ФТК-88-НС1-042/
24.01.2017

Становище

за дисертационен труд на тема

"МЕТОДИ И АЛГОРИТМИ ЗА ПОВИШАВАНЕ НА СИГУРНОСТТА И СЪХРАНЕНИЕТО НА ДАННИТЕ ПРИ ПРЕДАВАНЕТО НА ИНФОРМАЦИЯ В ТЕЛЕМЕТРИЧНИ СИСТЕМИ"

за присъждане на образователната и научна степен "доктор" в професионално направление 5.3. "Комуникационна и компютърна техника" по научна специалност "Автоматизирани системи за обработка на информация и управление (в комуникациите)" на **маг. инж. Иван Динков Иванов**

Обща характеристика на дисертационния труд

Дисертационният труд е оформен в увод, четири глави, заключение и изводи, авторски приноси в работата, списък на публикации на автора по темата, библиография и приложение, съдържащо справка за издаден патент, грамота за представяне на постер и доказателствен материал за внедрен алгоритъм за криптиране на данни. Общият обем е 146 страници. Броят фигури в дисертацията е 52, а броят на таблиците е 67. Списъкът на цитираните източници в изследваната научна област съдържа 117 заглавия, собствените публикации по темата са 6, цитиран е един проект с внедрени резултати от дисертационния труд и справка за издаден патент от 2013 г. От публикациите на автора по темата на дисертацията 4 са в съавторство, а две са самостоятелни. Няма публикации в издания с IF или SJR, не са приведени цитирания по тези публикации на автора.

Актуалност на разглеждания проблем.

Телеметричните системи навлязоха масово в ежедневието на хората, индустрията, бизнеса, медицината и др. Тези системи са част от комуникационната техника, която се занимава с изучаване на методите и средствата за автоматизирано събиране на данни от разстояние, постъпващи от дистанционно разположени датчици, сензори, видео-камери, тахометри, и др. Често пъти тези данни се използват за мониторинг и управление на критични инфраструктурни системи, съдържат лични данни и друга информация, достъпът до които обикновено е ограничен до малък кръг оторизирани лица. Защитата на тази информация е от критична важност за правилното функциониране на такива системи. Точно тази тематика е обект на изследване в настоящата дисертация. В последната година няколко хакерски атаки в най-развити и водещи в информационните технологии страни продемонстрираха неподготвеността и уязвимостта на нашето информационно общество към такъв род хулиганство или по-тежък вид престъпление. Гореизложеното еднозначно показва актуалността на разработваната в дисертацията теза.

Съдържание на дисертационната работа.

В първа глава на дисертационния труд е направен обзор на телеметричните системи и е показана необходимостта от защита на предаваните и съхранени данни в телеметричните системи. Определени са основните изисквания, на които трябва да отговарят криптографските алгоритми в телеметричните системи. Определени са целите и задачите на дисертационния труд. Във втора и трета глава е предложен метод и реализиран алгоритъм за криптиране на данни в телеметрични информационни системи и бази данни със специално предназначение и повишена степен на защита - 64-битов, симетричен блоков алгоритъм, използващ 256-битов криптографски ключ, състоящ се от 16 вътрешни цикъла, съдържащи транспозиции, субституции и нелинейни процедури. В четвърта глава са изследване основните параметри на предлижения алгоритъм.

Дисертационната работа се отличава с ясен стил на изложението, съдържанието е подходящо онагледено с голям брой фигури, резултатите са представени изчерпателно в таблици и са добре коментирани. Всичките литературни източници са включени в дисертацията и цитирани коректно

Научни и научно-приложни приноси на дисертационния труд. Преценка на публикациите. Валидация на резултатите

Приносите в дисертационния труд са формулирани прецизно в края на всяка глава. Освен това е включена допълнителен раздел в края на дисертацията, където е дадено обобщение на приносите. В края на всяка глава се цитират и публикациите на автора по съответния материал. Няма глава от дисертацията и авторски претенции, които да не са преминали публична защита на научен форум, специализиран по разглежданата тематика. По дисертационния труд са представени 6 публикации и един патент. От публикациите две са докладвани на научни форуми в чужбина и 4 в България. Независимо от близостта на предложения в дисертацията метод за криптиране на телеметрична информация до подхода на Фейстел и стандартизирания в САЩ алгоритъм за криптиране DES оригиналността на подхода не буди съмнение и доказателство за това е получения патент. Считам, че основните приноси на дисертацията са публично достояние и изискванията на законите и правилниците, касаещи условията за придобиване на научни степени са спазени. Силна положителна страна на работата е използването на получените резултати в проект и реализация на внедряване в Ентърпрайс Комюникайшънс Груп ООД, което дава основание да се смята, че получените резултати са валидирани.

Автореферат

Авторефератът е в обем от 32 стр. и отговаря напълно на съдържанието на дисертационния труд.

Забележки по дисертационната работа

Някои забележки по изложението:

1. Обзорната част за телеметрията е преоразмерена.

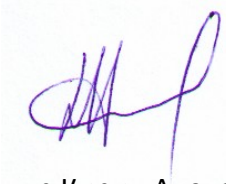
2. Основните цели и задачи на дисертационния труд се появяват едва на 33 стр. Тяхното естествено място е след уводната част, като обзорът в първа глава подпомага параметризирането на разработваната система.

3. Под функционалност на даден алгоритъм обикновено се разбира не доколко той е коректно/вярно реализиран (това е задължително условие), а как алгоритъмът си изпълнява предназначението, т.е. предоставя "добре" криптирани данни на ниска стойност (лекота при хардуерна/софтуерна реализация).

4. Като сериозен пропуск в дисертацията следва да се посочи, че не е отчетено като принос създаването на собствена схема за криптиране, различна от добре изучените и известни явни схеми като DES. При явните методи, при които се обявява публично схемата на работа, това не е преимущество, но при неявните методи за криптиране и тяхното хардуерно реализиране това е сериозно предимство пред потенциалните опити за несанкциониран достъп до данните. Такава реализация дава възможност за внедряване на персонални силно защитени криптиращи системи.

Заключение

Направените забележки ни най-малко не омаловажава научната стойност на представената работа. Дисертационният труд има всички достойнства на научноизследователски труд и представя автора като изграден специалист в областта на защитата на данните в телеметричните системи. Гореизложеното ми дава основание за положителна оценка. На основание на Закона за развитието на академичния състав в Република България и Правилника за негово прилагане, като член на научното жури предлагам почитаемото научно жури да присъди на **маг. инж. Иван Динков Иванов** образователната и научна степен „доктор” по професионално направление 5.3. "Комуникационна и компютърна техника".



24.01.2017 г. Рецензент:

София /Доц. д-р Кирил Алексиев/