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