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

Warszawa, 3 marca 2015 r

RECENZJA ROZPRAWY DOKTORSKIE J DLA
RADY NAUKOWEJ INSTYTUTU PODSTAW INFORMATYKI
POLSKIEJ AKADEMII NAUK

Tytuł rozprawy: Algorytmy ochrony informacji dla systemów urządzeń o ograniczonych możliwościach

Autor rozprawy: mgr inż. Piotr Syga, Politechnika Wrocławska

Wstęp

Recenzowana rozprawa doktorska poświęcona jest problematyce bezpieczeństwa urządzeń o ograniczonych możliwościach obliczeniowych. Jest to dziś temat niezwykle aktualny, ponieważ rozpowszechnienie technologii mobilnych oraz wdrożenie koncepcji „Internetu przedmiotów" (IoT – Internet of Things) sprawiło, że bezpieczeństwo takich urządzeń – a zwłaszcza jego brak, zaczyna dotyczyć dużych grup społecznych, a nie jedynie wąskiej grupy dysponentów informacji krytycznych, jak to było w nieodległej przeszłości. Tak więc nie ulega wątpliwości, że rozprawa dotyczy zagadnień ważnych i zdecydowanie wymagających znajdowania nowych rozwiązań.

Praca jest napisana w języku polskim i liczy 153 strony. Podzielona jest na 11 rozdziałów, z których rozdział pierwszy jest wstępem zawierającym wprowadzenie do tematyki i zwięzły opis uzyskanych w rozprawie wyników, a rozdział drugi stanowi wprowadzenie matematyczne do przeprowadzonych badań i zawiera notację oraz podstawowe fakty matematyczne wykorzystane w pracy. Kolejne dwa rozdziały (oznaczone numerami 3 i 4) stanowią przedstawienie urządzeń technicznych, których badania dotyczą, to znaczy RFID oraz bezprzewodowych siec i sensorów oraz problematyki ich bezpieczeństwa. Główne wyniki oryginalne rozprawy zawarte są w

rozdziałach od 5 do 10. W każdym z tych rozdziałów przedstawiono w sposób spójny konkretne protokoły kryptograficzne zapewniające bezpieczeństwo jednej w powyższych technologii w określonym zakresie. Tak więc rozdział 5 to opis protokołu identyfikacji RFID zapewniający zachowanie prywatności użytkowników (nazwanego Kameleon). Rozdział 6 zawiera opis i analizę bezpieczeństwa kilku wersji protokołów zabezpieczających komunikację między tagami RFID i czytnikiem. Rozdział 7 zawiera opis i analizę bezpieczeństwa protokołu komunikacyjnego dla sieci sensorowych o ograniczonych zasobach. W kolejnych trzech rozdziałach autor przedstawił propozycje protokołów gwarantujących poufność operacji wykonywanych w bezprzewodowych sieciach sensorów. Rozdział 8 przedstawia ogólny meta algorytm ukrywający przed adwersarzem dokładny przebieg protokołu w sieci, rozdział 9 poświęcony jest poufnej aproksymacji rozmiaru sieci a rozdział 10 – poufnej inicjalizacji sieci. W rozdziale 11 wyniki uzyskane w rozprawie zostały podsumowane i nakreślono możliwość dalszych badań w zakresie tematyki rozprawy. Poza opisanymi wyżej 11 rozdziałami rozprawa doktorska zawiera obszerne streszczenie w języku angielskim oraz bibliografię liczącą 120 pozycji, wśród nich 5 prac współautorstwa pana magistra inżyniera Piotra Sygi. W pracy umieszczono 39 rysunków (oraz 2 podpisy pod grupami rysunków, także nazwane rysunkami z przypisanymi numerami) i 5 tablic. Rozprawa zawiera też 59 wyróżnionych numerowanych fragmentów tekstu obejmujących definicje, twierdzenia, lematy i fakty, a także 11 algorytmów zapisanych w formie wyróżnionej (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 elementów 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) ?

W recenzowanej rozprawie teza pracy nie została sformułowana w wydzielonej formie. Sformułowano natomiast szereg zadań, których rozwiązanie jest przedmiotem pracy. Celem rozprawy jest konstrukcja nowych protokołów bezpieczeństwa dla

modeli systemów RFID oraz bezprzewodowych sieci sensorów oraz formalne dowody ich bezpieczeństwa. Dla systemów RFID dotyczy to głównie ochrony tożsamości użytkowników, to znaczy propozycji takich protokołów, w których trudna jest identyfikacja konkretnego taga RFID przez nieuprawniony czytnik oraz trudna do ustalenia jest rzeczywista liczba tagów w jego zasięgu odczytu. Dla bezprzewodowych sieci sensorów celem jest zaproponowanie metod ochrony informacji o rzeczywistym przebiegu protokołów związanych z inicjalizacją sieci. Ponieważ to formalna analiza i dowody bezpieczeństwa są głównym celem pracy, można uznać, że ma ona charakter teoretyczny. Zamieszczone w rozprawie wyniki symulacji stanowią uzupełnienie i pewną weryfikację wyników teoretycznych.

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 ?

Informacje literaturowe niezbędne do łatwiejszego zrozumienia pracy zostały przedstawione w trzech rozdziałach. Rozdział drugi rozprawy zawiera podstawowe informacje z zakresu matematyki dotyczące definicji i twierdzeń wykorzystywanych w rozprawie. Ten rozdział został bardzo dobrze skonstruowany, jest zwięzły a zarazem precyzyjnie przedstawia niezbędne fakty wraz z ich odniesieniem do właściwych źródeł literaturowych. Literatura dotycząca dwóch głównych środowisk komunikacyjnych, których bezpieczeństwo jest przedmiotem rozprawy, odnotowana jest w rozdziale trzecim i czwartym rozprawy. Rozdział trzeci zawiera opis działania systemów RFID oraz przedstawienie problematyki ich bezpieczeństwa, rozdział czwarty natomiast dotyczy tych samych aspektów działania bezprzewodowych sieci sensorów. O ile oba te rozdziały przedstawiają właściwie uwarunkowania bezpieczeństwa wynikające z małej wydajności tagów RFID i sensorów, to już przedstawienie zagadnień bezpieczeństwa jest bardzo powierzchowne. Po przedstawieniu wybranego problemu bezpieczeństwa autor wymienia zwykle kilka publikacji z adnotacją, że podobne zagadnienia zostały w nich przedstawione. Trudno to nazwać analizą źródeł. Oto kilka przykładów takich sformułowań:

Str. 26, o zastosowaniach RFID: „Przykłady innych, także potencjalnych, zastosowań

można znaleźć w pracach [16, 46, 85, 119]".

Str. 34, o inicjalizacji WSN: „problem ten był rozważany miedzy innymi w [49, 76]";

o wyborze lidera: „problem ten był rozważany miedzy innymi w [10, 43, 44, 88, 89]";

o estymacji rozmiaru sieci: „Problem ten był rozważany miedzy innymi w [22, 64, 73]".

Str. 35, o zagrożeniach w sieciach sensorów: „Przykładowe rezultaty można znaleźć w pracach [32, 42–44, 68, 69, 91, 95, 98]".

Str. 36, o zabezpieczeniach w WSN: „Ze względu na obszerność badań nad tą kwestią wspominamy jedynie część publikacji [14, 17–19, 29, 51, 84, 103, 112, 118]".

Takie przedstawienie stanu sztuki sprawia, że trudno ocenić jak metody zaproponowane przez doktoranta zwiększają globalne bezpieczeństwo analizowanej sieci, a nie tylko stanowią modyfikację konkretnego rozwiązania czy też ochronę wybranego aspektu bezpieczeństwa.

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

Cele pracy, polegające na analizie bezpieczeństwa i złożoności obliczeniowej zaprojektowanych przez Autora protokołów dla RFID i bezprzewodowych sieci sensorów, w tym także na formalnych dowodach ich bezpieczeństwa, zostały w pełni zrealizowane. W analizie i dowodach wykorzystano metody rachunku prawdopodobieństwa, w tym także teorię łańcuchów Markowa, a więc metody wewnętrznie spójne i często stosowane w podobnych rozważaniach.

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 ?

Recenzowana rozprawa zawiera szereg oryginalnych wyników, potwierdzonych niezależnie publikacjami i referatami na dobrych międzynarodowych konferencjach naukowych. Wyniki te powstawały w ramach pracy w zespole z udziałem promotora rozprawy, co nie tylko nie jest wadą, ale świadczy o umiejętności współpracy i

zazwyczaj sprzyja osiąganiu wartościowych wyników. Oryginalne wyniki uzyskane w rozprawie to szereg lekkich protokołów kryptograficznych służących bezpieczeństwu dwóch klas systemów informacyjnych: identyfikacji za pomocą RFID oraz komunikacji w bezprzewodowych sieciach sensorów. Zaprojektowane protokoły mogą stanowić elementy kompletnych systemów bezpieczeństwa dla, odpowiednio, RFID oraz bezprzewodowych sieci sensorów. Oryginalny i wartościowy element rozprawy to formalne modele protokołów, propozycje zabezpieczeń oraz przeprowadzone dowody bezpieczeństwa i oszacowania złożoności obliczeniowej protokołów. Dodatkowym wartościowym elementem są wyniki symulacji potwierdzające oszacowania teoretyczne.

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

Rozprawa jest napisana w sposób jasny, zwięzły i poprawny. Zawiera odpowiednio sformułowany problem naukowy poprzedzony starannie dobranymi informacjami wprowadzającymi (definicjami i twierdzeniami), precyzyjnie sformułowane teoretyczne wyniki naukowe opatrzone dowodami oraz wyniki symulacji numerycznych i wnioski z badań. Strona redakcyjna rozprawy wymaga drobnych poprawek. W rozprawie są też pewne nieliczne sformułowania, które zdaniem recenzenta mogłyby być inaczej przedstawione. Niżej wymienione są zauważone przez recenzenta usterki redakcyjne lub sformułowania dyskusyjne.

- W rozprawie jako tłumaczenie angielskiego zwrotu „ provable security" użyto sformułowania „dowodliwe bezpieczeństwo". W wielu dotychczasowych publikacjach w języku polskim używany jest termin „udowadnialne bezpieczeństwo".
- W twierdzeniach zamiast zwykle używanego w implikacji sformułowania: „jeżeli... to" jest często „Jeżeli .. wtedy".
- W sformułowaniu Faktu 6 występuje niepełne – urwane zdanie.
- W wielu fragmentach pracy są niepoprawnie rozmieszczone przecinki.
- W pracy w dwóch miejscach zastosowano dziwną numerację rysunków. Dwa

rysunki ograniczają się do samych podpisów wraz ze stosownymi numerami wynikającymi z ich rozmieszczenia w tekście rozprawy. Brak jest rysunku 5.7, podpis o tym numerze występuje jako zbiorczy podpis pod grupą rysunków 5.2-5.6.

- Podobnie brak rysunku 6.8, podpis o tym numerze występuje pod grupą rysunków 6.1-6.7.
- Podpisy z informacjami o zawartości tablic: w dwóch przypadkach umieszczone są pod tablicą, w trzech – nad tablicą.
- Nietypowa dla publikacji naukowych jest numeracja wydzielonych fragmentów tekstu (definicji, twierdzeń, itp.). Jest to jednolita numeracja prowadzona w sposób ciągły, bez rozróżnienia rodzaju numerowanego obiektu.

Jakie są słabe strony rozprawy i jej główne wady?

W pracy brak jest wyczerpującej analizy stanu wiedzy (z właściwie zacytowaną literaturą) dotyczącej problematyki bezpieczeństwa RFID oraz bezpieczeństwa bezprzewodowych sieci sensorów. Ta usterka rozprawy (nie wpływająca na jakość uzyskanych wyników oryginalnych) sprawia, że bez dodatkowych studiów literaturowych trudno jest docenić w pełni wartość uzyskanych wyników i określić, na ile zaprojektowane rozwiązania bezpieczeństwa są kompletne i wystarczające oraz jakia jest ich relacja do wyników uzyskanych przez innych autorów.

Do wad rozprawy zaliczyłbym również opisane wyżej usterki redakcyjne, które jednak w najmniejszym nawet stopniu nie obniżają wartości wyników naukowych uzyskanych w rozprawie i nie utrudniają zrozumienia tekstu.

Jaka jest przydatność rozprawy dla nauk matematycznych?

Oceniana rozprawa ma charakter matematyczny. Zawarte w niej rozumowania ujęte są w formie definicji i stwierdzeń z dowodami (nazwanymi w zależności od ich wagi i roli w wywodzie jako fakt, wniosek, twierdzenie, lemat, itd.). Praca wpisuje się w dwa nurty badań. Pierwszym jest lekka kryptografia, to znaczy kryptografia dla urządzeń o niewielkiej mocy obliczeniowej (i minimalnym akceptowalnym poziomie bezpieczeństwa), drugim jest idea udowadnialnego bezpieczeństwa, co w tym wypadku

oznacza zagwarantowanie realizacji tego minimalnego poziomu bezpieczeństwa. Moim zdaniem takie badania są cenne z teoretycznego punktu widzenia jako podejście systematyczne i ścisłe do problematyki bezpieczeństwa. Są one również przydatne w dzisiejszym świecie, gdy słabe urządzenia dominują liczebnie w praktycznym wykorzystaniu przez przeciętnego użytkownika i to one stanowią źródło największego zagrożenia dla jego prywatności. Wyniki uzyskane w rozprawie mogą być inspiracją dalszych badań dotyczących lekkiego bezpieczeństwa (kryptografii). Za najciekawsze uważam tu wykorzystanie meta algorytmów, które pozwalają uprościć konstrukcje i dowody bezpieczeństwa wielu podobnych do siebie algorytmów/protokołów komunikacyjnych; takich podobnych rozwiązań mamy w teleinformatyce wiele więc i metodyka taka może być bardzo skuteczna.

Podsumowanie i ocena rozprawy

W swojej rozprawie doktorskiej pan magister inżynier Piotr Syga przedstawił specyfikację kilku protokołów bezpieczeństwa dla systemów urządzeń o ograniczonych możliwościach oraz udowodnił, że spełniają one wymogi bezpieczeństwa w określonym zakresie. Tym samym zrealizował zadania przewidziane do wykonania w rozprawie doktorskiej. Wyniki tych prac były przedmiotem publikacji w materiałach czterech ważnych konferencji międzynarodowych i jednego artykułu złożonego do druku w renomowanym czasopiśmie, zostały więc zaprezentowane światowej społeczności naukowej. Równocześnie spełnione są ustawowe warunki przeprowadzenia przewodu doktorskiego.

Reasumując, rozprawę doktorską pana magistra inżyniera Piotra Sygi 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 matematycznych w dyscyplinie naukowej: informatyka i wnioskuję o jej dopuszczenie do publicznej obrony.

Prof. dr hab. inż. Zbigniew Kotulski

Kotulski