Prof. dr hab. inż. Zbigniew Kotulski,
Instytut Telekomunikacji Politechniki Warszawskiej

Warszawa, 16 grudnia 2018 r

RECENZJA ROZPRAWY DOKTORSKIEJ WRAZ Z UZUPEŁNIENIEM Z DNIA 19.10.2018 ROKU, WYKONANA DLA RADY NAUKOWEJ INSTYTUTU PODSTAW INFORMATYKI POLSKIEJ AKADEMII NAUK

Tytuł rozprawy: Zastosowanie i ochrona danych biometrycznych przy autoryzacji i identyfikacji

Autor rozprawy: mgr inż. Wojciech Wodo, Politechnika Wrocławska

Wstęp

Recenzowana rozprawa doktorska poświęcona jest problematyce bezpieczeństwa metod biometrycznych w zastosowaniach związanych z identyfikacją i uwierzytelnieniem osób oraz autoryzacją transakcji realizowanych drogą elektroniczną. Rozprawa została napisana w roku 2017 i zawiera wyniki badań oraz opinie Autora uzyskane do tego czasu. W ciągu roku 2018, w odpowiedzi na uwagi Recenzenta, pana prof. Andrzeja Pacuta, Doktorant przeprowadził dodatkowe badania niektórych przedstawionych zagadnień związanych z danymi biometrycznymi usuwając zauważone usterki i opracował wyjaśnienia kwestii niejasnych lub nieprecyzyjnie sformułowanych. Zostało to przedstawione w załączonym uzupełnieniu rozprawy.

Praca jest napisana w języku polskim i liczy 87 stron (uzupełnienie ma 4 strony). Podzielona jest na 6 rozdziałów, z których rozdział pierwszy (str. 4-12) jest wstępem zawierającym wprowadzenie do tematyki, tezę rozprawy poprzedzoną zestawieniem scenariuszy zrealizowanych w celu jej wykazania i zwięzły opis uzyskanych w rozprawie wyników z wykazem publikacji opracowanych na ich podstawie. Rozdział drugi (str. 13-31) stanowi wprowadzenie do metod ochrony danych biometrycznych.

Oprócz przedstawienia wybranych metod maskowania surowych danych biometrycznych, znanych z literatury przedmiotu, Doktorant przedstawił w tym rozdziale autorski protokół uwierzytelnienia biometrycznego dla anulowalnych biometryk wykorzystujący tzw. zbiory zachowujące prywatność i dowody z wiedzą zerową. Kolejne dwa rozdziały, oznaczone numerami 3 (str. 32-63) i 4 (str. 64-75) przedstawiają główne oryginalne wyniki badań ukierunkowane na ich praktyczne wykorzystanie. Rozdział 3 dotyczy analizy spersonalizowanej techniki uderzania w klawiaturę (ang. Keystroking) i ochrony tożsamości biometrycznej piszącego użytkownika. Główne wyniki tego rozdziału to propozycje algorytmów maskujących cechy charakterystyczne użytkowników, ich praktyczna implementacja i zbadanie skuteczności działania. Rozdział 4 zawiera propozycję systemu kontroli dostępu wykorzystującego dane biometryczne pobrane od użytkownika (w praktyce: obraz twarzy) i jego elektroniczny dokument tożsamości. W rozdziale 5 (str. 77-78) podsumowano wyniki przedstawione w rozprawie, a ostatni dwustronicowy rozdział 6 jest streszczeniem rozprawy w języku angielskim. Rozdział ten poprzedzony jest wykazem literatury składającym się z 84 pozycji (dodatkowo 5 pozycji bibliograficznych zawiera uzupełnienie), w tym 6 prac autorstwa lub współautorstwa pana magistra inżyniera Wojciecha Wodo. W pracy umieszczono 34 rysunki, 4 tablice i 4 specyfikacje algorytmów zapisanych w formie pseudokodu.

Dalszą część recenzji została przygotowana w punktach wzorowanych na schemacie stosowanym na Wydziale Elektroniki i Technik Informacyjnych Politechniki Warszawskiej, by nie pominąć w recenzji żadnego z istotnych aspektów rozprawy.

Omówienie i ocena rozprawy

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

Celem rozprawy jest opracowanie nowych metod ochrony danych biometrycznych oraz przygotowanie rozwiązań praktycznych realizujących metody ochrony wybranych biometryk.

Próbując zaliczyć pracę do jednej z kategorii: teoretycznych lub konstrukcyjnych skłonny byłbym do zaklasyfikować ją jako pracę ukierunkowaną na praktyczne wykorzystanie biometrii. W rozdziale drugim rozprawy przedstawiono wprawdzie interesujący wynik teoretyczny, jakim jest propozycja protokołu uwierzytelnienia z wiedzą zerową opartego na danych biometrycznych, jednak główne wyniki pracy dotyczą przygotowania praktycznych metod ochrony, ich eksperymentalnego przetestowania i przygotowanie do wdrożenia. Autor rozprawy przedstawia w rozprawie jako swoje ważne osiągnięcia nie tylko zgłoszenie patentowe dotyczące urządzenia do ochrony tożsamości biometrycznej, ale także zastrzeżenie w Urzędzie Patentowym RP znaku towarowego dotyczące tego urządzenia i uzyskanie dla prototypu laboratoryjnego potwierdzenie wymogów dyrektyw Nowego Podejścia Unii dla Europejskiego Obszaru Gospodarczego w zakresie kompatybilności elektromagnetycznej EMC, uprawniające producenta do oznaczenia wyrobu symbolem CE, zatem wdrożenie jest tu ważnym perspektywicznym celem badań prowadzonych w ramach doktoratu.

Jako tezę rozprawy sformułowano stwierdzenie, że „w wielu obszarach możliwa jest realizacja ochrony danych biometrycznych na stosunkowo zadowalającym poziomie". Aby wykazać tak sformułowaną tezę zaproponowano, i w znacznej mierze zrealizowano w praktyce, szereg przykładów algorytmów i aplikacji, w których zapewniono następujący zakres ochrony danych biometrycznych:

- Ochrona przed niezamierzonym przepływem danych biometrycznych stwarzającym zagrożenie ujawnienia tych danych. Zagadnienie to zrealizowano w przypadku ochrony tożsamości piszącego na klawiaturze komputera.
- Ochrona danych biometrycznych przed nieuprawnionym ujawnieniem w czasie realizacji protokołów uwierzytelnienia. Zagadnienie to było rozpatrywane w przypadku dowodów z wiedzą zerową oraz poprzez zastosowania znakowania wodnego danych biometrycznych wskazującego odbiorcę tych danych.
- Ochrona utajnionych danych biometrycznych w czasie ich przechowywania w bazach danych, repozytoriach i urządzeniach.
- Ochrona uprawnień do wykorzystania upublicznionych danych biometrycznych. Metodą ochrony jest tu znakowanie wodne danych.

Po przestudiowaniu rozdziału 1 doktoratu mogę stwierdzić, że cel, zakres i teza

rozprawy zostały jasno i zwięźle sformułowane przez Doktoranta. Uzupełnienie dołączone do rozprawy nieco modyfikuje uzasadnienie celowości wykorzystania danych biometrycznych do uwierzytelnienia i autoryzacji, ale nie ingeruje w treść samej tezy rozprawy.

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?

Tematyka rozprawy mieści się w zakresie dwóch obszarów badań: biometrii i technik uwierzytelnienia i autoryzacji. W rozprawie nie przedstawiono szerokiego spektrum rozwiązań zarówno w zakresie metod biometrycznych, jak i aktualnych tendencji dotyczących technik uwierzytelnienia, zwłaszcza uwierzytelnienia wielopoziomowego (ang. multi-factor authentication), które jest dzisiaj standardem, zwłaszcza, gdy jedna z metod uwierzytelnienia należy do biometrii. Najnowsze cytowane prace pochodzą z 2015 roku. Zatem brak jest w rozprawie przeglądu najnowszych osiągnięć z zakresu obejmującego tematykę rozprawy. Jest to jednak zrozumiałe: rozprawa jest ukierunkowana na praktyczne wdrożenia wybranych metod, a do wdrożeń zwykle wykorzystywane są metody nowe, ale już sprawdzone. W zakresie zagadnień związanych z proponowanymi przez Doktoranta metodami biometrycznymi i technikami ich analizy przedstawiane są właściwe odniesienia do literatury, dokonany jest przegląd wcześniejszych i podobnych rozwiązań, a wszystkie wykorzystywane metody i algorytmy zaczerpnięte z literatury są właściwie udokumentowane odnośnikami literaturowymi. Zatem bibliografia rozprawy i analiza przytoczonych w niej publikacji jest właściwa i świadczy o znajomości przez Doktoranta tematyki badań i o jego głębokiej wiedzy. W załączonym do rozprawy uzupełnieni Autor wykorzystują również i cytuje wyniki nowszych publikacji, w tym dostępnych on-line.

Czy autor rozwiązał postawione zagadnienia, czy użył właściwej do tego metody i czy przyjęte założenia są uzasadnione?

Cele pracy przedstawione w pierwszym rozdziale zostały zrealizowane, a teza

rozprawy (która była sformułowana w sposób dający wiele możliwości jej wykazania) została potwierdzona. Doktorant przedstawił zarówno teoretyczny model protokołu zabezpieczającego dane biometryczne, jak i zrealizował kilka praktycznych eksperymentów, z wykorzystaniem aplikacji i rozwiązań sprzętowych opracowanych przez siebie lub z dużym udziałem własnym, potwierdzających możliwość ochrony danych biometrycznych. Wykorzystane metody badawcze są nowoczesne, a sposób ich wykorzystania jest nowatorski i oryginalny. Załączony dodatek do rozprawy doprecyzowuje uzasadnienia wykorzystanych technik biometrycznych i sposobów ich ochrony oraz wyjaśnia wątpliwości wskazane w recenzji prof. Andrzeja Pacuta.

Na czym polega oryginalność rozprawy, co stanowi samodzielny i oryginalny dorobek autora, jaka jest pozycja rozprawy w stosunku do stanu wiedzy prezentowanej przez literaturę światową?

Oryginalne wyniki rozprawy zawarte są w trzech rozdziałach, z których każdy przedstawia inny zakres zagadnień związanych z biometrią. Odpowiada to przyjętej koncepcji pracy, według której zdecydowano się wykazać sformułowaną tezę poprzez zrealizowanie kilku niezależnych zadań. Według mnie, do najważniejszych oryginalnych wyników przedstawionych w rozprawie należą:

- Propozycja nowego protokołu uwierzytelnienia z wiedzą zerową wykorzystującego spersonalizowane dane biometryczne i chroniącego te dane przed ujawnieniem (rozdział 2 rozprawy).
- Zaprojektowanie mechanizmów ochronnych do maskowania charakterystyki sposoby pisania na klawiaturze przez użytkownika, ich praktyczna implementacja w układzie elektronicznym i wszechstronne przetestowanie tego rozwiązania (rozdział 3 rozprawy).
- Opracowanie systemu kontroli dostępu wykorzystującego biometrię twarzy, wspomaganego użyciem kart procesorowych oraz szerokie przebadanie jego efektywności (rozdział 4). Wyniki związane z tym systemem, w szczególności przeprowadzone eksperymenty, zostały dodatkowo wyjaśnione w uzupełnieniu.

Pan mgr inż. Wojciech Wodo przeprowadził obszerne badania eksperymentalne w środowisku zbliżonym do realnego środowiska pracy aplikacji. Tego typu badania, w połączeniu z dużą oryginalnością proponowanych rozwiązań mogłyby być

przedmiotem bardzo dobrych publikacji naukowych. Doktorant ograniczył się do publikacji konferencyjnych lub w czasopismach o mniejszym odbiorze w środowisku naukowym, zatem nie w pełni wykorzystał tę szansę.

Czy autor wykazał umiejętność poprawnego i przekonywującego przedstawienia uzyskanych przez siebie wyników (zwięzłość, jasność, poprawność redakcyjna rozprawy)?

Rozprawa jest napisana w sposób przejrzysty i zrozumiały. Teza pracy jest jasno sformułowana, a sposób jej udowodnienia również nie budzi wątpliwości. Terminologia naukowa jest (poza nielicznymi wyjątkami) poprawnie stosowana. W uzupełnieniu doprecyzowano niektóre definicje wykorzystywane w rozprawie. Również usterki językowe i redakcyjne są nieliczne. Niżej podaję kilka przykładów sformułowań niepoprawnie (moim zdaniem) użytych.

W pracy, głównie w rozdziałach 1 i 2, używane są terminy: „funkcja haszująca" i „hasz" (nie: angielskie sformułowania: „hash function" dla oznaczenia funkcji i „hash" dla oznaczenia wyniku jej działania). Zamiast tego, zgodnie z polską terminologią, powinny być użyte sformułowania „funkcja skrótu" (lub: „kryptograficznie bezpieczna funkcja skrótu") i „skrót".

Na stronie 9 użyto słowa „funkcjonalność" na oznaczenie funkcji, jakie pełni elektroniczny dokument tożsamości (dokładniej: jakie usługi bezpieczeństwa realizuje). Podobnie, błędnie użyto tego słowa na str. 66. (Słowo „funkcjonalność" to pojęcie z zakresu ergonomii).

Kilkakrotnie, np. str. 5, 22, 32, 33, użyto zwrotu „oparte o coś" zamiast „oparte na czymś", gdy jest mowa o wykorzystaniu pewnej własności do realizacji celu.

Kilkakrotnie użyto zwrotu „przy pomocy czegoś" zamiast „za pomocą czegoś", gdy była mowa o wykorzystaniu metody lub narzędzia do realizacji celu, np. str. 18, 67.

Znalazłem kilka błędów literowych w pracy i dostawiłem brakujące przecinki w wydrukowanym swoim egzemplarzu rozprawy.

Usterki redakcyjne są nieliczne i nie wpływają na moją pozytywną ocenę sposobu przygotowania rozprawy i jakości prezentacji.

Jakie są słabe strony rozprawy i jej główne wady?

Autor rozprawy zaproponował kilka interesujących rozwiązań bezpieczeństwa, zrealizował praktyczne implementacje algorytmów i wykonał wiele eksperymentów oceniając praktycznie jakość zaprojektowanych rozwiązań i odpowiadając na wiele nasuwających się pytań. Tym niemniej, zaprezentowane rozwiązania i pomysły ich rozwoju nasuwają kolejne pytania warte udzielenia odpowiedzi.

W rozdziale 3 jako charakterystykę piszącego przyjęto rozkłady czasów generowania digrafów. Jak te charakterystyki zmienią się, gdy zostanie użyta klawiatura z innym układem klawiszy? (np. „Polish (programmers)" i „Polish (214)").

Czy nie można zidentyfikować urządzenia użytkownika (a przez to i samego użytkownika) na podstawie analizy charakterystyki generatora pseudolosowego stosowanego do maskowania uderzeń w klawisze?

Jako jedną z metod ochrony prywatności piszącego Doktorant proponuje stosowanie charakterystyki uderzeń w klawiaturę odpowiadających innemu użytkownikowi (Rozdział 3.2.5), wskazując przy tym, że jest to rozwiązanie o wysokim poziomie bezpieczeństwa. Pomińmy pytanie, czy takie rozwiązanie jest etyczne (wyobraziłem sobie sytuację, gdy ktoś używa moich danych biometrycznych i sam odpowiedziałem sobie na to pytanie). Warto jednak byłoby ustalić, jak stosowanie takiej metody wygląda z punktu widzenia uregulowań prawnych? Jest to szczególnie ważne w czasach powszechnych „fake news" i „farm trolli" wykorzystywanych w Internecie.

Oceniają ogólnie wysoko wyniki zaprezentowane w rozprawie, chciałbym zwrócić uwagę, że najmniej dopracowanym jej elementem jest zaprezentowana w ostatnim podrozdziale rozdziału 4 koncepcja zdalnej identyfikacji użytkownika. Jest to raczej pomysł prac do zrealizowania, bez specyfikacji protokołów i analizy bezpieczeństwa. W tym wypadku przydałoby się wykorzystanie współczesnej wiedzy z zakresu wielopoziomowych technik uwierzytelnienia. Podobnie, zaprezentowany w rozdziale 4 system kontroli dostępu, aby stać się praktycznie realizowalny, powinien być systemem dwupoziomowym (przynajmniej z uwzględnieniem ochroną pinem karty procesorowej). O konieczności przetwarzania biometrycznych danych prywatnych w karcie pisze sam Autor jako o wersji rozwojowej systemu. Tak więc, nie podważając wartości wyników zaprezentowanych w tym obszarze rozprawy, chciałbym stwierdzić,

że poziom analizy, a zwłaszcza poziom gotowości technologicznej rozwiązania zaprezentowanego w rozdziale 3 jest znacznie wyższy niż ma to miejsce dla systemu kontroli dostępu.

Jaka jest przydatność rozprawy dla nauk technicznych?

Praca przedstawia przykłady oryginalnych i nowatorskich rozwiązań bezpieczeństwa dla systemów biometrycznych. Wykorzystują one zaawansowane metody matematyczne, są zaimplementowane programowo, a w przypadku systemu ochrony tożsamości piszącego – wdrożone do prototypu urządzenia. Wyniki uzyskane w pracy stanowią istotny wkład do rozwoju metod biometrycznych i ich bezpieczeństwa, poparty zasobem wyników eksperymentalnych przydatnych również dla innych autorów jako źródło danych porównawczych.

Podsumowanie i ocena rozprawy

W swojej rozprawie doktorskiej pan magister inżynier Wojciech Wodo poruszył ważny problem bezpieczeństwa danych biometrycznych używanych do identyfikacji tożsamości osób. Ochrona tych danych jest nieporównanie ważniejsza od ochrony analogicznych danych kryptograficznych, ponieważ są one jednoznacznie i niezmiennie przypisane do osób i ich kompromitacja nie może być naprawiona. Zaproponowane przez Doktoranta metody ochrony, sformułowane w postaci rozbudowanej tezy doktorskiej, zostały w rozprawie precyzyjnie opisane, profesjonalnie przebadane i częściowo wdrożone. Przydatność w praktyce zaproponowanych metod nie budzi wątpliwości, zatem sformułowaną w rozdziale 1 tezę rozprawy można uznać za udowodnioną.

Reasumując, rozprawę doktorską pana magistra inżyniera Wojciecha Wodo oceniam bardzo dobrze. Uważam, że spełnia ona wymagania stawiane przez *USTAWĘ z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki*, Dz.U. z 2003 r. Nr 65, poz. 595; z późniejszymi zmianami, tekst jednolity. Dz.U. 2014 poz. 1852, rozprawom doktorskim w dziedzinie nauk technicznych w dyscyplinie naukowej: informatyka i wnioskuję o jej dopuszczenie do publicznej obrony.

Kotulski

Prof. dr hab. inż. Zbigniew Kotulski