wyniki te ukazały największą skuteczność dla detektorów zaprojektowanych przez Doktoranta na bazie modeli uczenia maszynowego na podstawie sieci neuronowej,

6) zawartą w rozdziale 6 rozprawy propozycję sposobów usprawnień mechanizmu orkiestracji w obszarach brzegowych systemu oraz opis kompletnej polityki bezpieczeństwa wykorzystywanej w systemie AraMIS, tj. obejmującej wszystkie kolejne etapy działania systemu: od monitorowania zagrożeń do reagowania na nie.

3. Czy Autor rozwiązał postawiony problem i czy użył do tego celu właściwych metod?

Osiągnięcia opisane w rozprawie doktorskiej mgra inż. Wojciecha Niewolskiego skłaniają do wyciągnięcia wniosku, że Doktorant rozwiązał postawiony problem realizacji systemu dynamicznej adaptacji poziomu bezpieczeństwa do potrzeb usług realizowanych w nowych architekturach sieciowych, jak i przyjętej polityki bezpieczeństwa oraz, że wykazał tym samym tezę rozprawy dotyczącą możliwości zbudowania takiego systemu. Istotnie, na podstawie wyników rozprawy, można uznać, że zaprojektowany system AraMIS jest w stanie realizować zadanie dynamicznej adaptacji poziomu bezpieczeństwa adekwatnie do potrzeb oferowanych usług.

Zawartość rozdziałów rozprawy, w tym w szczególności rozdziałów 4-6 pokazuje, że Doktorant zastosował w celu rozwiązania postawionego problemu właściwe metody. Zarówno stopień złożoności problemu analizowanego w rozprawie, jak i mechanizmy wykorzystane w celu jego rozwiązania (w tym np. bazujące wykorzystaniu architektury sieci neuronowej do detekcji anomalii) należy uznać za adekwatne w odniesieniu do typowych wymagań stawianym rozprawom doktorskim.

Oprócz ocenianej rozprawy, na uwagę zasługują także:

1) publikacje Doktoranta, w tym cztery artykuły opublikowane w czasopismach ujętych jako pozycje [49], [123], [271], [272] wykazu literatury rozprawy:
   - IEEE Access (jedna praca) - obecnie 100 pkt MEiN z roku 2021,
   - Electronics, MDPI (dwie prace z 2021 r. i z 2022 r.) – obecnie 140 pkt MEiN,
   - Journal of Network and Computer Applications, Elsevier z 2023 r. – obecnie 140 pkt MEiN (praca mająca status "w recenzji" w rozprawie, lecz niedawno opublikowana),

   które mogą być uznane za powiązane z tematyką rozprawy doktorskiej,
2) wartości parametrów naukometrycznych, w tym w szczególności liczby cytowań prac Autora wynoszącej 59 (według Google Scholar) na dzień finalizacji niniejszej recenzji, które podkreślają rangę wyników badań Doktoranta w środowisku międzynarodowym.

Na podkreślenie zasługuje także wysoce praktyczny charakter osiągnięć Doktoranta, który wynika nie tylko z wdrożeniowego charakteru doktoratu przygotowanego w ścisłym związku z firmą Orange. Jest on widoczny również poprzez udział Doktoranta w dwóch projektach („Access control in 5G MEC" oraz "INSPIRE-5Gplus"), jak i szereg raportów wewnętrznych Orange współautorstwa Doktoranta, których sześć jest ujętych w wykazie literatury ocenianej rozprawy jako pozycje [121], [124]-[127] oraz [252].

Oceniana rozprawa doktorska charakteryzuje się ponadto poprawną strukturą, a jej treść została starannie opracowana i sformatowana. W mojej ocenie wykaz literatury obejmujący obszerny zestaw 276 pozycji ukazuje stan sztuki w sposób adekwatny do charakterystyki poruszanego tematu rozprawy.

4. Jakie są słabsze strony rozprawy?

Oceniana rozprawa doktorska jest moim zdaniem wysokiej jakości i pozbawiona istotnych wad. Moje uwagi są następujące:

1. Pomimo ogólnie bardzo dobrego stylu prezentacji wyników pracy, w pracy można zauważyć w kilku miejscach pewne kwestie stylistyczne/literowe, np.
   - str. 13: „... ze zwiększona potrzebą mocy obliczeniowych" → „...z potrzebą zwiększenia mocy obliczeniowej" lub „...z potrzebą zwiększonej mocy obliczeniowej"
   - str. 14: „...jest ona bardziej skompilowana..." → „...jest ona bardziej skomplikowana..."
   - str. 20: „Nie mniej" → „Niemniej"

2. Rysunki w rozprawie zostały ogólnie przygotowane w sposób staranny i szczegółowy. Jednakże, w przypadku kilu z nich należałoby rozważyć zwiększenie ich rozmiaru (np. rys 3.3, 3.4), gdyż tekst zawarty w nich jest słabo czytelny. Ogólnie zdecydowanie lepszym rozwiązaniem istotnie podnoszącym czytelność rysunków rozprawy byłoby wstawienie ich do rozprawy w formie grafiki wektorowej, a nie punktowej.

3. Doktorant analizując właściwości projektowanego systemu, bazuje na typowym cyklu obejmującym sekwencję etapów identyfikacji, ochrony, detekcji, reakcji i działań naprawczych, który klasycznie jest dedykowany reagowaniu na indywidualne zagrożenia. W tym kontekście warto byłoby rozszerzyć analizę o weryfikację skuteczności projektowanego systemu w scenariuszach:

   a) równoległego występowania zagrożeń (mogących wpływać na siebie wzajemnie, w tym w szczególności zwiększać rozmiar negatywnych konsekwencji),

   b) ataków przeprowadzanych w okresie, kiedy sieć nie ma pełnej zdolności operacyjnej (np. w okresie awarii masowej kilku jej elementów uwarunkowanej np. działaniem sił natury – pożarem, silnymi opadami deszczu, itp.).

Powyższe uwagi mają charakter uwag drobnych bądź polemicznych i nie rzutują na moją sumaryczną pozytywną ocenę rozprawy.

5. Do której z następujących kategorii Recenzent zalicza rozprawę:

a/ nie spełniająca wymagań,
b/ wymagająca wprowadzenia poprawek i ponownego recenzowania,
c/ zadowalająco spełniająca wymagania,
d/ wykraczająca ponad poziom zadawalający (spełniająca wymagania z nadmiarem),
e/ wybitna?

Moja sumaryczna ocena rozprawy doktorskiej mgra inż. Wojeciecha Niewolskiego jest **pozytywna**. Wynika ona przede wszystkim z istotnych osiągnięć Doktoranta zawartych w rozdziałach 4-6 rozprawy, jak i starannego przygotowania samej rozprawy. Z uwagi na spełnione moim zdaniem ustawowe wymagania, **wnoszę o dopuszczenie rozprawy doktorskiej mgra inż. Wojciecha Niewolskiego do publicznej obrony**.

Ponadto, ranga osiągnięć Doktoranta ukazanych w rozprawie poparta opublikowaniem przez Doktoranta szeregu prac w rozpoznawalnych czasopismach (które wymieniam w sekcji 3 niniejszej recenzji) sprawia, że niniejszą rozprawę zaliczam do kategorii:

d/ wykraczająca ponad poziom zadawalający (spełniająca wymagania z nadmiarem).

Z powyższych powodów, **wnoszę o rozpatrzenie możliwości wyróżnienia rozprawy.**

Jacek Rak