UNIVERSITÄT ZU LÜBECK
INSTITUTE FOR
THEORETICAL COMPUTER SCIENCE

Universität zu Lübeck · Institut für Theoretische Informatik
Ratzeburger Allee 160 · 23538 Lübeck

Prof. dr hab. Maciej Liśkiewicz

Ratzeburger Allee 160
23538 Lübeck

Tel. +49 451 3101 5312
Fax +49 451 3101 5304

maciej.liskiewicz@uni-luebeck.de

Lubeka, 19.10.2023

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

W przedstawionej rozprawie doktorskiej, Patryk Kozieł zajmuje się analizą bezpieczeństwa wybranych dwustronnych protokołów kryptograficznych, których celem jest ustalenie wspólnego klucza symetrycznego. Przedmiotem badań jest protokół PACE (*Password Authenticated Connection Establishment*), jego zmodyfikowana wersja PACE CAM (*PACE with Chip Authentication Mapping*), a także dalsze rozszerzenia wersji podstawowej. Protokół PACE został opracowany przez niemiecki Federalny Urząd Bezpieczeństwa Informacji (BSI) w celu uwierzytelniania i uzgadniania kluczy w oparciu o hasło i jest stosowany w dowodach osobistych z wbudowaną warstwą elektroniczną oraz w dokumentach podróżnych nadających się do odczytu maszynowego. Przedłożona praca doktorska dotyczy zatem tematyki mającej znaczenie praktyczne a jej wyniki mogą spotkać się z zainteresowaniem projektantów systemów zabezpieczeń informacji.

Celem badań omawianych w pracy doktorskiej była teoretyczna analiza protokołów rodziny PACE, które bazują na pomyśle podwójnej wymianie kluczy w oparciu o podejście Diffiego-Hellmana. Bezpieczeństwo tych protokołów jest kluczowym atrybutem mechanizmu zabezpieczającego integralność i autentyczność dokumentów personalnych. Próby takich analiz podejmowane były wcześniej w pracach Bender/Fischlin/Kügler [Information Security, 2009] oraz Kutyłowski/Kubiak [TrustCom, 2019], których wyniki stanowią punkt wyjściowy badań mgra inż. Kozieła.

Jednym z głównych osiągnięć rozprawy jest pełna i poprawiona wersja dowodów bezpieczeństwa dla protokołów PACE i PACE CAM przedstawionych w artykule Kutyłowski/Kubiak [TrustCom, 2019]. Analiza podana w Rozdziale 3, który stanowi zasadniczą część rozprawy, opierając się na pomyśle redukcji aktywnych przeciwników do wersji pasywnej, uzupełnia luki dowodowe w pracy Kutyłowskiego i Kubiaka. Podobnie jak w poprzednich pracach, podana analiza dotyczy bezpieczeństwa protokołów w podejściu, w którym pomija się szczegóły implementacyjne, w tym techniczne założenia dotyczące hardware'u.

Kolejnym osiągnięciem przedłożonej rozprawy jest opracowanie nowych modyfikacji protokołu bazowego: PACE MA (Mutual Authentication), jego wariantu PACE MA-light, oraz PACE PoP (Proof of Presence). Są one przedstawione i analizowane w Rozdziale 4. Motywacją dla konstrukcji tych protokołów są własności, których znane do tej pory metody rodziny PACE nie posiadają. W szczególności chodzi tu, odpowiednio, o uwierzytelnianie urządzenia terminalnego oraz o kryptograficzne potwierdzenie poprawnie przeprowadzonej sesji pomiędzy chipem a urządzeniem terminalnym. Zaproponowane modyfikacje w sposób atrakcyjny wzbogacają funkcjonalność poprzednich podejść. Analiza nowych protokołów opiera się na własnościach wersji podstawowych, których dowody przedstawiono w Rozdziale 3.

Dowodzenie odporności protokołów kryptograficznych na różnego typu ataki adwersarzy jest generalnie zadaniem trudnym i wymagającym biegłości w posługiwaniu się metodami opartymi na rachunku prawdopodobieństwa, teorii liczb i kombinatoryce. W szczególności, podjęte w rozprawie zadanie udowodnienia, że omawiana rodzina protokołów jest odporna na specyficzne ataki i spełnia inne wymagane własności, nie jest zadaniem rutynowym i wymaga pewnej pomysłowości i sprytu. Ciekawym podejściem przedstawionym w rozprawie jest zredukowanie ataków aktywnych do pasywnego adwersarza i pokazanie, że jeśli adwersarz jest pasywny, wówczas dane zapisane na chipie pozostają ukryte, przyjmując rozsądne założenia kryptograficzne Diffiego-Hellmana.

W tym celu zdefiniowano własność *fragility*, która polega na tym, że w przypadku jakiejkolwiek manipulacji komunikacji pomiędzy chipem i terminalem, prawdopodobieństwo pomyślnego zakończenia sesji jest prawie nieistotne (*negligible*). Kluczowy wynik (Twierdzenie 3.2) mówi, że PACE i PACE CAM spełniają tę własność w modelu *Random Oracle*, z wyjątkiem pewnych oczywistych manipulacji w pierwszej fazie DH w przypadku wersji podstawowej. Dowód tej własności opiera się na redukcjach do problemów Diffiego-Hellmana oraz do problemu zdefiniowanego w przyjętym założeniu KEA1 (*Knowledge of Exponent Assumption*). Przedstawione analizy są technicznie złożone i wymagają systematycznego rozpatrywania szeregu pod-przypadków. Część z pokazanych oszacowań na prawdopodobieństwa powodzenie przeprowadzonych ataków, wyrażona jest numerycznie, opierając się na wartościach parametrów rekomendowanych w specyfikacji ICAO.

Korzystając z udowodnionych powyższej wyników, w rozprawie pokazano własności protokołów rodziny PACE, które są istotne z punktu widzenia użytkownika. W szczególności dowodzi się, że protokoły zachowują poufność generowanego klucza (*key confidentiality*) oraz bezpieczeństwo hasła (*password security*) w różnego rodzaju scenariuszach. Użyte podejście jest ciekawe i wartościowe ponieważ znacznie upraszcza dowodzenie własności omawianych protokołów kryptograficznych. Także analiza nowych konstrukcji PACE MA i PACE PoP opiera się na wynikach pokazanych w Rozdziale 3. Podobnie jak w przypadku protokołów bazowych, pokazuje się, że nowe metody spełniają własność *fragility*, co znacznie upraszcza dowody bezpieczeństwa i prywatności nowych metod.

Powyższe wyniki stanowią interesujący wkład mgra inż. Kozieła w zakresie analizy bezpieczeństwa protokołów dwustronnych. Niestety, przedłożona rozprawa zawiera jednocześnie szereg niedociągnięć. W szczególności, protokoły PACE oraz PACE CAM, w wersji przyjętej w pracy (Fig. 3.1, odpowiednio Fig. 3.2), nie spełniają własności podanej w Twierdzeniu 3.2. Łatwo jest bowiem pokazać, że protokoły nie są *fragile*: adwersarz $\mathcal{A}$ może zmanipulować wiadomości Y_A, Y_B, T_A, oraz T_B w ten sposób, że $Y'_A := 1$, $Y'_B := 1$ oraz $T'_A := \mathrm{MAC}(H(1||3), (Y_B, \mathcal{G}))$, $T'_B := \mathrm{MAC}(H(1||3), (Y_A, \mathcal{G}))$. Obie strony akceptują T'_A, odpowiednio T'_B i obliczają wynik końcowy: $K_{Enc} = H(1||1)$, $K_{MAC} = H(1||2)$, co przeczy Twierdzeniu 3.2. Co więcej, powyższy scenariusz pokazuje, że omawiane protokoły nie są bezpieczne. Opisany atak daje sę łatwo wkluczyć, jeśli strony zweryfikują dodatkowo, że otrzymane $Y_A \neq 1$ oraz $Y_B \neq 1$. Przyjmuję zatem, że autor zakłada *niejawnie*, że chip (A) i terminal (B) weryfikują otrzymane wartości w ten sposób. Ciekawe byłoby wskazać miejsce w dowodzie Twierdzenia 3.2, w którym wykorzystuje się te założenia.

Ponadto, w opisie protokołu PACE podanym na str. 14, inaczej niż w wersji opisanej w Fig. 3.1, pomija się istotne założenia, że losowo wybrane wykładniki są różne od zera a w definicji dotyczącej *Assumption* 3.8 (*Extended KEA1*) brakuje założeń odnośnie ζ oraz y. Także interakcja pomiędzy challengerem $\mathcal{C}$ a adwersarzem $\mathcal{A}$ wykorzystywana w tym założeniu, wymaga bliższych szczegółów.

Kluczowa analiza bezpieczeństwa przedstawiona w Rozdziale 3 jest pełną i poprawioną wersją dowodów podanych w pracy Kutyłowskiego i Kubiaka z roku 2019. Autor rozprawy doktorskiej nie określa jednak bliżej własnego wkładu w otrzymaniu pełnego dowodu. W szczególności nie podaje które luki w dowodach bezpieczeństwa udało mu się uzupełnić oraz jakie własne pomysły umożliwiły uzyskanie przedstawionych rezultatów.

W rozprawie cytowane są dwie prace własne Autora (obie współautorskie): (1) *PACE with Mutual Authentication – Towards an Upgraded eID in Europe*, która opublikowana została w materiałach cenionej konferencji *European Symposium on Research in Computer Security (ESORICS)*, ocenianej kategorią **A** według *Computing Research and Education (CORE) Conference Rankings* i 140 pkt. MEiN oraz (2) *Poster: eID in Europe – Password Authentication Revisited*, która jest krótkim artykułem opublikowanym w materiałach mniej kompetytywnej konferencji *IFIP International Conference on Networking, (IFIP Networking)*, kategoria **B** według CORE i 140 pkt. MEiN. Prace te, są jednocześnie zawartością rozdziału czwartego, który prezentuje pełne i nieco zmodyfikowane dowody w oparciu o wyniki rozdziału trzeciego. W swoim dorobku, Doktorant posiada ponadto szereg innych prac (wszystkie współautorskie), w tym opublikowane w: *Information Sciences* (2020) IF 8.1, *Computer Networks* (2020) IF 5.6, *Computers & Security* (2019) IF 5.6, *Extremes* (2023) IF 1.3 oraz w materiałach konferencji *IEEE International Symposium on Network Computing and Applications (NCA, 2019)* CORE rank B i w materiałach lokalnej konferencji *International Joint Conference on e-Business and Telecommunications (ICETE, 2019)*. Tematyka tych artykułów dotyczy zabezpieczeń w bezprzewodowej komunikacji radiowej i systemach komputerowych, oraz problemów optymalizacji stochastycznej.

Przedłożona rozprawa oraz pozostałe opublikowane prace wymienione wcześniej, prezentują w sposób wystarczający ogólną wiedzę teoretyczną Doktoranta w zakresie bezpieczeństwa technik informatycznych i Jego dobre przygotowanie do pracy badawczej w tym temacie. Uważam, że wyniki przedstawione w rozprawie i pozostałych pracach, potwierdzają Jego kwalifikacje do prowadzenia rzetelnych badań naukowych w dziedzinie informatyki, a także są dowodem wykształcenia specjalistycznego połączonego z umiejętnością rozwiązywania problemów naukowych i stosowania metod badawczych w tej dziedzinie.

W podsumowaniu, rozprawa doktorska mgra inż. Patryka Kozieła zawiera wyniki, które uzupełniają analizy znanych do tej pory metod i proponują nowe konstrukcje wraz z analizą ich bezpieczeństwa. Autor uzyskał wartościowe rezultaty w zakresie analizy bezpieczeństwa protokołów kryptograficznych, które rozwiązują istotny problem aplikacyjny w dziedzinie informatyki i które mogą spotkać się z zainteresowaniem zarówno projektantów systemów zabezpieczeń informacji jak również środowiska teoretyków. Pomimo szeregu niedociągnięć, które omówiłem powyżej, oceniam pozytywnie wartość naukową przedłożonej rozprawy doktorskiej i uważam, że w sposób wystarczający spełnia ona kryteria stawiane rozprawom doktorskim przez Ustawę z 20 lipca 2018 roku (Dz. U. 2018 poz. 1668) "Prawo o szkolnictwie wyższym i nauce". Na tej podstawie wnioskuję o dopuszczenie mgra inż. Patryka Kozieła do dalszych etapów procedury uzyskania stopnia doktora w dyscyplinie informatyki technicznej i telekomunikacji.