МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

Кафедра математического моделирования и анализа данных

Аннотация к дипломной работе

ПРОВЕРКА SSLСЕРТИФИКАТА В IOS

Бочков Илья Витальевич

Научный руководитель:
кандидат физ.-мат. наук,
доцент кафедры ММАД
Палуха Владимир Юрьевич

Минск, 2022

РЕФЕРАТ

Дипломная работа: 45 с., 12 рис., 2 источника, 1 прил.

TLS, SSL, АТАКА ПОДМЕНОЙ СЕРТИФИКАТА, IOS.

Объект исследования – протокол TLS.

Предмет исследования – дополнительная защита протокола TLS.

Цель работы: внедрить в протокол TLSзащиту от атаки подменой сертификата.

Методы исследования: аналитическое и программное исследование.

Исследования и разработки: использую опыт, полученный при работе с ATS в iOS, реализовать и предоставить в открытый доступ фреймворк для защиты TLSот атаки подменой сертификата.

Э**лементы научной новизны**: исследование и улучшение безопасности протокола TLS.

Область возможного практического применения: внедрение фреймворка в iOS приложения с целью улучшения безопасности.

Автор работы подтверждает, что приведенный в ней расчетно-аналитический материал правильно и объективно отражает состояние исследуемого процесса, а все заимствованные из литературных и других источников методологические и методические положения и концепции сопровождаются ссылками на их авторов.

_____

(подпись студента)

РЭФЕРАТ

Дыпломнаяпраца: 45 с., 12 мал., 2 крыніцы, 1 дадатак.

TLS, SSL, АТАКА ПАДМЕНАЙ СЕРТЫФІКАТА, IOS.

Аб'ектдаследавання– пратаколTLS.

Прадметдаследавання – дадатковаяабаронапратаколуTLS.

Мэта працы:ўкараніць у пратаколTLSабарону ад нападу падменайсертыфіката.

Метадыдаследавання:аналітычнае і праграмнаедаследаванне.

Даследаванні і распрацоўкі:выкарыстоўваюдосвед, атрыманыпрыпрацы з ATS у iOS, рэалізаваць і падаць у адчынены доступ фрэймворк для абароныTLSад нападу падменайсертыфіката.

Элементы навуковайнавізны:даследаванне і паляпшэннебяспекіпратаколаTLS.

Вобласцьмагчымагапрактычнагапрымянення:ўкараненнефрэймворка ў iOSпрыкладання з мэтайпаляпшэннябяспекі.

Аўтарпрацыпацвярджае, штопрыведзены ў ёйразлікова-аналітычныматэрыялправільна і аб'ектыўнаадлюстроўвае стан доследнагапрацэсу, а ўсезапазычаныя з літаратурных і іншыхкрыніцметадалагічныя і метадычныястановішчы і канцэпцыісуправаджаюццаспасылкамі на іхаўтараў.

_____

(подпісстудэнта)

ABSTRACT

Graduate work: 45 pp., 12 pics, 2 sources, 1 abstracts.

TLS, SSL, CERTIFICATE SUBSTITUTION ATTACK, IOS.

The object of study is the TLS protocol.

The subject of research is the additional protection of the TLS protocol.

Purpose: implement protection against hacking by certificate substitution in the TLSprotocol.

Research methods: analytical and program research.

Research and development: using the experience gained while working with ATS in iOS, implement and make publicly available a framework to protect TLS from a certificate spoof attack.

The elements of scientific novelty: research and improvement of TLS protocol security.

The practical application: implementation of the framework in iOS applications in order to improve security.

The author of the work confirms that the calculation and analytical material presented in it correctly and objectively reflects the state of the process under study, and all methodological concepts borrowed from literary and other sources are accompanied by references to their authors.

_____

(student'ssignature)

Введение

В современном мире задача безопасного соединения клиента (мобильного приложения в моем случае) с сервером стоит как никогда остро. Стандартом безопасности стал протокол HTTPS, при передаче данных по которому выполняется шифрование по протоколу TLS. Он по умолчанию обеспечивает достаточный уровень безопасности для большинства приложений, однако не для всех. Уязвимости позволяют провести ряд атак, что является недопустимым для банковских приложений. В данной работе рассматривается одна из таких атак и способ ее решения. Также был реализован фреймворк для платформы iOS, позволяющий в удобно внедрить защиту в приложения сторонних разработчиков.