Szczecin, 15.07.2015

RECENZJA
rozprawy doktorskiej mgra inż. Lucjana Hanzlika pt. „Cryptographic Protocols for Modern Identification Documents”

Niniejszą recenzję przedstawiam na prośbę Rady Naukowej Instytutu Podstaw Informatyki Polskiej Akademii Nauk w Warszawie w ramach realizowanego przewodu doktorskiego mgra inż. Lucjana Hanzlika.

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 lub zamierza wydawać swoim obywatelom elektroniczne dokumenty tożsamości. Coraz bardziej wzrastająca liczba systemów elektronicznej identyfikacji opartych na tego typu dokumentach wspiera z jednej wiele nowych usług typu e-administracja i e-handel, ale równocześnie rodzi wiele nowych problemów związanych z zapewnieniem tego typu usługom zabezpieczeń i prywatności na jak najwyższym poziomie.

Problem utraty prywatności przez użytkowników elektronicznych dokumentów tożsamości jest uważany przez European Union Agency for Network and Information Security (ENISA) za jedno najważniejszych zagrożeń w systemach elektronicznej identyfikacji, pozwalające adwersarzowi na niezamierzone ujawnienie danych osobowych, a następnie ich nieuprawnione wykorzystywanie. Wymagania zapobiegające m.in. tego typu zagrożeniom zostały określone przez agencję ENISA w dokumencie *Privacy Features of European eID Card Specifications*[1]. Zalecenia agencji ENISA powinny być brane pod uwagę przez kraje członkowskie UE podczas projektowania i wdrażania swoich narodowych dokumentów eID. Zalecenia te są ważne także w kontekście nowego rozporządzenia eIDAS[2], w którym zaleca się nostryfikowanie krajowych systemów identyfikacji nie tylko zachowania prywatności, ale także interoperacyjności pomiędzy różnymi domenami elektronicznej identyfikacji oraz usług opartych na eID.

Jednym z najciekawszych realizowanych obecnie projektów z zakresu eID jest niemiecki

[1] I. Naumann, G. Hogben European *Privacy Features of European eID Card Specifications*, Network and Information Security Agency (ENISA), 2009 (http://www.enisa.europa.eu/activities/identity-and-trust/trust-services/eid-cards-en)

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 dnia 23.07.2014r. *w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym*

projekt nPA (niem. neuer Personalausweis). Według zgodnej opinii wielu ekspertów i naukowców w ramach tego projektu powstały i powstają najbardziej zaawansowane, praktyczne oraz zapewniające prywatność rozwiązania z zakresu dokumentów eID. Opinia ta w szczególności odnosi się do protokołów kryptograficznych projektowanych na potrzeby niemieckiego dokumentu eID zapewniających bezpieczną komunikację pomiędzy dokumentem (dokładniej zaawansowanym układem scalonym z kryptoprocesorem wbudowanym w dokument eID), a czytnikiem dokumentu oraz odpowiednio terminalem.

Niemiecki dokument eID zapewnia nie tylko możliwość konwencjonalnej identyfikacji w oparciu o dowód osobisty lub paszport (funkcja ePass), wykorzystywanej np. podczas kontroli granicznej, ale udostępnia także dwie nowe funkcje: funkcję eID (wzajemne potwierdzanie tożsamości w przypadku użytkowników oraz aplikacji typu e-administracja i e-handel wymagających wzajemnego uwierzytelnienia) i funkcję eSign (składanie kwalifikowanego podpisu elektronicznego).

Protokoły kryptograficzne dokumentu eID realizowane są w dwóch etapach. Początkowo, strony protokołu wykonują uwierzytelniany hasłem protokół ustanawiania połączenia (PACE), którego pomyślne zakończenie pozwala za zgodą użytkownika na utworzenie bezpiecznego kanału pomiędzy dokumentem eID a czytnikiem. Następnie pomiędzy dokumentem eID a zdalnym punktem końcowym, nazywanym terminalem lub dostawcą usługi (SP) uruchamiany jest protokół kontroli dostępu, np. protokół EAC (ang. Extended Access Control), pozwalający na wzajemne uwierzytelnienie oraz ustanowienie kolejnego bezpiecznego kanału pomiędzy dokumentem eID a zdalnym punktem końcowym. Należy zauważyć, że dokument eID jest tak zaprojektowany, że pozwala na zrealizowanie pomiędzy wymienionymi punktami opcjonalnego protokołu nazywanego protokołem ograniczonej identyfikacji (ang. Restricted Identification, RI). Protokół ten daje możliwość posiadaczowi dokumentu eID uwierzytelnienia się i uzyskania dostępu do usługi tylko na podstawie pseudonimu bez ujawnienia jakichkolwiek swoich danych osobowych.

Dokumentacja projektu nPA jest bardzo obszerna i zawiera szczegółowe opisy zaawansowanych mechanizmów zabezpieczeń elektronicznych dokumentów podróżnych (MRTD) oraz tokenów eIDAS stosowanych w systemach elektronicznej identyfikacji, uwierzytelniania oraz usług zaufania. Przeglądając te dokumenty można by odnieść wrażenie, że w zakresie protokołów kryptograficznych opisywanych w tych dokumentach nie ma już nic do zrobienia, zwłaszcza z punktu widzenia potencjalnych problemów naukowych. Okazuje się jednak, że jest to mylne wrażenie, co w znakomity sposób pokazał Autor recenzowanej rozprawy.

Autor założył, że głównym celem rozprawy jest zbadanie bezpieczeństwa algorytmów kryptograficznych wprowadzonych w ramach projektu nPA na potrzeby niemieckiego dokumentu eID. W wielu przypadkach protokoły nPA mają formę rozwiązań ramowych, w których dopracowanie szczegółów pozostawia się do dyspozycji implementatorom. Przykładem takiego protokołu jest protokół PACE, w którym stosowane mogą być różne funkcje odwzorowania pozwalające na generowanie różnych sesyjnych generatorów grupy. Tego typu protokoły może być inspiracją do projektowania własnych odwzorowań. Tak też zrobił Autor rozprawy proponując w rozdz. 3.7 protokół Pairing PACE|AA oparty na iloczynie dwuliniowym. Co prawda, własne wersje protokołów, zanim nabiorą znaczenia praktycznego, muszą uzyskać status protokołów znormalizowanych akceptowanych przez ICAO[3] lub BSI[4], ale nie oznacza to, że należy zrezygnować z nowych, innowacyjnych

[3] ang. International Civil Aviation Organization
[4] niem. Bundesamt für Sicherheit in der Informationstechnik

protokołów. Jest to o tyle istotne, że - jak słusznie zauważa Autor - wprowadzone w ramach projektu nPA protokoły kryptograficzne nie zostały wcześniej poddane wszechstronnej analizie bezpieczeństwa lub też ich bezpieczeństwo wymaga silnych założeń o zabezpieczeniach (zwłaszcza sprzętowych) dokumentów eID. Stąd słuszna jest uwaga Autora, że *chociaż niektóre dowody bezpieczeństwa zostały opublikowane już po wdrożeniu niemieckiego dokumentu eID, to bezwarunkowe zaufanie bezpieczeństwu sprzętu może budzić wątpliwości w wielu krajach*. W tym też Autor upatruje szansy na implementację własnych rozwiązań w krajowych systemach elektronicznej identyfikacji.

Biorąc pod uwagę powyższe fakty uważam, że obszar badawczy będący przedmiotem rozprawy został dobrze określony, jest bardzo aktualny i ma duże znaczenie praktyczne. To ostatnie stwierdzenie może budzić wątpliwości, ponieważ rozprawa ma wybitnie teoretyczny charakter. Jestem jednak przekonany, że każdy, kto bliżej przyjrzy się projektowi nPA łatwo przełoży algorytmy proponowane w rozprawie na praktyczne rozwiązania stosowane w systemach elektronicznej identyfikacji z użyciem dokumentów eID.

Doktorant w swojej rozprawie opracował szereg rozszerzeń protokołu PACE oraz przedstawił oryginalne propozycje protokołów kryptograficznych należących do rodziny protokołów PACE i RI, których implementacja nie wymaga rozbudowanej infrastruktury zaufania. Pewną wadą rozprawy jest brak jawnie sformułowanego problemu naukowego, na przykład w formie postawionej tezy pracy. Utrudnia to nieco ocenę merytorycznej wartości pracy. Dlatego na potrzeby tej oceny - w oparciu o przedstawione w rozprawie streszczenie - zakładam, że tezę można sprowadzić do następującego stwierdzenia: *pomimo osłabienia założeń o silnym bezpieczeństwie sprzętu stosowanego w systemie eID możliwe jest opracowanie nowych wersji protokołów kryptograficznych o udowadnialnym bezpieczeństwie*. Co prawda Autor we wstępie idzie jeszcze dalej pisząc, że jego *rozwiązania są bezpieczne nawet, gdy wystawca dokumentów nie może być obdarzony zaufaniem*, ale przy braku definicji zakresu tego zaufania tą część tezy pominę (wrócę jednak do niej w przedstawionych dalej uwagach merytorycznych). Niezależnie od tego przyjmuję dodatkowo, że opracowane w rozprawie nowe wersje protokołu PACE jedynie zwiększają słuszność sformułowanej tezy.

W mojej ocenie, tak sformułowana teza pracy została w pełni udowodniona, a postawiony w rozprawie cel polegający na analizie bezpieczeństwa niektórych protokołów kryptograficznych wprowadzonych w ramach projektu nPA na potrzeby niemieckiego dokumentu eID, a także zaproponowanych przez Autora rozszerzeń tych protokołów oraz oryginalnych propozycji został w pełni osiągnięty. Co więcej, rozważane w rozprawie zagadnienia są aktualne i istotne w obszarze informatyki.

2. Analiza treści rozprawy oraz uzyskanych wyników

Recenzowana rozprawa doktorska została przygotowana w języku angielskim. Jej struktura jest bardzo przejrzysta i składa się z czterech rozdziałów, streszczenia (w języku angielskim i polskim), podsumowania pracy oraz bibliografii obejmującej 55 pozycji literaturowych. Całość pracy obejmuje 116 stron i ma charakter teoretyczny. Wyniki własne doktoranta przedstawione są w rozdziałach 3 i 4.

We wprowadzeniu do pracy (rozdz. 1) Autor zwięźle opisał kontekst głównych zagadnień, projekt nPA oraz opracowaną na jego potrzeby rodzinę protokołów kryptograficznych. Zwrócił także uwagę na wady istniejących protokołów, możliwości ich usprawnienia/rozszerzenia oraz opracowania własnych wersji przy obniżonych wymaganiach nakładanych na bezpieczeństwo używanego sprzętu. Wadą tej części pracy jest brak nałożenia opracowanych lub opracowywanych protokołów na generyczną architekturę systemu eID

pokazującego podstawowe interakcje pomiędzy użytkownikiem (posiadaczem dokumentu eID) a pozostałymi komponentami systemu. Odczuwalny jest także, zwłaszcza w dalszej części pracy, brak zestawienia oznaczeń i skrótów używanych w pracy oraz jednoznacznych definicji komponentów i stron zaangażowanych w realizację protokołów, np. pojęcia czytnika, terminala, dostawcy usługi. W tej części pracy Autor nie umieścił – i słusznie – analizy literaturowej problemów z wiązanych z tematyką pracy. Zrobił to w kolejnych rozdziałach przed opisem formułowanych i rozwiązywanych problemów. Pozwala to Autorowi na bieżące udostępnianie niezbędnych faktów wraz odniesieniami do właściwych źródeł literaturowych, co znakomicie ułatwia zrozumienie omawianych problemów i ich znaczenia na tle innych rozwiązań. W podsumowaniu rozdziału Autor umieścił także krótki opis swoich najważniejszych osiągnięć.

Rozdział drugi zawiera podstawowe informacje i definicje z zakresu podstaw kryptografii, w tym m.in. definicję i własności iloczynu dwuliniowego, definicje trudnych problemów obliczeniowych, na których opierają się dowody bezpieczeństwa zaproponowanych w pracy protokołów kryptograficznych oraz definicje kryptograficznych elementów pierwotnych takich jak podpis cyfrowy, schemat szyfrowy, funkcja skrótu, kody uwierzytelniania wiadomości. W rozdziale tym Autor przedstawił także pojęcie bezpieczeństwa udowadnialnego oraz opisał rozważane w rozprawie modele bezpieczeństwa. Rozdział jest bardzo dobrze skonstruowany, precyzyjny i nie wykracza poza fakty, które są wykorzystywane w dalszej części rozprawy.

W rozdziale trzecim i czwartym przedstawione są najważniejsze wyniki rozprawy rozwijające praktyczną obserwację Autora, że projektowanie i implementacja protokołów kryptograficznych w projekcie nPA wymaga odpowiedniego dopasowania ich do cech części sprzętowej dokumentu eID (np. niewielkich pamięci operacyjnych oraz ograniczonych mocy obliczeniowych procesora) oraz do osłabionych, przez to mniej kontrowersyjnych, założeń dotyczących np. bezwarunkowego zaufania do stosowanych zabezpieczeń sprzętu, przy jednoczesnym zachowaniu pożądanych własności bezpieczeństwa modyfikowanych lub nowoprojektowanych protokołów kryptograficznych.

W rozdziale trzecim Autor najpierw przedstawił składnię protokołu wymiany kluczy uwierzytelnionej hasłem jednej strony (ang. Password One-side Authenticated Key Exchange, OS-PAKE). Celem tego protokołu jest ustanowienie bezpiecznej komunikacji pomiędzy dwoma stronami wyłącznie w oparciu o współdzielone hasło, przy zachowaniu poufności klucza sesyjnego oraz odporności na podszycie się. Następnie Autor przedstawił dwa własne rozszerzenia protokołu PACE, będące konkretnymi przykładami protokołów klasy OS-PAKE. Rozszerzenia te bazują na oryginalnych protokołach projektu nPA uzupełnionych o procedurę aktywnego uwierzytelniania, chroniące dokument eID przed klonowaniem. Pierwsze z rozszerzeń o nazwie SPACE|AA jest uproszczonym rozszerzeniem protokołu PACE z ogólnym odwzorowaniem (PACE-GM). Drugie z zaproponowanych rozszerzeń PPACE|AA oparte na iloczynie dwuliniowym jest o tyle ciekawe, że rozszerza nie tylko protokół PACE-GM, ale także PACE-IM (protokół PACE z odwzorowaniem zintegrowanym). Co prawda Autor pisze, że protokół może pracować z dowolnym odwzorowaniem, ale nie podaje żadnych szczegółów na potwierdzenie tej tezy. W mojej ocenie bardzo ważną, dopełniającą częścią tego rozdziału są cztery twierdzenia dotyczące bezpieczeństwa zdefiniowanych protokołów oraz ich formalne dowody przeprowadzone w modelu losowej wyroczni. Zwykle tego typu dowody są trudne technicznie. Tym bardziej bardzo wysoko oceniam wiedzę Autora oraz jego znajomość technik prowadzenia tego typu dowodów.

Z całą pewnością merytorycznie najciekawszą częścią pracy jest rozdział czwarty. Składają się na to dwa powody. Po pierwsze Autor zajął się wprowadzeniem i sformalizowaniem

protokołów uwierzytelniania pseudonimowego (ang. Pseudonymous Identification, PI). Protokoły PI, ściśle powiązane z ideą ograniczonej identyfikacji RI wprowadzonej w niemieckim dokumencie eID, zapewniają silne anonimowe uwierzytelnienie użytkownika niepozwalające na skojarzenie prowadzonej przez niego aktywności z jego tożsamością. Po drugie, Autor zaprezentował w nim dwie własne wersje protokołów typu PI: protokół ChARI-eCK oraz Pairing RI. Oba protokoły pozwalają na rozwiązanie problemu klucza grupy, polegającego na możliwości powiązania różnych pseudonimów użytkownika stosowanych przez niego w różnych domenach. Jednak z punktu widzenia efektywności lepszy jest protokół Pairing RI, który nie wymaga przechowywania pełnej listy pseudonimów upoważniających do dostępu do określonej domeny. Protokół ten zawiera także bardzo ciekawy pomysł zastosowania schematu szyfrowania Pailliera w algorytmach *Join* i *Issue*. W przypadku obu protokołów Autor sformułował twierdzenia ich bezpieczeństwa i udowodnił je.

Zakończeniem pracy jest bardzo krótkie podsumowanie, które zawiera trzy sugerowane przez Autora istotne usprawnienia w realizowanych obecnie projektach eID.

3. Najistotniejsze osiągnięcia przedstawione w rozprawie

Rozprawa doktorska mgra inż. Lucjana Hanzlika zawiera nowe, oryginalne wyniki dotyczące projektowania i modyfikacji protokołów uwierzytelniania stosowanych w projekcie nPA lub podobnych. Oryginalną wartość proponowanych protokołów podnoszą dodatkowo starannie sformułowane i udowodnione twierdzenia dotyczące ich bezpieczeństwa.

Rozprawa ma charakter teoretyczny, chociaż jak wspomniałem o tym na początku mojej recenzji (pisze o tym także Autor w konkluzji pracy), uzyskane wyniki można w praktyce wykorzystać w realizowanych lub planowanych projektach eID. Autor trafnie wybrał i uzasadnił obszar badań. Oryginalne wyniki Autora zostały przedstawione w rozdziałach 3 i 4. Zostały one zaczerpnięte z pięciu prac opublikowanych lub zgłoszonych do publikacji. Swój osobisty wkład w każdej z tych publikacji Autor przedstawił na początku pracy w punkcie *My contributions*. Niektóre wyniki opublikowane we wspomnianych pracach zostały przez Autora rozszerzone (dotyczy to zwłaszcza protokołów ograniczonej identyfikacji przedstawionych w rozdziale czwartym).

Moim zdaniem, najważniejsze wyniki, przedstawione w rozprawie obejmują:

- opracowanie protokołu SPACE|AA (rozdz. 3.6), będącego rozszerzeniem protokołu PACE-GM wymaganego przez ICAO w dokumentach podróżnych i chroniącego dokument eID przed klonowaniem; wart podkreślenia jest fakt, że mniej więcej w tym samym czasie podobne rozwiązanie zostało zaproponowane i opatentowane przez BSI i przyjęte przez ICAO;
- opracowanie oryginalnego protokołu Pairing PACE|AA (w skrócie PPACE|AA), który dzięki zastosowaniu iloczynu dwuliniowego pozwala na implementację protokołu PACE z ogólnym odwzorowaniem (GM) oraz z odwzorowaniem zintegrowanym (IM); efektywność protokołu PPACE|AA jest porównywalna z protokołem SPACE|AA i wymaga jedynie implementacji iloczynu dwuliniowego po stronie czytnika/terminala; ta ostatnia własność protokołu jest o tle istotna, że na rynku brakuje inteligentnych kar identyfikacyjnych przystosowanych do obsługi iloczynów dwuliniowych[5];

[5] Znany jest mi jedynie jeden przypadek karty, której wersja eksperymentalna została wyprodukowana przez firmę Gemalto (poprzednio Gemplus) w roku 2004 na potrzeby implementacji schematu szyfrowania IBE opracowanego przez Boneh-Franklina.

- opracowanie dwóch protokołów uwierzytelniania z ograniczoną identyfikacją, tj. protokołu ChARI-eCK (ang. Chip Authentication with Restricted Identification) oraz protokołu Pairing RI, które rozwiązują problem klucza grupowego; protokół ChARI-eCK jest dostosowaną do rozszerzonego modelu bezpieczeństwa Canetti-Krawczyka (eCK) wcześniejszą wersją tego protokołu, którego współautorem jest także Autor rozprawy; wadą protokołu ChARI-eCK jest konieczność tworzenia i dystrybuowania listy autoryzującej pseudonimy użytkowników; wada ta została wyeliminowania przez Autora w protokole Pairing RI;
- sformułowanie ośmiu twierdzeń dotyczących bezpieczeństwa protokołów uwierzytelniania opracowanych w rozprawie oraz protokołu EAC+RI opracowanego w ramach projektu nPA; prawdziwość każdego ze formułowanych twierdzeń została poprawnie udowodniona w przyjętym przez Autora modelu bezpieczeństwa; do szczególnie ciekawych należą dowody bezpieczeństwa protokołu ChARI-eCK dla modelu eCK.

Interesującymi dodatkami do rozdziału trzeciego i czwartego są rozważania Autora dotyczące efektywności opracowanych protokołów. Świadczą one o tym, że pomimo teoretycznego charakteru pracy Autor stara się nie tracić z widoku problemów praktycznej implementacji efektów swojej rozprawy.

4. Uwagi merytoryczne

Analiza struktury i zawartości rozprawy wskazuje na jej następujące trzy zalety: precyzyjne merytoryczne zakreślenie obszaru badań, solidną podstawę metodyczną oraz dużą swobodę Autora w projektowaniu/modyfikowaniu protokołów kryptograficznych, a następnie w formalnym dowodzeniu ich bezpieczeństwa. Autor bardzo dobrze porusza się w obszarze badań dotyczących protokołów kryptograficznych, powiązanych w szczególności z niemieckim dokumentem eID oraz dokumentami podróżnymi spełniającymi wymagania ICAO. W każdym miejscu rozprawy planowane przez Autora przedstawienie określonego protokołu poprzedzone jest syntetyczną prezentacją podobnych rozwiązań oraz przedstawieniem algorytmów i modeli będących podstawą proponowanego protokołu oraz ich formalnego dowodu bezpieczeństwa (przykładami tego typu podejścia są protokoły ChARI-eCK i Pairing RI).

Pomimo wymienionych powyżej niewątpliwych zalet pracy, podczas czytania rozprawy nasuwają się pewne uwagi o charakterze dyskusyjnym. Są to:

(a) Autor rozprawy w jawny sposób nie sformułował tezy pracy, co utrudnia określenie *oryginalnego rozwiązania problemu naukowego* w rozumieniu Art. 13.1 Ustawy *o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki*. Prawdą jest, że na początku rozdziału trzeciego i czwartego Autor każdorazowo poprzedza proponowane protokoły kryptograficzne sformułowaniem dedykowanych zadań, a następnie przedstawia ich rozwiązanie. Brakuje jednak spójnego, syntetycznego sformułowania ogólnego problemu naukowego, którego rozwiązanie byłoby bardziej widoczne i – co najbardziej pożądane – bezdyskusyjnie uzasadnione. Na początku niniejszej recenzji sformułowałem na własne potrzeby propozycję przykładowej tezy. Z tezą tą niekoniecznie musi zgadzać się Autor. Dlatego prosiłbym Autora o sformułowanie własnej tezy lub spójnego zestawu zadań, które rozwiązał w rozprawie i należycie to uzasadnił.

(b) Uważam, że tezę w wersji sformułowanej przez mnie we wstępie do niniejszej recenzji Autor udowodnił. Tym niemniej, Autor podczas obrony powinien odnieść się

do następujących sformułowań zawartych w streszczeniu pracy (str. iv, 2 akapit od dołu):

Pokażemy następnie, że rozwiązanie wprowadzone w nPA wymaga silnych założeń o bezpieczeństwie używanego sprzętu oraz dużego zaufania do organu wydającego eID. Dlatego proponujemy dwa rozwiązania, które posiadają tę samą funkcjonalność, ale nie wymagają one tak silnych założeń o sprzęcie. Co więcej, nasze rozwiązania są bezpieczne nawet, gdy wystawca dokumentów nie może być obdarzony zaufaniem.

Jakie wymagania bezpieczeństwa nakładane na sprzęt mogą być osłabione w kontekście proponowanych przez Autora protokołów oraz zagrożeń zdefiniowanych w profilach zabezpieczeń[6,7] opracowanych przez BSI? Ponadto z czego wynika przekonanie Autora, że proponowane przez niego protokoły są bezpieczne nawet, gdy wystawca dokumentów eID nie może być obdarzony zaufaniem? To ostatni problem jest o tyle istotny, że każde osłabienie zaufania do jakiegoś komponentu systemu musi być kompensowane zaufaniem do innego komponentu lub wynikać z dodatkowych procedur wprowadzonych w systemie.

(c) W rozprawie Autor często używa pojęcia „duża infrastruktura klucza publicznego (PKI)". Proszę o wyjaśnienie tego pojęcia oraz wyjaśnienie, kiedy tego typu infrastruktura jest akceptowalna, a kiedy nie w kontekście problemów rozważanych przez Autora w rozprawie.

(d) W pracy odczuwa się brak przedstawienia ogólnej architektury systemu elektronicznej identyfikacji. Utrudnia to zorientowanie się czytelnikowi, czy protokoły omawiane w rozdziale trzecim i czwartym nakładają się na siebie, czy są niezależne od siebie, czy też w końcu mogą być wykonywane w dowolnej kolejności. Brak takiej ogólnej architektury nie ułatwia także dokładnego zidentyfikowania ról stron biorących udział w protokole.

(e) Do analizy bezpieczeństwa protokołów w stosuje się w praktyce metody formalnego i automatycznego dowodzenia bezpieczeństwa protokołów kryptograficznych w oparciu o narzędzia typu np. AVISPA, VerICS, Proverif, Scyther lub Tamarin. Przedmiotem tego typu narzędzi nie jest badanie bezpieczeństwa algorytmów kryptograficznych, ale badanie błędów w logicznej strukturze protokołu. Co więcej wymienione narzędzia pozwalają na badanie bezpieczeństwa protokołów w przypadku zastosowania różnych modeli bezpieczeństwa, w tym bezpieczeństwa w przypadku zastosowania w dowodzie rozszerzonego modelu bezpieczeństwa Canetti-Krawczyka (takie możliwości ma np. narzędzie Tamarin). W związku z powyższym ciekawi mnie, czy Autor rozprawy rozważał zastosowanie narzędzi automatycznego dowodzenia bezpieczeństwa protokołów i jeśli tak, to co legło u podstaw rezygnacji z tego podejścia?

5. Uwagi formalne

Rozprawa jest napisana na bardzo wysokim poziomie językowym, choć obejmuje bardzo trudne zagadnienia teoretyczne. Zdania są poprawnie formułowane, widać dużą erudycję i łatwość pisania. Należy wyraźnie pochwalić Autora pracy za staranność jej przygotowania, zwłaszcza,

[6] Common Criteria - Protection Profile - Electronic Identity Card (ID_Card PP), Version 1.03 15th , December 2009, BSI-CC-PP-0061

[7] Common Criteria Protection Profile - Standard Reader - Smart Card Reader with PIN-Pad supporting eID based on Extended Access Control, Version 1.0, 29.11.2013, BSI-CC-PP-0083

że jest to praca pisana w języku angielskim oraz za poziom merytoryczny, który niestety nieczęsto jest spotykany w przypadku innych prac doktorskich.

Tym niemniej w pracy można znaleźć i wytknąć drobne usterki formalne. Są to między innymi:

(a) istotnym mankamentem utrudniającym studiowanie pracy jest brak spisu oznaczeń, skrótów (głównie związanych z nazwami protokołów) oraz podstawowych pojęć stosowanych w pracy; wymienione braki mają głównie wpływ na trudności nawigowaniu po pracy w przypadku napotkania oznaczenia, skrótu lub pojęcia, które jest wielokrotnie używane w pracy;

(b) w opisach wszystkich protokołów pominięto definicje używanych funkcji skrótu; definicje te są zwykle oczywiste, ale studiujący pracę nie powinien zaprzątać sobie tym głowy; co więcej, funkcje te są częścią parametrów systemowych i powinny być do nich dodane;

(c) str. 35, rys. 3.1: zamiast $Y'_C = \hat{g}^{y'_A}$ i $Y'_R = \hat{g}^{y'_B}$ powinno być odpowiednio $Y'_C = \hat{g}^{y'_C}$ i $Y'_R = \hat{g}^{y'_R}$; podobne błędy powtarzają się na rys. 3.2 i 3.3.

(d) str. 43, wyliczenie 3 od góry: Autor napisał, że *dla danej liczby użytkowników n, R tworzy i certyfikuje ich pary kluczy* (ang. *for a given number of users n, R creates and certifies their key pairs*); aby wystawiać certyfikaty R musi znać klucz prywatny CA; czy to jest świadome założenie, które nie ma wpływu na dowód twierdzenia 3.2, czy też nieświadomy błąd?

(e) str. 78, 84, 87, 88, 99, 101, 103: błędnie ponumerowane twierdzenia; twierdzenia mają numery od 4.10 do 4.17, powinno być odpowiednio 4.1 – 4.8;

(f) str. 46, rys. 3.1: przy obliczeniach wartości Y'_C i Y'_R użyto $\hat{g}_1$, zaś w formule obliczania wartości jednego z iloczynów dwuliniowych występuje $\hat{g}$;

(g) str. 77, 3 akapit od dołu: jest „This requires that the hardware used for the eID's **and** is leakage-resistant."; słowo „and" jest zbędne;

(h) str. 73-75: Algorytmy *Prove* i *Verify* muszą być wykonywane współbieżnie i synchronizowane w momentach przesyłania/odbioru komunikatów; opis algorytmów przedstawiony na str. 73-75 nie odzwierciedla tego wymagania; w związku z tym lepiej byłoby zastosować klasyczne opisy protokołów z formułowaniem komunikatów i kierunku ich przepływu; tego typu opisy bardzo dobrze odzwierciedlałyby diagram sekwencji przedstawiony na rys. 4.4; podobna uwaga odnosi się do opisu pozostałych protokołów;

(i) str. 76, rys. 4.4: brakuje opisu sposobu przekazywania weryfikatorowi listy *RevInfo* oraz zapewnienia jej autentyczności; wydaje się to oczywiste, ale taki opis zwróciłby uwagę studiującego pracę na rolę wydawcy dokumentu, zwłaszcza w kontekście sygnalizowanego przez Autora braku konieczności obdarzenia go zaufaniem; uwaga ta odnosi się także do rys. 4.5 i 4.7;

(j) str. 82, 5 akapit od góry: wykonując algorytm *Revoke* wydawca nie może obliczać pseudonimu użytkownika wg formuły $dnym = \left(g^{sk_{RI}}\right)^r$; powinno być $dnym = rt^{drt}$;

(k) str. 82, krok 6 algorytmu *Prove*: w formule obliczania epk_C zamiast sk_C należy użyć sk_{RI}; podobne błędy występują na str. 83 w kroku 7, 11 i 12, a także na str. 84, w kroku 10 algorytmu *Verify*;

(l) str. 85, rys. 4.5: w formule obliczania *dnym* zamiast sk_C należy użyć sk_{RI}.

Należy zauważyć, że wskazane usterki formalne nie wpływają w żaden sposób na merytoryczną ocenę pracy jako całości.

6. Konkluzja recenzji

Przedstawione powyżej uwagi merytoryczne i formalne nie umniejszają osiągnięć doktoranta, ani nie podważają zaproponowanych protokołów oraz dowodów ich bezpieczeństwa. Przedstawioną mi do oceny rozprawę oceniam bardzo wysoko, zarówno z uwagi na aktualność i ważność tematyki rozprawy, staranność jej przygotowania, zastosowany warsztat metodyczny, jak również dużą wiedzę Autora i znajomość literatury z zakresu metod projektowania i dowodzenia bezpieczeństwa protokołów kryptograficznych. Autor uzyskał wartościowe i oryginalne z naukowego punktu widzenia wyniki zawarte zwłaszcza w zaproponowanych protokołach ograniczonej identyfikacji oraz modelach i dowodach ich bezpieczeństwa. Uzyskane wyniki były opublikowane przez Autora w materiałach trzech renomowanych konferencji międzynarodowych oraz są przedmiotem dwóch artykułów, z których jeden został już opublikowany w tym roku w czasopiśmie Journal of Universal Computer Science. Dodatkowo pięć artykułów Autora jest indeksowanych w bazie Web of Science, zaś trzynaście w bazie Scopus.

Uważam, że Autor zrealizował cel rozprawy oraz wykazał się umiejętnościami i odpowiednim przygotowaniem do samodzielnej pracy naukowej w dyscyplinie informatyka. Na tej podstawie stwierdzam, że przedstawiona do oceny rozprawa doktorska mgr inż. Lucjana Hanzlika pt. „Cryptographic Protocols for Modern Identification Documents" **spełnia wymagania stawiane rozprawom doktorskim w Ustawie o stopniach naukowych i tytule naukowym z dnia 14 marca 2003 roku** (Dz. U. nr 65/2003, poz. 595) **i wnoszę o dopuszczenie jej Autora do publicznej obrony**.

Jerzy Pejaś

Dokument podpisany przez Jerzy Pejaś
Data: 2015.07.17 00:23:04 CEST
Powód: Recenzja rozprawy doktorskiej mgra inż. Lucjana Hanzlika pt. „Cryptographic Protocols for Modern Identification Documents"