БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра технологий программирования

Аннотация к дипломной работе

«Защита от атак по перебору паролей через доказательство вычислительной работы»

Кравцова Виктория Александровна

Научный руководитель – кандидат физ.-мат. наук, заведующий кафедрой
И.А. Бодягин

Минск, 2018

Реферат

Дипломная работа: 25 с., 5 рисунков, 10 источников, 1 приложения.

Ключевые слова – АТАКА ПО ПЕРЕБОРУ ПАРОЛЕЙ, ДОКАЗАТЕЛЬСТВО ВЫЧИСЛИТЕЛЬНОЙ РАБОТЫ, ЗАЩИТА ОТ АТАК, PROOF-OF-WORK, ОТЗЫВ СЕРТИФИКАТА.

Объект исследования – атаки по перебору паролей.

Цель работы – разработать алгоритм защиты от атак по перебору паролей через доказательство вычислительной работы.

За время работы были получены результаты:

– Проведен обзор атак, направленных на обход парольной защиты.

– Предложен алгоритм защиты веб-серверов от атак по перебору паролей, основанный на принципе Proof-of-Work.

– Поставлен эксперимент, отображающий зависимость между сложностью алгоритма и количеством итераций, необходимых для генерации алгоритма заданной сложности.

– Реализовано клиент-серверное приложение, реализующее защиту от атак по перебору паролей через доказательство вычислительной работы.

Результаты дипломной работы будут использованы при составлении государственного стандарта Республики Беларусь СТБ/34.101.78.

Abstract

Degree work: pages 25, 5 images, 10 sources, 1 applications.

Keywords: ATTACK ON PASSWORD INTERRUPTION, EVIDENCE OF COMPUTER WORK, PROTECTION FROM ATTACKS, PROOF-OF-WORK, CERTIFICATE REVIEW.

Object of study – attacks on password interruption.

The purpose of the work is to develop an algorithm for protecting against password-attack attacks through proof of computational work.

During the work the following results were obtained:

- A review of attacks aimed at bypassing password protection was conducted.

- An algorithm for protecting Web-servers from password attack attacks based on the principle of Proof-of-Work is offered.

- An experiment was made that reflects the relationship between the complexity of the algorithm and the number of iterations necessary to generate an algorithm of a given complexity.

- Implemented a client-server application that implements protection against password-based attacks through proof of computational work.

The results of degree work will be used when compiling the state standard of the Republic of Belarus STB / 34.101.78.