МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ
Кафедра математического моделирования и анализ данных

Аннотация к дипломной работе

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ДАННЫХ В IoT СИСТЕМАХ

Шиляев Иван Владимирович

Научный руководитель:
ведущий инженер-программист
ОРТСЗИ ГП «НИИ ТЗИ»
М.А. Казловский

Минск, 2022

Реферат

Дипломная работа: 69 страниц, 4 главы, 13 рисунков, 5 таблиц, 14 использованных источников, 5 приложений.

Ключевые слова: ИНТЕРНЕТ ВЕЩЕЙ, КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ДАННЫХ, АУТЕНТИФИЦИРОВАННОЕ ШИФРОВАНИЕ, КРИПТОГРАФИЧЕСКИЙ ПРОТОКОЛ, SPONGE-ФУНКЦИЯ.

Объект исследования: криптографическая защита данных в протоколах, применяемых в сфере интернета вещей.

Цель работы: изучение сетевых протоколов, применяемых в сфере интернета вещей, изучение и сравнение безопасности этих протоколов, анализ уязвимостей и угроз, разработка прототипа умного устройства и протокола взаимодействия с применением белорусских криптографических стандартов.

Методы исследования: а) теоретические: изучение источников, посвящённых протоколам, применяемым в сфере интернета вещей; изучение характеристик этих протоколов, методов, применяемых для защиты данных; б) практические: составление матрицы, сравнивающей устойчивость выбранных технологий к некоторому общему набору угроз в целях выявления наиболее криптостойкого решения; разработка прототипа умного устройства на собственной прошивке, использующей методы защиты данных, описанные в белорусском криптографическом стандарте.

Результат: сравнение технических характеристик выбранных протоколов; сравнение безопасности выбранных протоколов; описание известных угроз и успешно проведённых атак на различные версии протоколов; построенная матрица угроз; реализация алгоритмов аутентифицированного шифрования и хэширования из белорусского криптографического стандарта СТБ 34.101.77 на языках программирования Java и C++; разработанная прошивка для умного устройства на языке программирования C++ с использованием аутентифицированного шифрования; разработанный прототип умной лампочки, работающий на этой прошивке; разработанное веб-приложение для управляющего устройства на языке программирования Java.

Область применения: сфера информационной безопасности и интернета вещей.

Рэферат

Дыпломная праца: 69 старонак, 4 раздзела, 13 малюнкаў, 5 табліц, 14 выкарыстаных крыніц, 5 дадаткаў.

Ключавыя словы: ІНТЭРНЭТ РЭЧАЎ, КРЫПТАГРАФІЧНАЯ АБАРОНА ДАДЗЕНЫХ, АЎТЭНТЫФІКАВАНАЕ ШЫФРАВАННЕ, КРЫПТАГРАФІЧНЫ ПРАТАКОЛ, SPONGE-ФУНКЦЫЯ.

Аб'ект даследавання: крыптаграфічная абарона дадзеных у пратаколах, якія выкарыстоўваюцца ў сферы інтэрнэту рэчаў.

Мэта працы: вывучэнне сеткавых пратаколаў, якія прымяняюцца ў сферы інтэрнэту рэчаў, вывучэнне і параўнанне бяспекі гэтых пратаколаў, аналіз уразлівасцяў і пагроз, распрацоўка прататыпа разумнай прылады і пратаколу ўзаемадзеяння з ужываннем беларускіх крыптаграфічных стандартаў.

Метады даследавання: а) тэарытычныя: вывучэнне крыніц, прысвечаных пратаколам, якія прымяняюцца ў сферы інтэрнэту рэчаў; вывучэнне характарыстык гэтых пратаколаў, метадаў, якія прымяняюцца для абароны дадзеных; б) практычныя: складанне матрыцы, якая параўноўвае ўстойлівасць абраных тэхналогій да некаторага агульнага набору пагроз у мэтах выяўлення найболей крыптаўстойлівага рашэння; распрацоўка прататыпа разумнай прылады на ўласнай прашыўцы, якая выкарыстоўвае метады абароны дадзеных, апісаныя ў беларускім крыптаграфічным стандарце.

Вынік: параўнанне тэхнічных характарыстык выбраных пратаколаў; параўнанне бяспекі выбраных пратаколаў; апісанне вядомых пагроз і паспяхова праведзеных нападаў на розныя версіі пратаколаў; пабудаваная матрыца пагроз; рэалізацыя алгарытмаў аўтэнтыфікаванага шыфравання і хэшавання з беларускага крыптаграфічнага стандарту СТБ 34.101.77 на мовах праграміравання Java і C++; распрацаваная прашыўка для разумнай прылады на мове праграмавання C++ з выкарыстаннем аўтэнтыфікаванага шыфравання; распрацаваны прататып разумнай лямпачкі, які працуе на гэтай прашыўцы; распрацаванае вэб-прыкладанне для кліентскай прылады на мове праграмавання Java.

Вобласць ужывання: сфера інфармацыйнай бяспекі і інтэрнэта рэчаў.

Abstract

Diploma thesis: 69 pages, 4 chapters, 13 figures, 5 tables, 14 sources, 5 attachments.

Keywords: INTERNET OF THINGS, CRYPTOGRAPHIC DATA PROTECTION, AUTHENTICATED ENCRYPTION, CRYPTOGRAPHIC PROTOCOL, SPONGE-FUNCTION.

Object of study: cryptographic data protection in protocols used in the Internet of Things.

Purpose of work: study of networking protocols used in the Internet of Things, study and comparison of these protocols security, analysis of vulnerabilities and threats, development of a smart device prototype and interaction protocol using Belarusian cryptographic standards.

Research methods: a) theoretical: study of the sources devoted to protocols, used in the Internet of Things; study of these protocols characteristics and data protection methods; b) practical: creation of matrix comparing the robustness of the selected technologies to a common set of threats in order to identify the most crypto-resistant solution; development of a smart device prototype on its own firmware, using data protection methods described in the Belarusian cryptographic standard.

Result: comparison of selected protocols technical characteristics; comparison of selected protocols security; description of known threats and successful attacks on different versions of protocols; constructed threat matrix; implementation of authenticated encryption and hashing algorithms from the Belarusian cryptographic standard СТБ 34.101.77 in Java and C++ programming languages; developed firmware for smart device in C++ programming language using authenticated encryption; developed prototype of smart bulb running on this firmware; developed web application for client device in Java programming language.

Scope: the sector of information security and the Internet of Things.

Введение

Термин «Интернет вещей» («Internet of Things») появился более 20 лет назад, а история развития технологии насчитывает почти два столетия. Среди множества определений термина можно выделить следующее: интернет вещей — это глобальная сеть объектов, подключённых к интернету, которые взаимодействуют между собой и обмениваются данными без вмешательства человека.

Основными компонентами IoT систем являются:

- объекты, или «вещи»;
- данные, которыми они обмениваются;
- инфраструктура, с помощью которой осуществляется взаимодействие.

К последнему пункту можно отнести разнообразные виды соединения и каналы связи, программные средства и протоколы. Инфраструктура и её криптографический аспект представляют собой наибольший практический интерес и составляют предметную область данной работы.

Говоря о практическом применении Интернета вещей, многие отрасли выигрывают при использовании этой технологии. И в каждой из этих отраслей необходимо думать о безопасности и защите данных. В связи с этим возникают задачи актуализации знаний об алгоритмах и протоколах, применяемых в данной сфере, их сравнения и реализации в рамках программного обеспечения, изучения уязвимостей, а также рассмотрения вариантов модификации и улучшения этих протоколов с использованием белорусской криптографии. Эти задачи и легли в основу данной работы. В соответствии с задачами были поставлены следующие цели:

1. Изучить сетевые протоколы, применяемые в сфере IoT, и провести их сравнительный анализ;
2. Разобрать криптографический аспект изученных в соответствии с первой целью сетевых протоколов в контексте используемых в них криптографических протоколов и алгоритмов;
3. Описать уязвимости и угрозы используемых решений, а также составить матрицу угроз, демонстрирующую устойчивость выбранных технологий к некоторому общему набору угроз;
4. Разработать собственный прототип, состоящий из управляющего и умного устройств, а также протокол взаимодействия между этими устройствами с применением белорусских криптографических стандартов.