Zachodniopomorski
Uniwersytet Technologiczny
w Szczecinie

Wydział Informatyki

Szczecin, dn. 7 września 2023 r.

dr hab. inż. Jerzy Pejaś, prof. ZUT

Katedra Inżynierii Oprogramowania i Cyberbezpieczeństwa
Wydział Informatyki
Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

RECENZJA

rozprawy doktorskiej mgra inż. Patryka Kozieła pt. "PACE and PACE CAM: Security Issues and Protocol Extensions"

Niniejsza recenzja została wykonana w odpowiedzi na pismo Przewodniczącego Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Politechniki Wrocławskiej prof. dr hab. inż. Michała Woźniaka, realizującego uchwałę Rady z dnia 28 czerwca 2023 roku w sprawie powołania recenzentów w przewodzie doktorskim mgra inż. Patryka Kozieła.

1. Problematyka naukowa oraz przedmiot rozprawy

Przedmiotem rozprawy są protokoły kryptograficzne powiązane z elektronicznymi dokumentami tożsamości (w skrócie: dokument eID), będącymi istotnym elementem systemów elektronicznej identyfikacji i pozwalającymi na uniwersalną, jednoznaczną oraz niezawodną identyfikację i uwierzytelnianie obywateli. Obecnie wiele krajów wydaje swoim obywatelom elektroniczne dokumenty tożsamości (dowody osobiste lub paszporty), wykorzystywane w wielu nowych usługach typu e-administracja i e-handel, w tym także podczas kontroli granicznych.

Istotnym elementem dokumentów eID są protokoły kryptograficzne zapewniające bezpieczną komunikację pomiędzy dokumentem (dokładniej zaawansowanym układem scalonym z kryptoprocesorem wbudowanym w dokument eID), a terminalem. Efektem końcowym pomyślnie zakończonego protokołu powinna być jednoznaczna identyfikacja tożsamości posiadacza dokumentu, a także jedno- lub dwustronne uwierzytelnienie dokumentu i terminala.

W recenzowanej pracy doktorant zajął się protokołami uwierzytelniania zawartymi w standardzie przyjętym przez International Civil Aviation Organization (ICAO), rekomendowanymi w rozporządzeniach Unii Europejskiej do implementowania w warstwie elektronicznej oficjalnych dokumentów tożsamości. Autor założył, że głównym celem rozprawy jest zbadanie bezpieczeństwa dwóch podstawowych protokołów kryptograficznych przyjętych w standardzie ICAO: protokołu PACE (Password Authenticated Connection

Establishment) oraz protokołu PACE CAM (PACE with Chip Authentication Mapping).

Oba protokoły pozwalają na uzgodnienie pomiędzy układem scalonym z kryptoprocesrem dokumentu eID a terminalem (czytnikiem) sekretnych kluczy, wykorzystywanych później przez obie strony do poufnego i uwierzytelnionego przesyłania danych, np. danych biometrycznych podczas kontroli granicznej.

Problem bezpieczeństwa protokołów PACE i PACE CAM jest bardzo istotny z punktu widzenia ich praktycznego wykorzystywania w wielu systemach uwierzytelniania i identyfikacji tożsamości użytkowników eID. W literaturze przedmiotu temu problemowi poświęcono w zasadzie dwie podstawowe prace (Jens Bender, Marc Fischlin i Dennis Kügler [4] oraz Miroslaw Kutyłowski i Przemysław Kubiak [5] wg spisu literatury), odnoszące się bezpośrednio do analizy bezpieczeństwa protokołu PACE, znanego także pod nazwą PACE-GM (PACE General Mapping). Inne protokoły z rodziny PACE (np. PACE CAM) są rozszerzeniami protokołu PACE i ich bezpieczeństwo wyprowadzane jest z bezpieczeństwa protokołu PACE.

W przeciwieństwie do tradycyjnego udowadnialnego bezpieczeństwa zastosowanego w dowodzie przedstawionym w [4], w pracy [5] dowód bezpieczeństwa oparto na podejściu zorientowanym na praktykę (tzw. bezpieczeństwo konkretne), które pozwala na uzyskanie bardziej precyzyjnych oszacowań złożoności obliczeniowej zadań przeciwnika niż tradycyjne oszacowanie asymptotycznej równoważności trudnych problemów obliczeniowych.

Sformułowany cel rozprawy, którym jest przedstawienie pełnych wersji dowodów bezpieczeństwa własności protokołu PACE naszkicowanych w pracy [5] i przeniesienie uzyskanych wyników na protokół PACE CAM oraz inne rozszerzone protokoły PACE przedstawione w rozprawie jest ambitny. Biorąc to pod uwagę uważam, że obszar badawczy będący przedmiotem rozprawy mieści się w dyscyplinie informatyka techniczna i telekomunikacja jest bardzo aktualny i ma duże znaczenie praktyczne.

2. Struktura i zawartość pracy

Recenzowana rozprawa doktorska została przygotowana w języku angielskim i składa się z czterech rozdziałów, streszczenia (w języku angielskim i polskim), podsumowania pracy oraz bibliografii obejmującej 22 pozycje literaturowe. Całość pracy obejmuje 69 stron i ma charakter teoretyczny. Wyniki własne doktoranta przedstawione są w rozdziałach 3 i 4.

Struktura pracy jest przejrzysta, poszczególne rozdziały zwierają te treści, które są niezbędne do rozumienia idei prezentowanych w kolejnych rozdziałach:

- w rozdziale pierwszym wprowadzone zostało pojęcie elektronicznego dokumentu tożsamości (eID), przedstawiono główne problemy, kontekst prawny i zastosowania eID w ramach Unii Europejskiej oraz podano krótkie informacje o dwóch najważniejszych protokołach PACE i PACE CAM; doktorant opisał także swoje najważniejsze osiągnięcia dotyczące analizy bezpieczeństwa protokołów PACE i PACE CAM opartej na sformułowanych wymaganiach bezpieczeństwa oraz przedstawił rozszerzenia PACE with Mutual Authentication (PACE MA) i PACE with Proof of Presence (PACE PoP); wspomniane rozszerzenia zostały przedstawione w roku 2021 podczas konferencji ESORICS'21 i IFIP Networking;
- rozdział drugi zawiera podstawowe informacje i definicje z zakresu kryptografii, w tym m.in. definicję grupy cyklicznej, definicje trudnych problemów obliczeniowych, na których opierają się dowody bezpieczeństwa omawianych (w tym zaproponowanych)

w pracy protokołów kryptograficznych oraz definicje kryptograficznych elementów pierwotnych takich jak podpis cyfrowy Schnorra, schemat identyfikacji Schnorra, schemat szyfrowy, funkcja skrótu oraz kody uwierzytelniania wiadomości AES-MAC; w rozdziale tym Autor przedstawił także pojęcie adwersarza oraz pojęcie pomijalnej i praktycznie pomijalnej przewagi (ang. negligible and practically negligible advantage) w kontekście tzw. bezpieczeństwa konkretnego;

- w rozdziale trzecim przedstawiono opisy protokołów PACE i PACE CAM oraz przeprowadzono analizę ich bezpieczeństwa; na potrzeby analizy sformułowano dziewięć autorskich twierdzeń i udowodniono je; pokazano w ten sposób, że w przypadku protokołu PACE CAM adwersarz nie może aktywnie ingerować w przebieg sesji protokołu (z małym wyjątkiem nie dotyczy to protokołu PACE), nie może także naruszyć poufności zestawionego kanału kryptograficznego; przy założeniu, że adwersarz nie zna hasła użytkownika dokumentu eID, rozważane są także problemy odporności protokołów na przełamanie hasła, przejęcie sesji oraz śledzenie; przeanalizowano także protokół PACE CAM z punktu widzenia wiarygodnego uwierzytelnienia układu scalonego wbudowanego w dokument tożsamości; w mojej ocenie jest to najważniejszy rozdział rozprawy;
- rozdział piąty zawiera dwie autorskie propozycje rozszerzenia protokołu PACE: protokół PACE (PACE Mutual Authentication) oraz protokół PACE Proof of Presence (PACE PoP); pierwszy z protokołów pozwala na wzajemne uwierzytelnianie pomiędzy układem scalonym z kryptoprocesorem wbudowanym w dokument eID, a terminalem (czytnikiem), z kolei w wyniku pomyślnego zakończenia drugiego protokołu dostarczany jest niezaprzeczalny dowód, że określony dokument eID uczestniczył w tej sesji; dowody bezpieczeństwa obu protokołów bazują na wynikach analizy protokołów PACE i PACE CAM i sprowadzają się do pokazania, że trudność ataków na protokoły PACE MU lub PACE PoP można zredukować do trudności ataków na protokół PACE lub PACE CAM; ciekawym elementem tego rozdziału jest także krótki zestaw zasad projektowania rozszerzeń, który obejmuje zasadę wstecznej kompatybilności, zasadę minimalnych zmian, zasadę reużywalności kodu i operacji kryptograficznych oraz zasadę zachowania własności bezpieczeństwa posiadanych przez rozszerzaną wersje protokołu;
- zakończeniem pracy jest bardzo krótkie podsumowanie uzyskanych wyników; Doktorant podkreśla, że ważnym kierunkiem dalszych prac powinno być projektowanie nowych rozszerzeń protokołu PACE; wynika to nie tylko z indywidualnych zainteresowań badaczy, ale także z praktycznych potrzeb użytkowników oraz zmieniających się wymagań prawnych.

Rozprawa jest poprawnie zredagowana. Jej stosunkowo nieduży rozmiar jest (prawdopodobnie) wynikiem świadomej decyzji doktoranta pomijania w pracy informacji, które są zbędne z punktu widzenia osiąganych celów. Najobszerniejszym rozdziałem w pracy jest rozdział trzeci. Oczywiście, jego wartość jest znacząca i zawiera największe osiągnięcia doktoranta, które wymagają często obszernych i zaawansowanych rozważań teoretycznych.

3. Najistotniejsze osiągnięcia przedstawione w rozprawie

Rozprawa doktorska mgra inż. Patryka Kozieła zawiera oryginalne wyniki dotyczące analizy bezpieczeństwa protokołów PACE i PACE CAM oraz propozycje nowych protokołów będących

rozszerzeniami protokołów PACE i PACE CAM. Oryginalną wartość analizowanych oraz proponowanych protokołów podnoszą dodatkowo starannie sformułowane i udowodnione twierdzenia dotyczące ich bezpieczeństwa.

Do najważniejszych oryginalnych badań teoretycznych przedstawionych w rozprawie należy zaliczyć:

- Dowody bezpieczeństwa dwóch podstawowych protokołów uwierzytelniania PACE i PACE CAM (Twierdzenie 3.2).

  Dowody są twórczym rozwinięciem podejścia przyjętego w pracy Mirosława Kutyłowskiego i Przemysława Kubiaka [5] oraz przedstawionych tam szkiców dowodów bezpieczeństwa protokołu PACE. Dotyczy to w szczególności pokazania, że wszystkie możliwości aktywnego adwersarza można zredukować do możliwości adwersarza pasywnego. Oryginalnym osiągnięciem doktoranta jest przedstawienie pełnego dowodu bezpieczeństwa obu protokołów, przy czym przyjęta strategia dowodu polegała na udowodnieniu najpierw bezpieczeństwa protokołu PACE, a następnie na wnioskowaniu na tej podstawie o bezpieczeństwie protokołu PACE CAM. Strategia ta została wykorzystana także w dowodach bezpieczeństwa rozszerzeń protokołów zaproponowanych w rozdz. 4.

- Dowody poufności sesji (kanałów kryptograficznych) zestawionych w wyniku pomyślnego zakończenia protokołów uwierzytelniania PACE lub PACE CAM (twierdzenie 3.3).

- Analiza relatywnie silnej ochrony przed atakami na hasła używanymi w protokołach PACE i PACE CAM podczas ustanawiania sesji pomiędzy układem scalonym eID, a terminalem z wykorzystaniem protokołu PACE i PACE CAM (Twierdzenia 3.5, 3.10, 3.11, 3.12, 3.14).

  Rozważane są trzy rodzaje ataków na hasła: łamanie haseł, przejęcie sesji, śledzenie (użytkownika, dowód obecności). Dowody bezpieczeństwa są bardzo obszerne (obszerniejsze niż dowody bezpieczeństwa protokołów PACE i PACE CAM oraz poufności kuczy sesyjnych razem wziętych). Z dowodów wynika, że mimo relatywnie silnej ochrony haseł protokół PACE gwarantuje jedynie słabe uwierzytelnienie dokumentu eID z układem scalonym.

- Dowód silnego uwierzytelnienia dokumentu eID z układem scalonym w przypadku zastosowania protokołu PACE CAM (Twierdzenie 3.15 i 3.16).

  Jest to ważna cecha protokołu PACE CAM (tzw. aktywne uwierzytelnienie), która pozwala na zapewnienie zarówno uwierzytelnienie danych w dokumencie eID, jak również uwierzytelnienie układu scalonego

- Opracowanie protokołu uwierzytelniania PACE Mutual Authentication (PACE MA) i jego „lekkiej" wersji PACE MA-light oraz protokołu PACE Proof of Presence, (PACE PoP).

  Wszystkie wymienione protokoły są rozszerzeniami protokołu PACE lub PACE CAM. Protokoły PACE MA i PACE MA-light są rozszerzeniami protokołu PACE CAM i umożliwiają wzajemne uwierzytelnienie eID oraz terminala. Z kolei protokół PACE PoP dostarcza posiadaczowi dokumentu eID poświadczenie o pomyślnym zestawieniu sesji z autentycznym terminalem. Dowody bezpieczeństwa zaproponowanych są krótkie (stwierdzenia 4.0.1, 4.0.2 i 4.0.3) i odwołują się najczęściej do własności bezpieczeństwa protokołów PACE CAM i PACE.

Dowody nie bazują na standardowych modelach bezpieczeństwa, ale na praktycznym podejściu do analizy bezpieczeństwa, tj. zamiast analizować wszystkie możliwe zagrożenia i odpowiadające im scenariusze ataków należy w pierwszej kolejności pokazać, że każdy aktywny udział adwersarza w protokole kończy się niepowodzeniem. Oznacza to, że w tym przypadku wystarczy pokazać, że protokół nie pozwala na ujawnienie żadnych wrażliwych danych, bo oznaczałoby to rozwiązanie trudnego problemu obliczeniowego, który leży u podstaw projektu protokołu. Doktorant pokazał, że protokoły PACE CAM i PACE (z jednym wyjątkiem) są wrażliwe (ang. fragile) na manipulacje adwersarza i tym samym pozwalają na poprawne zestawie sesji pomiędzy eID, a terminalem.

Należy podkreślić, że prawdziwość każdego ze formułowanych twierdzeń została poprawnie udowodniona w przyjętym przez doktoranta modelu bezpieczeństwa; do szczególnie ciekawych należą dowody twierdzeń 3.2 i 3.3.

Dorobek dodktoranta publikacyjny obejmuje 8 publikacji (baza Google Scholar i Scopus), z których 4 zostały opublikowane w czasopismach indeksowanych na liście JCR (*Extremes*, *Computer Networks*, *Information Sciences* i *Computers & Security*), zaś pozostałe materiałach bardzo dobrych konferencjach tematycznych (m.in. na konferencjach *Computer Security - ESORICS 2021*, *IFIP Networking Conference and Workshops 2021*). W spisie literatury wskazane zostały tylko dwie publikacje bezpośrednio związane z tematyką rozprawy. Publikacje powstały w latach 2018-2023 i są potwierdzeniem dobrej aktywności publikacyjnej doktoranta oraz rozsądnego lokowania publikacji w czasopismach i konferencjach, które powiązane są z obszarem jego zainteresowań.

W trzech publikacjach, w tym w jednej bezpośrednio powiązaną z rozprawą doktorant jest pierwszym autorem. Najważniejsze wyniki rozprawy zostały przedstawione w rozdziałach 3 i 4. Zostały one zaczerpnięte z opublikowanych prac [15, 16] lub zgłoszonych do publikacji przez doktoranta (informacja ze str. 15). O ile wkład doktoranta w artykule zgłoszonym do publikacji jest oczywisty, o tyle w przypadku publikacji [15, 16] wkład ten jest trudny do określenia.

4. Uwagi krytyczne

Analiza struktury i zawartości rozprawy wskazuje na jej następujące trzy zalety: precyzyjne merytoryczne zakreślenie obszaru badań, solidną podstawę metodyczną oraz dużą umiejętność doktoranta rozszerzania protokołów kryptograficznych (przy zachowaniu zdefiniowanych w rozdz. 4 zasad rozszerzania protokołów klasy PACE), a następnie w formalnym dowodzeniu ich bezpieczeństwa. Autor bardzo dobrze porusza się w obszarze badań dotyczących protokołów kryptograficznych, a zwłaszcza stosowanych podejść do dowodzenia ich bezpieczeństwa.

Pomimo wymienionych powyżej niewątpliwych zalet pracy, podczas czytania rozprawy nasuwają się pewne uwagi o charakterze merytorycznym i formalnym.

Uwagi merytoryczne

(a) Praktyczne podejście do oceny bezpieczeństwa wymaga dobrego zidentyfikowania potencjalnych możliwych zagrożeń oraz możliwości adwersarza. W rozprawie zagrożenia oraz możliwości adwersarza określane są zwykle w momencie dowodzenia twierdzeń. Utrudnia to analizę poszczególnych części dowodu i często zmusza do

szukania uzasadnienia celu rozważania przez doktoranta kolejnego scenariusza ataku. Z protokołami PACE (szerzej, z dokumentami MRAD organizacji ICAO) związane są dwa profile ochrony (ang. protection profiles, PPs):

- Common Criteria Protection Profile Version 1.10, 25th March 2009 *Machine Readable Travel Document with „ICAO Application", Basic Access Control*;
- Common Criteria Protection Profile 1.3.0, January 2012 *Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE*.

W dokumentach tych zdefiniowano praktyczne wymagania bezpieczeństwa nakładane na eID dokument. Ich zebranie i przedstawienie w rozprawie pozwoliłoby na pokazanie możliwych scenariuszy ataków na dokument eID i zdefiniowanie kolejnych celów analizy bezpieczeństwa.

(b) rozprawa ma charakter teoretyczny, ale dotyczy bardzo praktycznego i technicznego problemu bezpieczeństwa kontroli tożsamości, np. osób przekraczających granice. Protokół PACE jest istotnym elementem infrastruktury *„automatyzacji procesu kontroli granicznej z użyciem paszportów biometrycznych"*.

Brak w rozprawie opisu ogólnej architektury systemu elektronicznej identyfikacji nie pozwala na precyzyjne określenie stanu systemu, w którym rozpoczyna się wykonywanie protokołu PACE i stwierdzenie, że stan ten jest bezpieczny. Na przykład, z opisu na str. 6 rozprawy wynika, że hasło do terminala wprowadza posiadacz eID (*"As the chip holder explicitly enters the password in the terminal, chip authentication is very weak"*). W systemach kontroli granicznych hasło nie jest wprowadzane, a generowane przez terminal w oparciu o skanowane parametry paszportu (obszary MRZ oraz CAN) – pisze o tym także doktorant na str. 4 i str. 16. Jak w powyższym kontekście uzasadnione jest założenie, że *"A*(dversary) *does not know the password used by the other party or parties"* (str. 31). Czy obligatoryjnie jest to jeden z przyjętych stanów bezpiecznych? Jakie uprawnienia dostępu do układu scalonego z kryptoprocesorem ma terminal?

(c) Doktorant przypisuje adwersarzowi kolejne cele i dowodzi, że przy założonych parametrach, np. dostępnym czasie lub ograniczonej liczbie operacji adwersarz ma pomijalnie małe szanse na osiągnięcie celu. W każdym takim kroku w zależności od celu brane są pod uwagę możliwości adwersarza. Potencjalnie zdefiniowane możliwości adwersarza mogą być błędne lub przeoczone. Czy doktorant analizował takie przypadki i jakie może to mieć wpływ na zaufanie do przeprowadzonych analiz bezpieczeństwa?

(d) Oryginalne wyniki Autora zostały przedstawione w rozdziałach 3 i 4. Zostały one powiązane z pracami opublikowanymi lub zgłoszonymi do publikacji (deklaracja doktoranta na str. 15). Brakuje określenia osobistego wkładu doktoranta w każdą z przywoływanych publikacji oraz w przygotowywanym artykule.

(e) W rozprawie doktorant często odwołuje się do publikacji „ICAO. Machine Readable Travel Documents - Part 11: Security Mechanism for MRTDs. Doc 9303" roku 2015. W roku 2021 ukazało się zaktualizowane ósme wydanie tego dokumentu. W dokumencie tym zdefiniowano m.in. nowe rekomendacje dotyczące algorytmów kryptograficznych: nie rekomenduje się dalszego używania np. funkcji skrótu RIPEMD-160 i SHA-1. Czy doktorant analizował wprowadzone zmiany i czy mogą one mieć wpływ na analizy przedstawione w rozprawie?

Uwagi formalne

(a) Pojęcie symulowalności protokołu (Defincja 3.3) powinno być wprowadzone wcześniej, np. przed rozdz. 3.3, a najlepiej przed pierwszym użyciem słowa „simulate". Byłoby to okazja do skonfrontowania obu tych pojęć w kontekście redukcji bezpieczeństwa (ang. security reduction) protokołu do trudnego problemu obliczeniowego, np. w oparciu o symulację protokołu przedstawioną na str. 23.

(b) W pracy brakuje zestawienia używanych w rozprawie skrótów, np. PACE-CAM.

(c) Str. 21, 35 i 40: brak jednolitej numeracji twierdzeń; twierdzenie nr 3.2 na tej stronie sugeruje, że gdzieś w pracy sformułowano twierdzenie 3.1, podobnie nie ma twierdzeń o numerach 3.4, 3.6, 3.7, 3.8, 3.9;

(d) Niejasne są przyjęte zasady numerowania wniosków (ang. corollaries), stwierdzeń (ang. claims), lematów oraz uwag (ang. notes); w przypadku twierdzeń, definicji i założeń numer składa się z dwóch liczb rozdzielonych kropką: pierwsza liczba oznacza numer głównego rozdziału, zaś druga liczba jest numerem kolejnego twierdzenia w rozdziale. Zasada ta nie jest przestrzegana w pozostałych przypadkach.

(e) Dodanie w spisie literatury numeru DOI ułatwiłoby wyszukiwanie artykułów w dostępnych sieciowych bazach publikacji.

Wskazane powyżej usterki merytoryczne oraz formalne nie wpływają w żaden sposób na końcową ocenę rozprawy jako całości. Uwagi merytoryczne mają charakter dyskusyjny lub uzupełniający. Mam nadzieję, że zostaną wzięte pod uwagę przez doktoranta w przyszłych publikacjach powiązanych z wynikami przedstawionymi w rozprawie. Praca jest napisana starannie, jej poziom nie budzi moich wątpliwości. Stąd nie znalazłem w prac zbyt dużo usterek, a te które wskazałem mają charakter pomyłek edycyjnych oraz sugestii tego, czego brakuje w pracy.

6. Konkluzja recenzji

Recenzowana rozprawa zawiera jasno sformułowane cele rozprawy (pełny dowód bezpieczeństwa protokołów PACE i PACE CAM oraz projekty dwóch rozszerzeń protokołu PACE wraz dowodami ich bezpieczeństwa). Prace badawcze z zakresu analizy bezpieczeństwa protokołów kryptograficznych zostały przeprowadzone poprawnie z wykorzystaniem nowoczesnych metod kryptograficznych, w tym technik redukcji bezpieczeństwa.

Przedstawione powyżej uwagi merytoryczne i formalne nie umniejszają osiągnięć doktoranta, ani nie podważają zaproponowanych protokołów oraz dowodów ich bezpieczeństwa. Przedstawioną do oceny rozprawę oceniam bardzo wysoko, zarówno z uwagi na aktualność i ważność tematyki rozprawy, staranność jej przygotowania, zastosowany warsztat metodyczny, jak również wiedzę doktoranta i znajomość literatury z zakresu metod projektowania i dowodzenia bezpieczeństwa protokołów kryptograficznych. Doktorant uzyskał wartościowe i oryginalne wyniki rozwiązania problemu naukowego, które przedstawił w rozprawie w postaci dowodu bezpieczeństwa protokołu PACE i PACE PCM, nowych projektów protokołów PACE MA, PACE MA-light i PACE PoP oraz dowodów ich bezpieczeństwa. Uzyskane wyniki były opublikowane przez doktoranta w materiałach dwóch renomowanych konferencji międzynarodowych oraz są przedmiotem publikacji, która w momencie złożenia pracy była w recenzji.

Biorąc pod uwagę powyższe wyniki naukowe uważam, że doktorant zrealizował cel rozprawy oraz wykazał się umiejętnościami i odpowiednim przygotowaniem do samodzielnej pracy

naukowej w dyscyplinie informatyka techniczna i telekomunikacja. Na tej podstawie stwierdzam, że przedstawiona do oceny rozprawa doktorska mgra inż. Patryka Kozieła pt. *„PACE and PACE CAM: Security Issues and Protocol Extensions”* **spełnia wymagania stawiane rozprawom doktorskim w Ustawie *Prawo o szkolnictwie wyższym i nauce*** (Dz. U. 2023, poz. 742 z późniejszymi zmianami) **i wnoszę o dopuszczenie jej Autora do dalszych etapów postępowania doktorskiego prowadzonego w dziedzinie nauk inżynieryjno-technicznych w dyscyplinie Informatyka techniczna i telekomunikacja.**