Warszawa, 05.09.2023

Instytut Podstaw Informatyki Polskiej Akademii Nauk
dr hab. inż. Paweł Morawiecki, prof. IPI PAN
Kierownik Zespołu Kryptografii IPI PAN

Recenzja rozprawy doktorskiej „PACE and PACE CAM: Security Issues and Protocol Extensions" autorstwa Patryka Kozieła

Tematyka rozprawy

Tematyka rozprawy dotyczy analizy bezpieczeństwa protokołów PACE i PACE CAM (ang. Password Authenticated Connection Establishment with Chip Authentication Mapping). Protokół PACE umożliwia bezpieczne autoryzowanie i uwierzytelnianie dwóch stron komunikacji, przy użyciu hasła lub innego wspólnego tajnego klucza. PACE jest często stosowany w kontekście komunikacji między dwoma urządzeniami, takimi jak karty chipowe (np. karty EMV używane do płatności zbliżeniowych) lub urządzenia IoT (Internet of Things). PACE CAM to rozszerzenie protokołu PACE, które łączy uwierzytelnianie za pomocą hasła z uwierzytelnianiem na podstawie karty chipowej lub innych rodzajów kart inteligentnych.

Protokoły te stanowią ważne narzędzie w dziedzinie bezpieczeństwa komunikacji, szczególnie w przypadku aplikacji, gdzie konieczne jest bezpieczne uwierzytelnianie przy użyciu hasła lub innego wspólnego sekretnego klucza. PACE ma na celu zabezpieczenie komunikacji, eliminując potrzebę przesyłania haseł w czystej postaci przez sieć. Dzięki temu zmniejsza ryzyko ataków typu "man-in-the-middle" i innych prób złamania bezpieczeństwa.

WPŁYNĘŁO
28 -09- 2023
RDN-IIT / 179 / 2023

Problemy badawcze w rozprawie

Autor stawia dwa problemy badawcze, których rozwiązanie przedstawia w rozprawie. Pierwszy problem/zagadnienia to wnikliwa analiza bezpieczeństwa tytułowych protokołów ze szczególnym uwzględnieniem poufności i prywatności. Wyniki bazują na wcześniejszych pracach i są wzmocnione wynikiem redukcji aktywnych adwersarzy do ich pasywnych odpowiedników.

Drugą część rozprawy koncentruje się wokół możliwości poszerzenia funkcjonalności protokołów PACE GM. Autor rozprawy przedstawia dwa nowe rozszerzenia tj. obustronne uwierzytelnianie karty i terminala oraz kryptograficznie potwierdzony dowód zaistnienia transakcji.

W pracy brak wyraźnie postawionych celów i hipotezy badawczej.

Struktura rozprawy

Rozprawa podzielona jest na 5 rozdziałów.

Pierwszy rozdział jest wprowadzeniem w tematykę protokołów PACE wraz z prawnym kontekstem stosowanych rozwiązań. Autor przybliża istniejące regulacje i pewne szczegóły implementacji rozwiązań elektronicznych kart ID. W podrozdziale 1.5 omówiona jest krótko literatura przedmiotu badań.

Rozdział 2 stanowi krótki przegląd teoretycznych podstaw rozprawy i wprowadza pojęcia używane w dowodach i twierdzeniach w dalszej części pracy. W szczególności zdefiniowany jest adwersarz i jego możliwości obliczeniowe, rozróżnienie między pojęciami „pomijalna przewaga" (ang. negligible advantage) i „praktycznie pomijalna przewaga" (ang. practically negligible advantage) w kontekście ataków na protokoły. Dalej krótko przedstawione są definicje funkcji skrótu, szyfrowania, podpisu i schematu identyfikacyjnego Schnorra. Rozdział kończy się opisem algorytmu generującym kod MAC (ang. message authentication code).

W kolejnym rozdziale przedstawione i przeanalizowane są kluczowe funkcje zabezpieczeń protokołów PACE i PACE CAM. Analiza ta w dużej mierze bazuje na pracy „Privacy and Security Analysis of PACE GM Protocol" autorstwa M. Kutyłowskiego i P. Kubiaka, w której zarysowane są dowody bezpieczeństwa. Przeprowadzona analiza dla protokołu

PACE w większości pokrywa się z wnioskowaniem dla PACE CAM, ze względu na podobieństwo obu protokołów.
Rozdział 4 zawiera autorskie rozszerzenia protokołu PACE. Pierwsze rozszerzenie do PACE Mutual Authentication, które oferuje obustronne uwierzytelnianie zarówno dla karty chipowej jak i terminala. Ten fragment pracy bazuje na publikacji konferencyjnej:

Patryk Kozieł, Przemysław Kubiak, and Mirosław Kutyłowski. PACE with Mutual Authentication – Towards an Upgraded eID in Europe. In Computer Security – ESORICS 2021, pages 501–519. Springer Interna- tional Publishing, 2021.

Drugie oryginalne rozszerzenie protokołu to kryptograficzne potwierdzenie, że dana transakcja miała miejsce (proof of presence). By uzyskać tę funkcjonalność Doktorant wykorzystuje jeden z wariantów protokołu identyfikacyjnego Schnorra. Wyniki dotyczące tej części pracy ukazały się wcześniej w pracy:

Mirosław Kutyłowski, Przemysław Kubiak, Patryk Koziel, and Yanmei Cao. Poster: eID in Europe - Password Authenticatio Revisited. In 2021 IFIP Networking Conference (IFIP Networking), pages 1–3, 2021.

Rozprawa zakończona jest krótkim podsumowaniem i nakreśleniem obiecujących dalszych kierunków badań.

Uwagi

Praca jest interesująca, podejmuje ważny współcześnie temat i nawiązuje do konkretnych rozwiązań legislacyjno-technicznych. Styl i język pracy jest zwięzły, Autor nie stroni od formalizmu matematycznego. Miejscami rozprawa jest trudna w odbiorze, brakowało mi więcej treści „z lotu ptaka", który przyjaźniej wprowadzałby w najbardziej technicznie złożone fragmenty dysertacji. Znajduje to odzwierciedlenie w bardzo skromnej literaturze (22 pozycje bibliograficzne) oraz brak jakichkolwiek schematów, rysunków czy diagramów. W mojej ocenie rozprawa doktorska powinna wyjść poza ramy typowego artykułu konferencyjnego skierowanego do wąskiej grupy specjalistów i poszerzać kontekst. Tym samym być bardziej przystępna dla nieco większego grona czytelników.

Zdecydowanie pozytywnie oceniam Rozdział 4 dotyczący projektowania rozszerzeń protokołów. Przyjęta metodologia projektowanie dobrze wykorzystuje istniejące rozwiązania i pozwala na łatwą adaptację nowych funkcjonalności.

Poniżej przedstawiam kilka uwag szczegółowych i wątpliwości.

W rekomendacji do protokołu PACE pojawia się funkcja skrótu SHA-1. Funkcja ta została złamana i nie powinna być rekomendowana. Szczególnie, że nowsze rozwiązania standardy są bezpieczniejsze i bardziej wydajne.

W podrozdziale 3.5.1 Privacy „Tracking" pada zdanie:
„Unless the CAN numbers are issued in a heavy non-uniform way, the probability of false positives in tracking is quite limited."

Pojęcie „heavy non-uniform" jest bardo luźno użyte, warto byłoby dookreślić co Autor ma na myśli. Szczególnie, że w całej pracy widać dbałość o definicję używanych pojęć.

Niektóre zdania są zdecydowanie za długie, rozciągają się na kilka linijek. Przykładowo zdanie ze strony 18 „While for some scenarios, an authentication merely by..." zajmuje cztery linijki, trudno się czyta.

Inne drobne błędy językowe:
strona 7: jest „adversary not able", powinno być „adversary is not able"
strona 12: „The brute-force attack way..." nie brzmi dobrze (lepiej bez „attack")
strona 65: jest „they were presented", powinno być „there were presented"

Konkluzja

Wiedzę Kandydata z zakresu tematyki rozprawy i dyscypliny oceniam wysoko. Autor w przedłożonej rozprawie rozwiązał oryginalny problem naukowo-badawczy tj. wprowadził nowe funkcjonalności dla rodziny protokołów PACE. Konkludując, uważam, że złożona rozprawa mgr Patryka Kozieła spełnia wymagania ustawowe i zwyczajowe stawiane pracom doktorskim i może stanowić podstawę nadania stopnia doktora w dziedzinie nauk inżynieryjno-technicznych w dyscyplinie informatyka techniczna i telekomunikacja.

Paweł Morawiecki

Paweł Morawiecki