RADA NAUKOWA DYSCYPLINY

INFORMATYKA TECHNICZNA I TELEKOMUNIKACJA POLITECHNIKI WARSZAWSKIEJ

zaprasza na

OBRONĘ ROZPRAWY DOKTORSKIEJ

mgr. inż. Germana Peinado Gomeza

która odbędzie się w dniu **16 września 2025 roku,** o godzinie **12:00** w trybie stacjonarnym

Temat rozprawy:

„ *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. inż. Jordi Mongay Batalla – Politechnika Warszawska

Recenzenci: prof. dr hab. inż. Marek Amanowicz – NASK - PIB Warszawa

dr hab. inż. Sławomir Hausman, prof. uczelni – Politechnika Łódzka

dr hab. inż. Marcin Niemiec, prof. uczelni – Akademia Górniczo-Hutnicza w Krakowie

Obrona odbędzie się w sali nr 478 na Wydziale Elektroniki i Technik Informacyjnych Politechniki Warszawskiej, ul. Nowowiejska 15/19, 00-665 Warszawa. Osoby zainteresowane uczestnictwem w obronie proszone są o zgłoszenie chęci uczestnictwa w formie elektronicznej na adres sekretarza komisji: dr hab. inż. Andrzej Bęben, email: andrzej.beben@pw.edu.pl, do dnia 15 września 2025r. godz. 23:59.

Z rozprawą doktorską i recenzjami można zapoznać się w Czytelni Biblioteki Głównej Politechniki Warszawskiej, Warszawa, Plac Politechniki 1.

Streszczenie rozprawy doktorskiej i recenzje są zamieszczone na stronie internetowej: https://www.bip.pw.edu.pl/Postepowania-w-sprawie-nadania-stopnia-naukowego/Doktoraty/Wszczete-po-30-kwietnia-2019-r/Rada-Naukowa-Dyscypliny-Informatyka-Techniczna-i-Telekomunikacja/mgr-inz.-German-Peinado-Gomez

Przewodniczący Rady Naukowej Dyscypliny
Informatyka Techniczna i Telekomunikacja
Politechniki Warszawskiej

prof. dr hab. inż. Jarosław Arabas

Abstract

Mobile Network Operators interconnect their networks to provide roaming services based on Service Level Agreements (SLAs) directly with peers or through roaming intermediaries. The SLAs include security clauses that are translated into security requirements in the interconnection links. Whilst the security architecture in the fifth generation of mobile networks (5G), in comparison with previous generations, has introduced significant advancements towards a new end-to-end security paradigm, the security posture in the interconnection of mobile networks cannot be considered static and solely dependent on policies part of contractual documents. On the contrary, the security posture in this context requires a continuous adaption to the ever-growing interconnection ecosystem and threat landscape, considering the unavoidable coexistence of the three protocol stacks since the beginning of the mobile networks, i.e., SS7 (2G/3G), Diameter (4G) and HTTP/2 (5G).

The primary aim of this research was to build a risk-based security framework capable of anticipating major security issues and reacting to changes in the security level of the interconnection links established between peer Mobile Network Operators and/or roaming intermediaries. To achieve this, I have developed four building blocks, connected to form a comprehensive security lifecycle. Firstly, I have designed a dynamic risk evaluation mechanism at both message and sequence levels using expert knowledge and data mining techniques applied to data streams. As a baseline for computing the risk, I have adopted the Common Vulnerability Scoring System. Secondly, I have proposed a novel approach to determine a trust score for Mobile Networks in roaming context, with risk measurement as the main input. Thirdly, I have introduced the concept of security profiling in 5G interconnection as a catalyzer to implement the new security end-to-end paradigm in 5G. Finally, I have designed a new method to dynamically create and enforce the security policies in the interconnection gateways, acting as enforcement points, by enhancing the current 5G Policy Control framework, making security an actual quality element of the network.

The security framework has been validated with a theoretical key use case such as location tracking, as well as with an anonymized trace of real Diameter signaling traffic between two operators in Asia. Several procedures following the actual 5G-Advanced standardization are provided to demonstrate the adequacy of the novel methods in the 5G system, even when privacy and security

concerns to access the signaling data in interconnection hinder wide academic experimentation in this field.

Keywords: mobile networks, security, roaming, interconnection, signaling, SLA, 3GPP, 5G, 4G, Diameter, HTTP/2, IPX, risk management, data mining, security enforcement, trust score, security profiling.

Prof. dr hab. inż. Marek Amanowicz
NASK – PIB
ul. Kolska 12
01-045 Warszawa

Warszawa, dn. 07.05.2025 r.

Recenzja
rozprawy doktorskiej mgr. inż. German Peinado Gomez
pt. Development of a Risk-based Security Framework for Mobile Networks Interconnection Applied in Roaming Service Level Agreements within the 5G Context.

Przedstawiona do recenzji rozprawa zatytułowana *"Development of a Risk-based Security Framework for Mobile Networks Interconnection Applied in Roaming Service Level Agreements within the 5G Context"* jest efektem doktoratu wdrożeniowego realizowanego przez mgr. inż. German Peinado Gomez pod kierunkiem naukowym prof. dr. hab. inż. Jordi Mongay Batallia oraz dr. Liliann Miche, która była opiekunem pomocniczym ze strony firmy Nokia. Ze względu na szczególny cel takiego doktoratu wymagający rozwiązania konkretnego problemu, z którym zmaga się przedsiębiorca zatrudniający doktoranta, pożądanym jest umieszczanie stosownej informacji w materiałach udostępnianych recenzentowi.

1. Tematyka rozprawy

Rozprawa dotyczy opracowania ramowej struktury bezpieczeństwa bazującej na koncepcji szacowania ryzyka umożliwiającej ocenę stanu bezpieczeństwa w połączeniach sieci mobilnych ustanowionych do realizacji usług roamingowych oraz dynamiczne reagowanie operatora na zidentyfikowane zagrożenia. Doktorant wprowadza także bardzo ważne założenie, że powinny one wpisywać się w architekturę bezpieczeństwa sieci mobilnych piątej generacji oraz uwzględniać współistnienie trzech stosów protokołów stosowanych w sieciach mobilnych kolejnych generacji, tj. SS7, Diameter oraz HTTP/2.

Tematyka rozprawy doktorskiej w pełni wpisuje się w prace badawcze i standaryzacyjne nad rozwojem architektury bezpieczeństwa piątej i szóstej generacji sieci mobilnych i odpowiada aktualnym potrzebom operatorów sieci mobilnych związanych z uwzględnieniem efektywnych mechanizmów bezpieczeństwa w umowach o gwarantowanym poziomie świadczenia usług roamingowych. Jest ona w mojej ocenie ważna z punktu widzenia poznawczego, jak również praktycznego znaczenia przedstawionych rozwiązań.

Doktorant, uwzględniając zidentyfikowane potrzeby i oczekiwania operatorów sieci mobilnej wskazuje na szereg cech, jakimi powinna charakteryzować się struktura bezpieczeństwa oraz formułuje następujące trzy tezy rozprawy:

1. Zaufanie między operatorami sieci mobilnych podczas świadczenia usług roamingu, odzwierciedlone w klauzulach bezpieczeństwa w umowach SLA (ang. Service Level Agreement), musi być stale oceniane poprzez pomiar i kontrolę poziomu ryzyka w łączach sygnalizacyjnych w trzech technologiach współistniejących obecnie w sieciach mobilnych, tj. SS7 (2/3G), Diameter (4G) i HTTP/2 (5G).
2. Złożoność operacyjna wprowadzona przez nowy paradygmat bezpieczeństwa end-to-end w architekturze sieci 5G, gdy granularne polityki bezpieczeństwa mają być uzgadniane między interesariuszami roamingu poprzez pomiar ryzyka i zaufania,

powinna zostać znacznie zmniejszona poprzez wprowadzenie koncepcji profili bezpieczeństwa.

3. Ujednolicone ramy polityki 5G powinny zapewniać skuteczny mechanizm egzekwowania bezpieczeństwa, elastyczny w tworzeniu nowych polityk oraz zwinny, aby reagować na stale zmieniające się środowisko w całej architekturze sieci mobilnej.

Pragnę zauważyć, że są one raczej wymaganiami (wytycznymi) do opracowania architektury bezpieczeństwa dla realizacji usług roamingowych, a nie stricte tezami naukowymi, których prawdziwość należałoby udowodnić w rozprawie. Tym niemniej, dobrze określają one na cele szczegółowe powadzonych badań, których osiągnięcie Doktorant potwierdza w kolejnych rozdziałach rozprawy. Stwierdzam zatem, że problem badawczy został dostatecznie jasno i trafnie sformułowany.

2. Charakterystyka rozprawy

Rozprawa doktorska mgr. inż. Peinado Gomez została napisana w języku angielskim na 159 stronach i składa się z 10 rozdziałów. W rozdziale pierwszym Autor przedstawił tematykę, cele i tezy rozprawy oraz opisał układ pracy. Zawiera on jasno sformułowane powody podjęcia tematu ze wskazaniem na problemy z którymi zmagają się operatorzy sieci mobilnych. Autor zawarł w nim także przejrzystą i spójną metodologicznie koncepcję realizacji badań wraz ze wskazaniem publikacji Autora oraz uzyskanych patentów będących efektem prowadzonych prac.

Wyczerpujący przegląd stanu wiedzy w zakresie tematyki rozprawy Doktorant zawarł w rozdziale 2. Został on przeprowadzony zgodnie z przyjętymi szczegółowymi celami badań, rozpoczynając od przeglądu bieżącego stanu oraz wyzwań związanych z aspektami bezpieczeństwa w realizacji usług roamingowych w ramach architektury poszczególnych generacji sieci mobilnych, poprzez analizę aktualnie wykorzystywanych oraz proponowanych rozwiązań dotyczących:

- oceny ryzyka w sygnalizacyjnych połączeniach międzysieciowych
- oceny poziomu zaufania do sieci i jego wykorzystania w umowach SLA ze stronami uczestniczącymi w roamingu
- określania polityk bezpieczeństwa i profilowania związanych z realizacją usług roamingowych, a także ich egzekwowania.

Na marginesie należy zauważyć, że mgr inż. Peinado Gomez nie wskazuje explicite w rozprawie na rodzaj ocenianego ryzyka. W istocie dokonuje on oceny ryzyka cybernetycznego, choć miejscami odnosi się wrażenie, że utożsamia on ryzyko z możliwością naruszenia bezpieczeństwa realizacji usług roamingowych ze względu na luki (podatności) występujące w infrastrukturze oraz w procedurach.

Dokonując przeglądu, Doktorant odwoływał się do wielu dokumentów standaryzacyjnych i analiz technicznych, w tym prezentowanych w prasie specjalistycznej, oraz publikacji w czasopismach i materiałach konferencji naukowych. W efekcie zidentyfikował on szereg luk oraz wyzwań związanych z zapewnieniem wysokiego poziomu bezpieczeństwa świadczonych usług roamingowych. Szkoda tylko, że rozdział ten nie zawiera syntetycznego ich podsumowania ze wskazaniem, które ze zidentyfikowanych luk zostają wypełnione przez mechanizmy zaproponowane w rozprawie.

Rozwinięte uzasadnienie opracowania struktury bezpieczeństwa dla wzajemnych połączeń sieci mobilnych bazującej na ocenie ryzyka cybernetycznego i uwzględniającej współistnienie

trzech standardów sygnalizacji połączeń międzysieciowych Autor rozprawy przedstawił w rozdziale 3. Zawiera on przejrzysty, wysokopoziomowy schemat proponowanego rozwiązania wraz z opisem poszczególnych jego komponentów, które szczegółowo zostały omówione w kolejnych częściach rozprawy. Przyjęte przez Doktoranta założenia nie budzą zastrzeżeń. Istotną cechą jego propozycji jest wymóg jej realizowalności nie tylko w stosach protokołów połączeń międzysieciowych w obecnie występujących sieciach mobilnych, ale także możliwość jej zastosowania w kolejnych ich generacjach.

W rozdziale 4 Doktorant przedstawił oryginalne podejście do dynamicznej oceny ryzyka cybernetycznego w sygnalizacyjnych połączeniach międzysieciowych, która stanowi kluczowy element proponowanej struktury bezpieczeństwa i jest podstawą specyfikacji pozostałych jej komponentów. Ocenę poziomu zagrożeń dokonuje on poprzez analizę poszczególnych wiadomości sygnalizacyjnych wymienianych pomiędzy operatorami w różnych schematach połączeń międzysieciowych oraz analizę sekwencji w ruchu sygnalizacyjnym, co pozwala między innymi na ocenę poziomu zaufania do operatora. Wskazanym byłoby wyjaśnienie, jak uwzględnia się zmiany poziomu zaufania do operatora wynikające z dynamiki zaistniałych zdarzeń bezpieczeństwa (np. działań oponenta), a także sposobu określania wartości parametru delta, o którym mowa na stronach 62 i 63. Bazując na notacji wprowadzonej w początkowej części tego rozdziału, Doktorant wprowadza także formalny opis zaproponowanych procedur. W analizach proponuje on wykorzystanie różnorodnych metod i technik pozwalających na dogłębną identyfikację i ocenę potencjalnych czynników ryzyka. Zaprezentowane ujęcie tego fragmentu rozprawy uważam za niezwykle interesujące i wskazujące na bardzo dobre rozeznanie przez Autora realnych zagrożeń wpływających na bezpieczeństwo świadczenia usług roamingowych. W rozdziale 4.3 zaproponował on metodę dynamicznego szacowania ryzyka na poziomie wiadomości, sekwencji oraz każdego łącza międzysieciowego będącą analogią podejścia stosowanego w systemach teleinformatycznych wykorzystującego standard CVSS. Ponieważ standard ten nie obejmuje systemów telekomunikacyjnych, Autor zaproponował własne rozwiązanie obejmujące miary podstawowe oraz miary zagrożenia. Pożądanym byłoby wskazanie powodów, dla których nie uwzględnił on miar środowiskowych i dodatkowych występujących w tym standardzie.

Doktorant słusznie stwierdza (str. 78), że wartość ryzyka jest funkcją poziomu narażenia wynikającego z wartości wskaźnika CVSS oraz potencjalnych konsekwencji wyrażonych ważoną sumą wrażliwości przekazywanych danych i wywoływanego skutku. Jednakże nie wskazuje on jak należałoby wyznaczać te wagi. Nie podaje on również jakie wartości mogą przyjmować wskaźniki wrażliwości oraz skutku, a także reguł ich wyznaczania. Autor stwierdza, że ryzyko jest oceniane w sposób ciągły na każdym etapie analizy bezpieczeństwa na poziomie wiadomości i sekwencji dla uzyskania wyniku w czasie quasi-rzeczywistym dla każdego łącza międzysieciowego. W tym kontekście interpretacji wymaga użycie pojęcia „ciągłość oceny". Do wyznaczenia ogólnej wartości wskaźnika CVSS Doktorant zaproponował kilka rozwiązań, w tym średnią ważoną wskaźników CVSS, maksymalną wartość wskaźnika oraz skumulowany wpływ, jednakże bez wskazania, które rozwiązanie i w jakich sytuacjach należałoby stosować.

Zgodnie z prezentowaną w rozprawie koncepcją, wynik oceny ryzyka w połączeniach międzysieciowych stanowi podstawę wyznaczenia poziomu zaufania względem każdej sieci uczestniczącej w roamingu. Autor rozprawy opisuje w rozdziale 5 koncepcję określania takiego wskaźnika, którego wykorzystanie powinno wspierać operatora sieci mobilnej w podejmowaniu decyzji dotyczących stosowanych polityk i profili bezpieczeństwa oraz ich egzekwowania. Doktorant stwierdza na str. 82, że koncepcja tworzenia wyniku zaufania

opracowana w ramach prowadzonych przez niego badań jest chroniona patentem, którego jest on współautorem, oraz dodaje na str. 86, że „określenie wyniku zaufania uzupełnia odpowiedź na tezę 1 niniejszej rozprawy, przekształcając pomiar ryzyka w wynik zaufania dla każdego połączonego MNO i/lub pośrednika roamingu". Jednakże należy zauważyć, że takie przekształcenie nie zostało jednak explicite przedstawione w rozprawie.

Doktorant w kolejnych dwóch rozdziałach w sposób uzasadniony ogranicza swoje rozważania wyłącznie do sieci 5G celem wykorzystania zdefiniowanej dla nich struktury sterowania polityką bezpieczeństwa, która wspiera tworzenie różnego rodzaju spójnych reguł obejmujących całą sieć oraz ich udostępnianie innym funkcjom sieciowym płaszczyzny sterowania. Na podkreślenie zasługuje, że zaprezentowana w rozprawie koncepcja tworzenia profili bezpieczeństwa została opatentowana oraz wdrożona w specyfikacji standardów odpowiadających 5G-Advanced. Stanowi to jednoznaczne potwierdzenie istotności zaproponowanego rozwiązania oraz jego innowacyjności. Z kolei w rozdziale 7 Doktorant przedstawił oryginalne rozwiązanie pozwalające na dynamiczne egzekwowanie polityki bezpieczeństwa w bramach międzysieciowych. Zostało ono także opatentowane oraz opisane w artykule naukowym mającym już kilkanaście cytowań.

Rozdział 8 rozprawy został zatytułowany „Walidacja proponowanej struktury bezpieczeństwa". Przyjmuje się, że walidacja jest działaniem mającym na celu zbadanie odpowiedniości, trafności lub dokładności proponowanego rozwiązania. W przypadku recenzowanej rozprawy celem walidacji byłoby sprawdzenie, czy i w jakim stopniu zaproponowane rozwiązania umożliwiają ocenę stanu bezpieczeństwa w połączeniach sieci mobilnych ustanowionych do realizacji usług roamingowych oraz dynamiczne reagowanie operatora na zidentyfikowane zagrożenia. Pożądanym byłoby sformułowanie kryteriów takiej oceny. Należy zauważyć, że Autor dokonuje oddzielnej walidacji poszczególnych komponentów proponowanej struktury bezpieczeństwa. W przypadku oceny ryzyka przedstawia on wyniki analizy dla dwóch wybranych przypadków użycia tj. hipotetycznego oraz bazującego na zanonimizowanych danych rzeczywistych. Walidacja mechanizmu określającego poziom zaufania jest przeprowadzona poprzez opis wybranej opcji wdrożenia procedury, a walidacja pozostałych komponentów sprowadza się do opisu ich implementacji w rozszerzeniach standardów zdefiniowanych w specyfikacjach 3GPP. Osobiście oczekiwałbym, że Doktorant zdefiniuje co najmniej jeden przypadek użycia i konsekwentnie przeprowadzi czytelnika poprzez kolejne komponenty proponowanego rozwiązania, poczynając od oszacowania ryzyka, poprzez wynikający z niego poziom zaufania do operatorów, aż do dynamicznego wymuszenia polityki bezpieczeństwa, potwierdzając tym samym skuteczność reagowania operatora na zagrożenia bezpieczeństwa. Tym niemniej, sposób w jaki Autor dokonuje walidacji proponowanych rozwiązań umożliwia potwierdzenie spełnienia wymogów ujętych w tezach rozprawy.

W rozdziale dziewiątym, Autor opisał ograniczenia wynikające z przyjętej koncepcji struktury bezpieczeństwa i sposobu prowadzenia analiz. Wskazał także na potencjalne obszary dalszego rozwoju proponowanych mechanizmów oraz problemów wymagających przeprowadzenia szczegółowych badań. Ostatni rozdział rozprawy zawiera syntetyczne podsumowanie najbardziej istotnych innowacyjnych elementów rozprawy ze wskazaniem, które zaprezentowane rozwiązania odnoszą się do zdefiniowanych na wstępie tez.

3. Ocena rozprawy

Mgr inż. Penaido Gomez podjął się rozwiązania złożonego zdania związanego z opracowaniem kompleksowego podejścia do budowy struktury bezpieczeństwa w sygnalizacyjnych

połączeniach międzysieciowych oraz zaproponowania rozwiązań umożliwiających dynamiczne reagowanie operatów na występujące zagrożenia. Jego złożoność wynika także z potrzeby zapewnienia spójności tworzonych mechanizmów z rozwijaną obecnie architekturą bezpieczeństwa systemów piątej i kolejnych generacji sieci mobilnych. Dla rozwiązania tego zadania Autor w sposób poprawny sformułował problem badawczy określając jego cel ogólny oraz cele szczegółowe. Przyjętą przez Doktoranta ogólną koncepcję struktury bezpieczeństwa w sygnalizacyjnych połączeniach międzysieciowych uważam za niezwykle interesującą, pozwalającą uwzględniać współistnienie różnych stosów protokołów sygnalizacyjnych stosowanych w sieciach mobilnych kolejnych generacji oraz tworzyć zbiór powiązanych ze sobą mechanizmów bezpieczeństwa.

Bibliografia rozprawy obejmuje 115 pozycji, w tym: 47 prac naukowych, z których istotna część została opublikowana w ostatnich latach w wysoko punktowanych czasopismach lub była prezentowana na prestiżowych konferencjach naukowych, 10 powołań na artykuły w czasopismach specjalistycznych omawiające zagrożenia wynikające z luk bezpieczeństwa w połączeniach międzysieciowych, 55 powołań na dokumenty standaryzacyjne i rekomendacje, głównie 3GPP, GSMA, IETF, a także 3 powołania na patenty będące efektem badań prowadzonych przez Autora. Stanowi ona reprezentatywny przegląd aktualnego stanu wiedzy w zakresie tematyki rozprawy, świadczy o dobrej znajomości współczesnej literatury oraz osiągnięć naukowych, a także ich wykorzystania do rozwiązania postawionego problemu.

Przyjętą przez Autora rozprawy metodykę prowadzenia badań oraz przyjęte rozwiązania uważam za odpowiednie dla osiągnięcia celu rozprawy. Mechanizmy zaproponowane przez Autora wykorzystują zawansowane metody analizy i przetwarzania danych świadczące o bardzo dobrej znajomości architektur sieci mobilnych i uwarunkowań ich użycia. Na podkreślenie zasługuje, że zaproponowane przez Doktoranta rozwiązania cechuje wysoki poziom innowacyjności, potwierdzony między innymi przyznanymi patentami międzynarodowymi oraz ich praktyczne znaczenie dla operatorów sieci mobilnych w zakresie zapewnienia bezpieczeństwa realizacji usług roamingowych. Wykorzystanie opracowanego przez Doktoranta mechanizmu profilowania w rozwijanym obecnie standardzie bezpieczeństwa sieci mobilnych piątej generacji stanowi potwierdzenie walorów użytkowych rozprawy. Uwzględniając ponadto ogólną poprawność prowadzonych wywodów i dyskusji uzyskanych wyników stwierdzam, że mgr inż. German Peinado Gomez potwierdził swoją rozprawą posiadanie umiejętności skutecznego prowadzenia badań naukowych.

Do oryginalnych elementów rozprawy zaliczam:

- opracowanie kompleksowej struktury bezpieczeństwa w sygnalizacyjnych połączeniach międzysieciowych uwzględniającej współistnienie różnych stosów protokołów sygnalizacyjnych stosowanych w sieciach mobilnych kolejnych generacji oraz tworzącej zbiór powiązanych ze sobą mechanizmów bezpieczeństwa

- sposób oceny zagrożeń występujących w sygnalizacyjnych połączeniach międzysieciowych z wykorzystaniem wiedzy eksperckiej oraz analizy online strumieni danych przesyłanych w wiadomościach sygnalizacyjnych

- opracowanie metody dynamicznej oceny ryzyka cybernetycznego w sygnalizacyjnych połączeniach międzysieciowych

- opracowanie, wpisujących się w istniejące ramy architektury sieci piątej generacji, mechanizmów oceny poziomu zaufania do sieci uczestniczących w roamingu, uzgadniania

profili bezpieczeństwa w umowach o gwarantowanym poziomie świadczenia usług oraz wymuszania w bramach międzysystemowych przyjętej polityki bezpieczeństwa.

Układ rozprawy jest przejrzysty, a sposób prowadzenia narracji nie budzi zastrzeżeń. Jednakże bardzo duża liczba skrótów (161) używanych w tekście rozprawy znacznie utrudnia jej czytanie. Pożądanym byłoby, aby Autor częściej stosował pełne rozwinięcia tych terminów. Czytelność teksty poprawiłoby także numerowanie równań oraz zamieszczenie wykazu użytych symboli matematycznych. Szereg uwag zgłoszonych przeze mnie w poprzednim punkcie niniejszej recenzji, w tym wskazujących na potrzebę użycia bardziej precyzyjnych i uzasadnionych sformułowań nie wpływa na moją wysoką ocenę rozprawy.

4. Wniosek końcowy

Stwierdzam, że przedstawiona do recenzji rozprawa stanowi oryginalne rozwiązanie sformułowanego przez jej Autora problemu badawczego i potwierdza posiadanie przez mgr. inż. German Peinado Gomez wiedzy w zakresie nauk inżynieryjno-technicznych oraz w obszarze telekomunikacji niezbędnej do ubiegania się o nadanie stopnia naukowego doktora. Rozprawę doktorską oceniam jako z nadmiarem spełniającą wymagania stawiane rozprawom doktorskimi oraz wnoszę o jej dopuszczenie do publicznej obrony.

Ponadto, uwzględniając aktualność oraz znaczenie pojętej przez Autora tematyki dla zapewnienia bezpieczeństwa realizacji usług roamingowych i wsparcia działań operatorów sieci mobilnych, kompleksowość ujęcia problemu badawczego, innowacyjność i wysoki poziom merytoryczny zaproponowanych rozwiązań oraz potwierdzone ich walory użytkowe, wnioskuję w wyróżnienie rozprawy.

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

dr hab. inż. **Marcin Niemiec**, prof. AGH
Instytut Telekomunikacji
Wydział Informatyki, Elektroniki i Telekomunikacji
Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie
al. Mickiewicza 30
30-059 Kraków
tel. 12 617 48 03
niemiec@agh.edu.pl

Kraków, 28.05.2025

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

Tytuł rozprawy: Development of a Risk-based Security Framework for Mobile Networks Interconnection Applied in Roaming Service Level Agreements within the 5G Context

Autor rozprawy: mgr inż. German Peinado Gomez

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

Rozprawa doktorska dotyczy problematyki bezpieczeństwa w połączeniach pomiędzy sieciami komórkowymi. Operatorzy sieci zawierają umowy o gwarantowanym poziomie świadczonych usług w celu zapewnienia roamingu. Jednak bezpieczeństwo takich połączeń jest ciągle aktualnym wyzwaniem, bez względu na generację sieci komórkowej (2G/3G, 4G czy 5G). W szczególności istnieje potrzeba opracowania mechanizmów umożliwiających dynamiczną reakcję i adaptację odpowiednich rozwiązań bezpieczeństwa do bieżących warunków w łączu.

W celu zwiększenia bezpieczeństwa połączeń międzyoperatorskich, Autor rozprawy zaproponował podejście bazujące na szacowaniu ryzyka związanego z obsługiwanym ruchem. Postawiono tezę, iż zaufanie między operatorami połączonych sieci komórkowych powinno być oceniane poprzez ciągłą weryfikację poziomu ryzyka w łączach sygnalizacyjnych połączeń międzyoperatorskich, obejmując współistniejące obecnie technologie w sieciach mobilnych, tj. SS7 (2G/3G), Diameter (4G) oraz HTTP/2 (5G). Poza tym, oszacowany poziom ryzyka może posłużyć do dalszych działań w celu zwiększenia efektywności czy bezpieczeństwa. Podejście bazujące na zastosowaniu zdefiniowanych uprzednio profili bezpieczeństwa może spowodować bardziej efektywne ustalanie parametrów bezpieczeństwa charakteryzujące dane łącze, w porównaniu do podejścia z dynamiczną negocjacją takich parametrów. Z kolei wiedza na temat bieżącego poziomu ryzyka w łączu międzyoperatorskim może być wykorzystana do dynamicznego utworzenia i egzekwowania adekwatnej polityki bezpieczeństwa.

Tak przedstawione zagadnienie naukowe zostało dostatecznie jasno sformułowane przez Autora oraz przedstawia ważne i aktualne zagadnienie badawcze we współczesnej telekomunikacji. Rozprawa ma głównie charakter teoretyczny (opis koncepcji), choć praktyczny aspekt badań potwierdzają przeprowadzone przez Autora działania standaryzacyjne.

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?**

Wprowadzenie do tematyki bezpieczeństwa połączonych sieci komórkowych znajduje się w drugim rozdziale rozprawy. Ta część szczegółowo opisuje podejścia do ochrony łączy międzyoperatorskich dla kolejnych generacji: sieci 2G/3G (głównie bazujące na zaporach sieciowych), 4G (protokół Diameter) oraz architekturze bezpieczeństwa dla sieci 5G. Rozwiązania te zostały opisane szczegółowo, co potwierdza dużą wiedzę Autora w tematyce rozprawy doktorskiej. Prawdopodobnie dlatego w tekście zdarzają się pewne określenia nieformalne/kolokwialne, stosowane raczej w środowisku firmowym niż akademickim, np. "*firewalling functionalities*", "*down to the bit level*", "*something digestible*" czy "*ZTA lingo*", a także nazewnictwo typu: „*confidentiality and integrity protected*" czy „*end-to-end integrated protected*". Aby dopełnić tą część, warto byłoby dokładnie wyjaśnić schematy na rysunkach przedstawiających architekturę bezpieczeństwa różnych generacji sieci komórkowych, np. rysunek 2.1.2-1 (generacja 4G) czy rysunek 2.3-1 (generacja 5G).

Wspomniany rozdział 2 rozprawy zawiera także istotną część analizy literaturowej bezpośrednio związanej z tematyką rozprawy. Pozostałe części analizy znajdują się w innych miejscach – głownie w rozdziale 4 („*4.2.3.1 Streaming data preprocessing*" czy „*4.2.3.2 Data mining*") oraz w końcowej części opisującej możliwe kierunki dalszych badań. Wprawdzie poruszana tematyka jest obecnie intensywnie rozwijana i można byłoby odwołać się do większej liczby prac, ale przedstawiona analiza źródeł jest wystarczająca. Przeprowadzono ją w sposób właściwy, a wnioski sformułowane na jej podstawie są jasne i przekonywujące. Umiejscawia to rozprawę na tle innych badań w dziedzinie oraz właściwie identyfikuje problem badawczy. Autor w bibliografii zamieścił również 9 własnych prac związanych z tematem swojej rozprawy doktorskiej (prace opublikowane w ciągu ostatnich sześciu lat), w tym uzyskane patenty.

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

Postawione zagadnienie badawcze zostało rozwiązane przez Autora rozprawy. Zaproponowany został autorski model/struktura bezpieczeństwa dla łączy międzyoperatorskich w sieciach komórkowych. Składa się on z kilku elementów, wśród których kluczowym jest pierwszy – odpowiedzialny za analizę bezpieczeństwa ruchu sygnalizacyjnego w takim łączu i na podstawie szczegółowej weryfikacji poszczególnych wiadomości oraz całych sekwencji danych szacujący poziom ryzyka. Kolejne elementy modelu – na podstawie przeprowadzonej analizy bezpieczeństwa i oszacowanym ryzyku – są w stanie określić poziom zaufania do poszczególnych jednostek w sieci, wybrać adekwatny profil bezpieczeństwa by ułatwić negocjacje parametrów bezpieczeństwa, a także dynamicznie ustalić i egzekwować odpowiednie polityki bezpieczeństwa. Autor założył, że model ma być możliwy do zastosowania w różnych generacjach sieci komórkowych. Metody badawcze wybrano właściwie, a formalny opis modelu oraz analiza przykładowych scenariuszy w większości potwierdzają, że autorski mechanizm stanowi rozwiązanie postawionego zagadnienia. Jednak zarówno formalny opis jak i weryfikacja modelu zawierają pewne nieścisłości, które zostały opisane poniżej.

W rozprawie najlepiej opisany został pierwszy element autorskiego modelu bezpieczeństwa, odpowiedzialny za szacowanie ryzyka. Jednak formalny zapis zawiera pewne niejednoznaczności (np. z opisu na str. 47 wynika, że atrybut może być formalnie reprezentowany zarówno przez $A^{(j)}$ jak i samo j) czy kolizje oznaczeń (np. symbol małej delty został użyty zarówno jako tzw. „*risk factor*" jak i "*desired probability level*". Poza tym, w rozdziale 4 ryzyko jest rozważane dość niekonsekwentnie w poszczególnych fragmentach – od bardzo ogólnego, poprzez zgrubne szacowanie (np. wysokie czy niskie ryzyko), po dokładną liczbową

wartość współczynnika ryzyka. Zaskakuje także niejednorodność opisu poszczególnych elementów modelu bezpieczeństwa. Niektóre zostały zaprezentowane bardzo ogólnikowo, bez formalnego opisu, np. eksploracja danych, gdzie na końcu znajduje się wprost zalecenie: „*Future implementers are kindly invited to test those and other similar algorithms, and accordingly select the most suitable for their environments*". Z drugiej strony, np. na str. 48 znajduje się bardzo dokładny opis trzech różnych model strumieni danych, które w późniejszych rozdziałach nie są wprost używane (a tym bardziej nie wiadomo dlaczego są tam rozpatrywane bardzo specyficzne warunki, jak choćby założenie że $F_t[j'] = F_{t-1}[j']$ dla wszystkich $j' \neq j$). W przypadku weryfikacji zaproponowanego modelu bezpieczeństwa, pewien niedosyt pozostawia brak implementacji modelu (lub jego kluczowych elementów) oraz przeprowadzenie kompleksowej weryfikacji funkcjonalnej. Po części jest to spowodowane brakiem dostępu do rzeczywistego ruchu, ale nawet bazując na posiadanych próbkach ruchu, można byłoby przeprowadzić ocenę działania choćby poszczególnych elementów modelu. Zamiast tego Autor zdecydował się na przedstawienie kilku przykładowych i raczej prostych scenariuszy użycia.

Pomimo wspomnianych niedoskonałości zastosowanych metod badawczych, ostatecznie Autor potwierdził, że można zaprojektować model bezpieczeństwa, dzięki któremu zaufanie między operatorami połączonych sieci komórkowych będzie oceniane poprzez ciągłą weryfikację poziomu ryzyka w łączach międzyoperatorskich. Z kolei podejście bazujące na zastosowaniu zdefiniowanych uprzednio profili bezpieczeństwa może spowodować bardziej efektywne ustalenie parametrów bezpieczeństwa danego połączenia, w porównaniu do podejścia z dynamiczną negocjacją takich parametrów. Ostatecznie wiedza na temat aktualnego poziomu ryzyka może być wykorzystana do dynamicznego utworzenia i egzekwowania adekwatnej polityki bezpieczeństwa dla ruchu w łączu międzyoperatorskim. Dla ścisłości należy wspomnieć, że tezy są postawione dość radykalnie i według recenzenta zamiast określeń „*needs to*" czy „*should*" raczej powinny sugerować, że mechanizmy zaproponowane w rozprawie mogą rozwiązać pewne problemy z bezpieczeństwem czy wydajnością (nie wykazano jednoznacznie, że zaproponowane podejścia są najlepsze). Jednak opracowany model z pewnością pomaga zwiększyć poziom bezpieczeństwa połączeń pomiędzy sieciami komórkowym.

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?

Oryginalny dorobek opisany w rozprawie doktorskiej dotyczy przede wszystkim opracowania kompletnego modelu/struktury bezpieczeństwa dla łączy międzyoperatorskich w sieciach komórkowych. Oryginalny dorobek bardzo dobrze podsumowuje rozdział 3, a szczególnie rysunek 3.2-1, na którym nie tylko zaprezentowano poszczególne elementy modelu, ale także zwizualizowano w jaki sposób są od siebie zależne (Autor wspomniał o podejściu, gdzie działanie elementów składowych modelu można potraktować jako kompleksowy cykl życia zabezpieczeń). Samodzielny wkład Autora rozprawy jest istotny oraz oryginalny w stosunku do stanu wiedzy i poziomu techniki. Szkoda tylko, że w rozprawie brak informacji jaki jest autorski wkład we wspólne prace z innymi współautorami (np. patenty), na które powołuje się Autor, np. „*Our patented solution [11] provides...*". Recenzent wyodrębnił najważniejsze oryginalne elementów rozprawy, które zostały krótko podsumowane poniżej.

- Autor rozprawy zaproponował formalny schemat analizy poszczególnych wiadomości w łączu międzyoperatorskim, w skład którego wchodzi kilka kryteriów oceny (np. źródło pochodzenia wiadomości, protokół, itd.), a także schemat analizy całych sekwencji wiadomości, gdyż na ich podstawie można uzyskać dodatkową wiedzę, niedostępną w procesie analizy jedynie pojedynczych wiadomości w łączu międzyoperatorskim.

- Na podstawie wyników analizy wiadomości oraz sekwencji wiadomości, zaproponowana została metoda szacowania ryzyka w sposób ilościowy. Sposób określenia

poszczególnych wartości bazuje na podejściu CVSS (*Common Vulnerability Scoring System*). Według recenzenta, szczególnie interesujące są dwa współczynniki: „*Data Sensitivity (DS)*" oraz „*Potential Impacts of the Vulnerability (PIV)*" oraz wyliczony na ich podstawie współczynnik CF_i. Na uwagę zasługuje także sposób wyliczenia współczynnika ryzyka oraz próba skorygowania liczbowej wartości ryzyka dla niektórych zdarzeń/podatności.

- Zaproponowana została koncepcja wykorzystania oszacowanego ryzyka do takich celów jak: określenie poziomu zaufania do poszczególnych jednostek w sieci, wybór adekwatnego profilu bezpieczeństwa w celu ułatwienia negocjacji parametrów bezpieczeństwa dla połączenia czy dynamiczne ustalanie i egzekwowanie odpowiednich polityk bezpieczeństwa.

- Przeanalizowano sposób działania wybranych mechanizmów w przykładowych scenariuszach, przede wszystkim przedstawiono oszacowanie ryzyka w teoretycznym scenariuszu ze śledzeniem lokalizacji oraz bardziej praktycznym, w którym zaprezentowano wyniki badań bazujących na rzeczywistym ruchu międzyoperatorskim. Przedstawiono także przykłady (wysokopoziomowe, bez szczegółów) związane z profilami ochrony danych oraz ustaleniem nowej polityki bezpieczeństwa.

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

Autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników, ale poziom językowy i edycyjny rozprawy niestety nie jest najwyższy. W tekście można znaleźć wiele błędów językowych, ale na szczęście w większości nie wpływają one negatywnie na zrozumienie zawartości merytorycznej pracy. Autor niepotrzebnie zapisuje niektóre nazwy stosując dużą literę w środku zdania (np. „*field of Security*"), często robiąc to zupełnie niekonsekwentnie (np. „*in the core network*", „*in the Core Network*", „*of the Core networks*"). Zapis nazwy protokołu bywa różny: „Diameter" oraz „diameter". Niekonsekwentny (a czasami błędny pod względem jezykowym) jest również zapis w przypadku odnośników do rozdziałów (np. „*in Sections 3-7*", „*section 4.2.2*", „*in Chapter 4*", „*in chapter 6*" „*subchapter 6.2*", „*the subchapter 8.2*". Podobnie brak jest konsekwencji w zapisie zmiennych: „the $_t$th item", „the $i-_t h$ signalling message" lub bez kursywy „the ith transaction". Opisując nowe rozwiązania, Autor stosuje czasem formę zdań w pierwszej osobie liczby pojedynczej („*I highlight...*") a czasem mnogiej („*we highlight...*"). W pracy występują jednozdaniowe akapity czy zdania niepoprawne językowo (np. brak orzeczenia w zdaniu „*Diameter message manipulation, Attribute Value Pair (AVP) doubling.*"). Częste są także problemy z interpunkcją, (np. poprzez zastosowanie dwukropka tabela na str. 56 jest potraktowana jak część zdania).

Strona edytorska dokumentu powinna być bardziej staranna. W rozprawie zdarzają się mało czytelne rysunki (np. bardzo mała czcionka na rysunku 4.2.2-1) czy brak opisu poszczególnych kroków na rysunkach 7.2.2-1 oraz 8.2-2. Rysunki i tabele występują w różnych stylach. Niekonsekwentna jest także edycja dokumentu jako całości, np. czasem rozdziały drugiego poziomu są rozpoczynane od nowej strony (np. pusta połowa strony przed rozdziałem 6.3), a czasem nie (np. wcześniejszy podrozdział 6.2). Pewne zamieszanie wprowadzają cytowania rysunków i tabel wraz z oryginalnymi oznaczeniami w rozdziale 8.4. Brak konsekwencji w zapisie tytułów rysunków (czasem wyrazy są pisane małą, a czasem dużą) i w tytułach tabel (np. tabela 8.2-1 ma tytuł pisany dużymi literami). W spisie skrótów niepotrzebnie niektóre skróty są pisane kursywą. Również zapis poszczególnych pozycji w bibliografii powinien być lepiej zredagowany, np. brak daty dostępu w przypadku linków internetowych, niektóre pozycje to tylko link bez żadnych innych informacji (np. [35]), czasem brak dokładnej daty wydania (np. kiedy odbyło się wydarzenie [60] czy na którą wersję publikacji [63] powołuje się Autor).

Wspomniane problemy w pewnym stopniu obniżają jakość pracy, ale należy podkreślić, że tekst nie zawiera poważnych błędów merytorycznych. Nawet podczas uważnego czytania rozprawy można znaleźć jedynie kilka drobnych błędów tego rodzaju, które jednak można potraktować jako niezamierzone literówki, a nie błędy merytoryczne, np. na rysunku 3.1-1 zamiast nazwy „N" powinno być „N32", na rysunku 4.2.2-1 jest literówka „*roamin-in*", na str. 53 zamiast „(0 ... 0 1 1 0 0)" w podanym przykładzie powinien być zapis „(0 0 1 1 0 0)", czy drobny błąd w oznaczeniu "*as indicated in subchapter 3.3*" (prawdopodobnie Autor chciał wskazać na rozdział 4.3). Zatem podsumowując – rozprawa została napisana językiem zrozumiałym, a wspomniane problemy nie zmieniają ogólnej pozytywnej oceny rozprawy.

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

O pewnych słabych stronach rozprawy (np. niejednoznaczności w formalnym opisie, błędy językowe czy niedoskonałości związane ze strukturą rozprawy i stroną edytorską) wspomniano już w poprzednich punktach. Poniżej przedstawione zostały uwagi merytoryczne, które według recenzenta są kluczowe dla ocenianej rozprawy doktorskiej.

- Aby określić poziom ryzyka w sposób ilościowy, Autor używa podejścia bazującego na CVSS. Jednak CVSS określa w sposób liczbowy wagę danej podatności, a nie miarę ryzyka związanego z konkretnym zdarzeniem. Choć ryzyko jest pojęciem trudnym do zdefiniowania w sposób całkowicie jednoznaczny, zwykle szacowane jest na podstawie prawdopodobieństwa wystąpienia oraz wpływu danego zdarzenia na rozpatrywany system. Z tego względu w rozprawie niejasne jest przejście od oszacowania wagi podatności przy użyciu CVSS do wartości współczynnika ryzyka. Również sam formalny opis nie pomaga w określeniu ostatecznego algorytmu ustalania tej wartości, gdyż niejasne jest co się dzieje z wartością R_i (jak wpływa ona na końcową wartość ryzyka czy jaka relacja występuje pomiędzy R_i oraz *Overall Score*), a także dlaczego Autor zakłada akurat proste mnożenie wartości $CVSS_i$ i CF_i.
  Dodatkowo, w rozprawie brakuje także umotywowania decyzji Autora co do wyboru niektórych wartości w tabeli 4.3-1 (przede wszystkim tych w kolumnie *Corrected*) czy co do danych branych pod uwagę w analizie statystycznej sekwencji wiadomości sygnalizacyjnych. Bez wyjaśnienia powodów, podjęte decyzje wydają się mocno arbitralne (jako przykład można zacytować fragment: „*this dissertation considers just what I judge as the most important one in the proposed security analysis*".

- Rozpatrując drugi element zaproponowanego modelu bezpieczeństwa, pewien niedosyt sprawia brak formalnego opisu jak przejść od oszacowanego poziomu ryzyka (pierwszy element modelu) do zaufania do pojedynczej jednostki, które będzie określone w sposób ilościowy (tzw. „*transforming the measurement of the risk into a trust score*").

- Element trzeci modułu bezpieczeństwa zakłada zastosowanie wcześniej zdefiniowanych profili bezpieczeństwa, zawierających określone zestawy parametrów bezpieczeństwa. Zamiast negocjować poszczególne parametry, zakładamy wybór odpowiedniego profilu. Jednak założono, że profile te są odpowiednio uszeregowane, tak aby obie strony transmisji mogły wybrać najbardziej odpowiedni zestaw. Pojawia się zatem pytanie czym się różni takie podejście (a jeśli tak to na ile jest to istotna różnica) od typowej negocjacji parametrów, jaką można spotkać w rozwiązaniach typu IKE (*Internet Key Exchange*) i SA (*Security Association*) czy w protokole TLS (*Transport Layer Security*).

- Słabą stroną rozprawy jest brak obiektywnej oceny zaproponowanego modelu bezpieczeństwa. W zasadzie wyniki zaprezentowane w rozdziale 8 nie są walidacją czy weryfikacją funkcjonalną modelu lub jego poszczególnych elementów, ale stanowią prezentację przykładowych scenariuszy użycia. Jeden scenariusz jest mocno teoretyczny, a jedynie drugi bazuje na danych rzeczywistych. Brak jest prawdziwej

implementacji modelu bezpieczeństwa, a następnie jego weryfikacji funkcjonalnej, badań poszczególnych scenariuszy w różnych środowiskach, dogłębnej analizy czy słusznie wybrano poszczególne wartości ryzyka, badań nad dostosowaniem progów na podstawie danych rzeczywistych, do których miał dostęp Autor, itd. Poza tym niektóre z fragmentów rozdziału 8 nie są związane z testowaniem opracowanych rozwiązań (np. rozdział 8.3 nie tylko nie jest walidacją rozwiązania, ale także nie jest scenariuszem użycia, więc raczej powinien być częścią rozdziału 5).

7. Jaka jest przydatność rozprawy dla nauk technicznych?

Recenzent wysoko ocenia przydatność ocenianej rozprawy doktorskiej dla nauk technicznych. Rozprawa dotyczy aktualnego i ważnego problemu z zakresu telekomunikacji i bezpieczeństwa: jak zapewnić wysoki poziom bezpieczeństwa połączeń pomiędzy sieciami komórkowymi różnych operatorów. Autor zaproponował uniwersalne podejście (z punktu widzenia połączeń sieci komórkowych różnych generacji) bazujące na dynamicznym szacowaniu ryzyka związanego z ruchem międzyoperatorskim – zarówno związanym z pojedynczymi wiadomościami sygnalizacyjnymi jak i strumieniami danych. Co istotne – ryzyko w takim podejściu jest szacowane w sposób ilościowy, co pozwala np. na ustalanie akceptowanych progów ryzyka czy szacowaniu poziomu zaufania do jednostek. Dodatkowo – propozycja ściśle zdefiniowanych i uszeregowanych profili bezpieczeństwa może poprawić efektywność ustalania parametrów bezpieczeństwa danego łącza, a stała kontrola bezpieczeństwa w łączu międzyoperatorskim może być wykorzystana do dynamicznego tworzenia i egzekwowania adekwatnej polityki bezpieczeństwa. Oba te podejścia są przedmiotem prac standaryzacyjnych i patentów przyznanych w ciągu ostatnich kilku miesięcy, co dodatkowo potwierdza użyteczność wyników rozprawy dla nauk technicznych.

8. Konkluzja – do której z następujących kategorii Recenzent zalicza rozprawę:

a) niespełniająca wymagań stawianych rozprawom przez obowiązujące przepisy
b) wymagająca wprowadzenia poprawek i ponownego recenzowania
c) <u>spełniająca wymagania</u>
d) spełniająca wymagania z wyraźnym nadmiarem
e) wybitnie dobra, zasługująca na wyróżnienie

9. Uzasadnienie

Biorąc po uwagę wszystkie wspomniane aspekty rozprawy doktorskiej, moja końcowa konkluzja jest jednoznacznie pozytywna. Autor zaprezentował w rozprawie ogólną wiedzę teoretyczną w dyscyplinie i przedstawił oryginalne rozwiązanie problemu naukowego. Zaproponował nowy model/strukturę bezpieczeństwa, dzięki której możliwe jest oszacowanie ryzyka związanego z ruchem w łączach międzyoperatorskich, a następnie określenie poziomu zaufania do poszczególnych jednostek w sieci, wybór adekwatnego profilu bezpieczeństwa w celu ułatwienia negocjacji parametrów bezpieczeństwa czy dynamiczne ustalanie i egzekwowanie odpowiednich polityk bezpieczeństwa. Tym samym Autor rozprawy potwierdził umiejętność samodzielnego prowadzenia pracy naukowej.

Podsumowując stwierdzam, że rozprawa doktorska spełnia wymagania *Ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce* oraz wnioskuję o dopuszczenie Pana mgr. inż. Germana Peinado Gomeza do dalszych etapów przewodu doktorskiego.