dr hab. inż. Sławomir Hausman, prof. uczelni

Afiliacja:
Instytut Elektroniki
Wydział Elektrotechniki, Elektroniki, Informatyki i Automatyki
Politechnika Łódzka
al. Politechniki 8
93-590 Łódź, budynek B9

Recenzja rozprawy doktorskiej

Autor rozprawy: **mgr inż. Germán Peinado Gómez**

Tytuł: **" Development of a Risk-based Security Framework for Mobile Networks interconnection applied in Roaming Service Level Agreements within the 5G context"**

Promotor: **prof. dr hab. Jordi Batallia**

Praca wykonana na **Wydziale Elektroniki i Technik Informacyjnych Politechniki Warszawskiej**

1. Jakie zagadnienie naukowe jest rozpatrzone w pracy /teza pracy/ i czy zostało ono dostatecznie jasno sformułowane przez Autora? Jaki charakter ma rozprawa (teoretyczny, doświadczalny, inny)?

Badania opisane przez mgra inż. Gómeza w jego dysertacji doktorskiej obejmują rozwój schematów bezpieczeństwa opartych na ryzyku dla połączeń między sieciami różnych generacji (2G–5G), ze szczególnym uwzględnieniem połączeń roamingowych w ramach umów SLA (Service Level Agreements). Autor koncentruje się na dynamicznej ocenie ryzyka, pomiarze zaufania między operatorami, definiowaniu profili bezpieczeństwa oraz automatyzacji egzekwowania polityk z uwzględnieniem współistnienia różnej generacji protokołów sygnalizacyjnych (SS7, Diameter, HTTP/2).

Problem wyjściowy, który był motywacją podjęcia badań, można scharakteryzować następująco, posługując się przykładem standardowej architektury 5G: NWDAF (Network Data Analytics Function) zbiera i analizuje dane sieciowe (np. ruch, wydajność, zdarzenia bezpieczeństwa), ale nie podejmuje decyzji. PCF (Policy Control Function) zarządza politykami, głównie związanymi z QoS (Quality of Service) i dostępem do usług, ale bez wbudowanego komponentu ryzyka/bezpieczeństwa. SEPP (Security Edge Protection Proxy) chroni komunikację międzyoperatorską (np. w roamingu), ale działa głównie na podstawie statycznych polityk i certyfikatów, bez dynamicznej adaptacji do zagrożeń. Brak integracji powoduje, że reakcja na zmieniające się ryzyko (np. atak wykryty przez analitykę) jest opóźniona i wymaga ręcznej rekonfiguracji polityk w PCF i SEPP. Doktorant proponuje zautomatyzowany przepływ danych i decyzji pomiędzy tymi elementami systemu, tworząc nowatorski, dynamiczny cykl bezpieczeństwa. W takim ujęciu NWDAF wykrywa anomalie, podejrzane wzorce ruchu i potencjalne zagrożenia (np. skanowanie portów, nieautoryzowane zapytania lokalizacyjne) i dostarcza je do rozszerzonego modułu PCF. Wygenerowane/zaktualizowane polityki bezpieczeństwa mogą być natychmiast egzekwowane przez SEPP, który może z kolei zbierać dane o skuteczności polityk i nowych incydentach, zwracając je do NWDAF w celu dalszej analizy. NWDAF udoskonala swoje modele analityczne na podstawie tych danych. Dzięki temu możliwe jest m.in. zamknięcie pętli sprzężenia zwrotnego: Analiza -> Decyzja/Polityka -> Realizacja polityki -> Sprzężenie zwrotne ->

Analiza. Powyższy opis rozważanego problemu nie wyczerpuje zakresu prac Autora, a jedynie zarysowuje kontekst i praktyczne znaczenie prowadzonych badań.

Autor w podrozdziale 1.2. sformułował trzy tezy dotyczące kluczowych wyzwań w zakresie bezpieczeństwa połączeń roamingowych, które można streścić następująco: 1) konieczność ciągłej oceny zaufania między operatorami (odzwierciedlonego w SLA) poprzez pomiar ryzyka w sygnalizacji międzyoperatorskiej (SS7/Diameter/HTTP/2); 2) potrzeba redukcji złożoności operacyjnej w 5G poprzez wprowadzenie profili bezpieczeństwa upraszczających negocjację polityk między operatorami, a także 3) wykorzystanie ujednoliconych ram polityk 5G do dynamicznego egzekwowania zabezpieczeń, reagującego na zmiany w środowisku sieciowym. W dysertacji Autor szczegółowo omawia swoje rozwiązania, sposób i wyniki ich weryfikacji/walidacji i dowodzi słuszności postawionych tez.

Praca ma charakter teoretyczno-aplikacyjny.

2. Czy w rozprawie przeprowadzono w sposób właściwy analizę źródeł (w tym literatury światowej, stanu wiedzy i zastosowań w przemyśle) świadczący o dostatecznej wiedzy autora? Czy wnioski z przeglądu źródeł sformułowano w sposób jasny i przekonywujący?

W rozdziale drugim rozprawy Doktorant przedstawił obecny stan wiedzy w zakresie bezpieczeństwa połączeń międzysieciowych w systemach mobilnych 2G-5G. Wykorzystana bibliografia zawiera 115 pozycji (artykuły, standardy, raporty, książki), które są, moim zdaniem, poprawnie dobrane, a także są powoływane w dysertacji we właściwym kontekście. Najwięcej cytowanych źródeł pochodzi z lat 2020–2024 (maksimum w 2023 r.) – co odzwierciedla aktualność tematyki 5G i bezpieczeństwa. Pojedyncze odniesienia sięgają lat dziewięćdziesiątych i wczesnych dwutysięcznych, np. w kontekście SS7 i SIGTRAN. Autor wykazał się znakomitą znajomością stanu wiedzy, cytując istotne standardy branżowe (3GPP TS 33.501, GSMA FS.19, IETF RFC), najważniejsze publikacje naukowe, patenty i projekty (np. kluczowy unijny projekt 5G-ENSURE). Przegląd obejmuje architektury bezpieczeństwa 2G–5G, zarządzanie ryzykiem (ISO/IEC 27005), modele zaufania (ETSI, NIST Zero Trust) oraz realizację wynikających z nich polityk bezpieczeństwa. Sformułowane przez Autora wnioski z przeglądu stanu wiedzy i techniki jasno wskazują luki w istniejących rozwiązaniach, w szczególności: brak dynamicznych mechanizmów oceny ryzyka w połączeniach międzysieciowych, „ręczne zarządzanie" politykami w bramach SEPP, nieuwzględnianie zaufania w SLA roamingowych. Wnioski są przekonujące i stanowiły motywację Autora do podjęcia pracy badawczej będącej przedmiotem dysertacji.

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

Autor w swojej dysertacji określił jasno cele pracy i zawarł je w trzech tezach (podrozdział 1.2). Zdefiniował także i opisał zastosowaną metodykę badawczą. Zastosował podejście łączące analizę standardów, literatury naukowej, modelowania matematycznego oraz walidacji empirycznej. Takie podejście jest konieczne, aby praca w zakresie bezpieczeństwa sieci mogła mieć rzeczywistą wartość aplikacyjną, a nie tylko teoretyczną lub przyczynkarską. W szczególności praca uwzględnia istniejące standardy w telekomunikacji, Ponadto, w stopniu wynikającym z ograniczeń dostępności danych z rzeczywistej sieci, została w części zweryfikowana z wykorzystaniem realnych danych. Doktorantowi udało się pozyskać dane o rzeczywistym ruchu z protokołem Diameter i użyć ich do częściowej walidacji proponowanych przez siebie rozwiązań.

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

Jak już wcześniej zaznaczono, głównym problemem badawczym podjętym przez Autora jest statyczność obecnych polityk bezpieczeństwa w połączeniach międzysieciowych sieci mobilnych (roaming), które opierają się na klauzulach umów SLA. Autor dowodzi, że postawa bezpieczeństwa wymaga dynamicznej adaptacji do ewoluującego ekosystemu połączeń i krajobrazu zagrożeń, uwzględniając przy tym współistnienie protokołów różnych generacji, np. SS7, Diameter, HTTP/2.

Do oryginalnych wyników pracy zaliczam:

- Opracowanie stanu wiedzy w zakresie istniejących metod zarządzania ryzykiem, zaufaniem i politykami bezpieczeństwa w sieciach mobilnych (rozdział 2), w tym analiza standardów bezpieczeństwa 5G opracowanych przez 3GPP (grupa SA3) oraz przegląd dokumentów organizacji operatorów GSMA, dotyczących bezpieczeństwa roamingu/połączeń międzysieciowych.
- Klasyfikacja i analiza istotnych z punktu widzenia bezpieczeństwa elementów informacji w protokołach SS7 (2G-3G), Diameter (4G) i HTTP/2 (5G).
- Zaplanowanie ogólnej ramowej architektury bezpieczeństwa (architektura wysokopoziomowa opisana w podrozdziale 3.2), obejmującej cztery główne komponenty: analizę ryzyka, wskaźnik zaufania, profile bezpieczeństwa i egzekwowanie polityk.
- Opracowanie szczegółowego matematycznego modelu dynamicznej oceny ryzyka (opisany w podrozdziałach 4.2 i 4.3). Omówienie możliwych i rzeczywiście zastosowanych w dysertacji technik eksploracji danych i analizy strumieni danych sygnalizacyjnych.
- Walidacja dla teoretycznego studium przypadku danych lokalizacyjnych (8.1) oraz praktyczna walidacja na podstawie zanonimizowanego śladu ruchu sygnalizacyjnego Diameter w roamingu 4G (podrozdziały 8.2. i 8.3).

Proponując swoje oryginalne rozwiązanie, Autor posłużył się podejściem znanym z Common Vulnerability Scoring System (CVSS), rozwijanym przez FIRST.org, który służy do oceny i klasyfikacji wagi luk zabezpieczeń w oprogramowaniu. To jest podejście stosowane w informatyce do sformalizowanego wyznaczenia wartości liczbowej ryzyka związanego z lukami, co np. ułatwia priorytetyzację działań naprawczych. Formalizacja polega na zdefiniowaniu metryk (stałych, zmiennych w czasie i środowiskowych) i wyznaczeniu ryzyka, które np. wymaga natychmiastowej reakcji. Doktorant dostosował te metryki do specyfiki transportu komunikatów np. Diameter mapowanych na strumienie HTTP/2. Dodał czynniki kontekstowe: wrażliwość danych (np. lokalizacja użytkownika) i potencjalne skutki (finansowe, prawne). Wyznaczona wartość wpływa na indeks ryzyka połączenia, która jest podstawą do obliczenia wskaźnika zaufania „trust score" operatora. Adaptowany CVSS uwzględnia grupę metryk, które odzwierciedlają kontekst ataku w czasie rzeczywistym, co jest (lub powinno być) kluczowe w dynamicznych środowiskach międzyoperatorskich. Adaptacja CVSS opracowana przez p. Gómeza stanowi, w moim przekonaniu, nowatorskie podejście do oceny ryzyk a w sieciach mobilnych, w szczególności w kontekście roamingu i ogólniej połączeń międzyoperatorskich.

Autor zdefiniował cztery komponenty: dynamiczną ocenę ryzyka (opartą na analizie wiadomości i sekwencji), wyznaczanie wskaźnika zaufania (ang. trust score) dla operatorów, zdefiniowanie profil bezpieczeństwa dla automatyzacji negocjacji w 5G i w końcu rozszerzenie PCF (ang. Policy Control Function) przez dodanie polityki bezpieczeństwa jako wymiaru równorzędnego z QoS.

Proponowane w dysertacji połączenie tych elementów w jeden cykl życia oznacza możliwość stworzenia zintegrowanego, samouczącego się systemu bezpieczeństwa dla połączeń

międzysieciowych (zwłaszcza roamingu) w 5G. System ten automatycznie wykrywa zagrożenia, dynamicznie tworzy optymalne polityki reakcji i natychmiast je wdraża, a następnie uczy się na podstawie efektów, zamykając pętlę sprzężenia zwrotnego. To fundamentalna zmiana w stosunku do dotychczasowych, rozproszonych i statycznych podejść.

Wymienione wyżej osiągnięcia Autora stanowią istotną oryginalną i nowatorską wartość dodaną w stosunku do wcześniejszego stanu wiedzy.

5. Czy autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników /zwięzłość, jasność, poprawność redakcyjna rozprawy/?

Rozprawa, wraz z bibliografią oraz spisami użytych skrótów, tabel i rysunków, ma objętość 158 stron. Jej układ uważam za dostosowany do tematyki i zakresu badań opisywanych przez Autora. Rozprawa podzielona jest w logiczny sposób na dziesięć rozdziałów, bibliografię oraz spis użytych akronimów, rysunków i tabel. Rozprawa jest przygotowana w języku angielskim. Poprawność redakcyjna nie budzi moich zastrzeżeń. Poziom językowy dysertacji jest bardzo wysoki, więc pojedyncze, drobne uchybienia językowe (np. this article → this dissertation – p. 69) przypisuję omyłkom pisarskim i przedstawianie ich listy uważam za zbędne. Wszystkie argumenty są przedstawione w pracy w sposób zrozumiały, a czytanie rozprawy nie przedstawia trudności, pominąwszy fragmenty np. rozdziału czwartego, które zawierają dużą liczbę symboli i nazw zmiennych (ale to trudność dla czytelnika nieunikniona).

6. Jakie są słabe strony rozprawy i jej główne wady?

Nie dostrzegłem w rozprawie istotnych usterek merytorycznych, ale podczas lektury dysertacji nasunęło mi się kilka uwag krytycznych lub dyskusyjnych:

1. Publikacje Doktoranta są współautorskie, więc powinien on doprecyzować swój indywidualny wkład w ich powstanie. W podrozdziale 1.3 opisano najistotniejsze osiągnięcia każdej z tych publikacji, ale warto byłoby dodać informacje na czym polegał własny wkład Doktoranta.
2. Autor używa pojęcia optymalizacji, ale w znaczeniu potocznym, a nie w ścisłym sensie matematycznym, tj. nie definiuje formalnej funkcji celu, ani nie przedstawia zastosowanych algorytmów optymalizacyjnych. W szczególności, pisząc o Count-Min Sketch, autor używa pojęcia „optymalizacji" parametrów algorytmu (np. długości strumienia danych, dopuszczalnego błędu, prawdopodobieństwa), co ma na celu uzyskanie kompromisu między dokładnością i złożonością obliczeniową. Nie pojawia się formalna funkcja celu, ani procedura jej minimalizacji/ maksymalizacji. Jest to raczej podejście heurystyczne, oparte na analizie eksperckiej. Słowo optymalizacja czasem trudno zastąpić innym, ale Autor powinien zaznaczyć, że w swoich badaniach rozumiał je w znaczeniu potocznym.
3. Ograniczona walidacja: Testy na rzeczywistych danych objęły tylko ruch w protokole Diameter (4G), brak danych 5G z powodu ograniczeń w dostępie do nich. Jest to słabość rozprawy, ale niezawiniona przez jej Autora. Dostęp do rzeczywistych danych od operatorów stanowi znaczącą trudność dla badaczy, co wynika z kombinacji czynników prawnych (ochrona danych osobowych – lokalizacja, zachowania, kontakty – nawet usunięcie metadanych może nie zapewnić pełnej anonimizacji), technicznych (problem z wyodrębnieniem potrzebnych podzbiorów danych z rozproszonych źródeł i różnych formatów danych) i biznesowych (ryzyko reputacyjne operatora).
4. Proponowany schemat bezpieczeństwa nie został przetestowany w środowisku produkcyjnym operatora/operatorów (przeprowadzono natomiast wyżej wymienione testy). To tylko zwrócenie uwagi na to, że zaproponowane rozwiązania nie przeszły jeszcze testów w pełnej skali.

Trzeba zauważyć, że Autor dostrzega ograniczenia wymienione w p. 3 i 4, wspomina o nich w rozdziale 9 i proponuje je jako kierunki przyszłych badań i wdrożeń.

7. Podsumowanie oceny rozprawy i oceny wiedzy doktoranta

Wybór tematyki poruszanej w dysertacji jest w pełni uzasadniony jej aktualnością i dużym znaczeniem praktycznym dla systemów telekomunikacyjnych. Opisane badania odpowiadają na ważne i aktualne zapotrzebowanie dotyczące bezpieczeństwa w sieciach mobilnych, a praca zawiera oryginalne wyniki, które rozszerzyły wiedzę w przedmiotowym zakresie, co podkreślono we wcześniejszych częściach recenzji, omawiających elementy oryginalności.

Autor omawia zagadnienia ujęte w pracy kompetentnie i z uwzględnieniem aktualnego stanu wiedzy. Dowodzą tego między innymi powołane w pracy publikacje – dobrane stosownie do rozważanej tematyki oraz zakresu prowadzonych badań. O kompetencji Autora świadczy, między innymi, jego dorobek publikacyjny, który obejmuje współautorstwo (od 3 do 7 autorów) 5 publikacji związanych tematycznie z omawianą dysertacją, w wydawnictwach i czasopismach o wysokim prestiżu (Wiley, IET, IEEE Transactions on Intelligent Transportation Systems, IEEE Wireless Communications, IEEE Communications Standards Magazine, Computer Communications). Lista publikacji jest następująca:

[1] Mongay Batalla, Jordi, Luis J. de la Cruz Llopis, Germán Peinado Gómez, Elzbieta Andrukiewicz, Piotr Krawiec, Constandinos X. Mavromoustakis, and Houbing Herbert Song, "Multi-Layer Security Assurance of the 5G Automotive System Based on Multi-Criteria Decision Making." IEEE Transactions on Intelligent Transportation Systems 25, no. 5 (May 2024): 3496–3512 (Liczba autorów: 7)

[2] Mongay Batalla, Jordi, Elżbieta Andrukiewicz, German Peinado Gomez, Piotr Sapiecha, Constandinos X. Mavromoustakis, George Mastorakis, Jerzy Żurek, and Muhammad Imran, "Security Risk Assessment for 5G Networks: National Perspective." IEEE Wireless Communications 27, no. 4 (August 2020): 16–22. (Liczba autorów: 7)

[3] Peinado Gomez, German, Jordi Mongay Batalla, Yoan Miche, Silke Holtmanns, Constandinos X. Mavromoustakis, George Mastorakis, and Noman Haider, "Security Policies Definition and Enforcement Utilizing Policy Control Function Framework in 5G." Computer Communications 172 (April 2021): 226–237. (Liczba autorów: 6)

[4] Dhanasekaran, R. M., Jing Ping, and German Peinado Gomez, "End-to-End Network Slicing Security Across Standards Organizations." IEEE Communications Standards Magazine 7, no. 1 (March 2023): 40–47. (Liczba autorów: 4)

[5] Andreou, Andreas, Constandinos X. Mavromoustakis, Houbing Herbert Song, German Peinado Gomez, and Jordi Mongay Batalla, "Transforming Ageing in the Metaverse: Embracing Virtual Communities for Enhanced Well-Being and Empowerment." In Advanced Metaverse Wireless Communication Systems, 457–494. (Liczba autorów: 5).

Co bardzo istotne, Doktorant jest także współautorem (liczba autorów od 2 do 4) trzech patentów:

[1] German Peinado Gomez, Anja Jerichow, Chaitanya Aggarwal, "Security enforcement and assurance utilizing policy control framework and security enhancement of analytics function in communication network." Patent No. (Granted): US 12,126,658 B2. Date of Patent: Oct. 22, 2024. (Liczba autorów: 3).

[2] Anja Jerichow and German Peinado Gomez, "Apparatus, method, and computer program of protecting communications between networks using predefined security profiles." Patent No. (Granted): US 12,192,208 B2. Date of Patent: Jan. 7, 2025. (Liczba autorów: 2).

[3] Borislava Gajic, German Peinado Gomez, Saurabh Khare, and Tejas Subramanya, "Method and apparatus for determining and utilizing a trust indication in mobile networks," US20230413029A1, Dec.21, 2023. (Liczba autorów: 4).

Wprawdzie w.w publikacje i patenty są wieloautorskie, ale telekomunikacja jest obszarem tematycznym, w którym dominuje praca zespołowa. Doktorant wykazał się ważną umiejętnością prowadzenia badań naukowych w zespołach, w tym międzynarodowych. Powyższe osiągnięcia spełniają z nadmiarem wymóg formalny autorstwa publikacji w recenzowanym czasopiśmie. Przyznane patenty są dowodem na aplikacyjny charakter prowadzonych prac.

Recenzowany dorobek jest dowodem dojrzałości naukowej Doktoranta, o czym świadczą wymienione wcześniej oryginalne wyniki, publikacje, patenty, udział w pracach standaryzacyjnych, czy w końcu krytyczna analiza ograniczeń przeprowadzonych badań i ich wyników oraz przedstawienie realistycznych propozycji kierunków ich kontynuacji. Warto dodać, że Kandydat, ze względu na swoje doświadczenie zawodowe, jest ekspertem łączącym wiedzę naukową z techniczną, operacyjną, strategiczną, standaryzacyjną i regulacyjną w zakresie bezpieczeństwa sieci telekomunikacyjnych, w kontekście systemów 2G–5G.

Podsumowując ocenę dysertacji i wiedzy Autora, wykazał się on istotnymi osiągnięciami badawczymi oraz szeroką wiedzą teoretyczną i praktyczną z zakresu dyscypliny informatyka techniczna i telekomunikacja, w której ubiega się o nadanie stopnia doktora.

8. Konkluzja

Po zapoznaniu się z przedłożoną mi do recenzji dysertacją mgr inż. Germána Peinado Gómeza, stwierdzam, że spełnione są wymagania art. 187 ustawy z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2018 r., poz. 1668), z późniejszymi zmianami,, gdzie mowa o oryginalnym rozwiązaniu problemu naukowego, ogólnej wiedzy teoretycznej kandydata w danej dyscyplinie naukowej oraz umiejętność samodzielnego prowadzenia pracy naukowej. W związku z tym, stawiam wniosek o przyjęcie przedłożonego mi do recenzji opracowania jako rozprawy doktorskiej i dopuszczenie mgr inż. Gómeza do dalszych etapów postępowania doktorskiego, w tym do publicznej obrony w dyscyplinie informatyka techniczna i telekomunikacja.

Jednocześnie, wnioskuję o wyróżnienie rozprawy. Praca charakteryzuje się bardzo wysokim poziomem merytorycznym i oryginalnością, w tym prekursorską propozycją dynamicznego modelu bezpieczeństwa dla połączeń międzyoperatorskich w sieciach 2G–5G. Stanowi istotny wkład w dyscyplinę informatyka techniczna i telekomunikacja, potwierdzony patentami oraz publikacjami w prestiżowych czasopismach i wydawnictwach. Zaproponowane rozwiązania mają znaczny potencjał aplikacyjny.

Łódź, 14 czerwca 2025 r.

Sławomir Hausman