

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

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 zmagają 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. Ujednoczone 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 czasopiśmie 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 reguły 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 połączanego 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

profilu bezpieczeństwa w umowach o gwarantowanym poziomie świadczenia usług oraz wymuszania w ramach 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 tekstu 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.

