Szkoła Główna Gospodarstwa Wiejskiego
w Warszawie
Wydział Zastosowań Informatyki i Matematyki

Mateusz Tracz
172391

Implementacja serwisu umożliwiającego dwuetapową weryfikację użytkownika

Implementation of two factor authentication service
at the Warsaw University of Life Sciences – SGGW

Praca dyplomowa inżynierska
na kierunku Informatyka

Praca wykonana pod kierunkiem
dr. hab. Alexandera Prokopenya, prof. SGGW

Wydział Zastosowań Informatyki i Matematyki

Katedra Zastosowań Informatyki
Zakład Modelowania i Analizy Systemów

Warszawa 2017

Oświadczenie promotora pracy

Oświadczam, że niniejsza praca została przygotowana pod moim kierunkiem i stwierdzam, że spełnia ona warunki do przedstawienia tej pracy w postępowaniu o nadanie tytułu zawodowego.

Data ..... Podpis promotora pracy .....

Oświadczenie autora pracy

Świadom odpowiedzialności prawnej, w tym odpowiedzialności karnej za złożenie fałszywego oświadczenia, oświadczam, że niniejsza praca dyplomowa została napisana przeze mnie samodzielnie i nie zawiera treści uzyskanych w sposób niezgodny z obowiązującymi przepisami prawa, w szczególności z ustawą z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. Nr 90 poz. 631 z późn. zm.)

Oświadczam, że przedstawiona praca nie była wcześniej podstawą żadnej procedury związanej z nadaniem dyplomu lub uzyskaniem tytułu zawodowego.

Oświadczam, że niniejsza wersja pracy jest identyczna z załączoną wersją elektroniczną. Przyjmuję do wiadomości, że praca dyplomowa poddana zostanie procedurze antyplagiatowej.

Data ..... Podpis autora pracy .....

Spis treści

Streszczenie

TODO: POLSKI TYTUŁ
TODO: POLSKIE STRESZCZENIE

Słowa kluczowe – TODO: POLSKIE TAGI implementacja, SGGW, Szkoła Główna Gospodarstwa Wiejskiego

Summary

TODO: ANGIELSKIE TYTUŁ
TODO: ANGIELSKIE STRESZCZENIE

Keywords – TODO: ANGIELSKIE TAGI thesis, implementation, SGGW, Warsaw University of Life Sciences

1 Wstęp

1.1 Cel pracy

1.2 Pojęcie uwierzytelnienia wielopoziomowego

1.3 Korzyści płynące z używania uwierzytelnienia wielopoziomowego

2 Elementy kryptografii

2.1 Kryptografia symetryczna oraz asymetryczna

2.2 Szyfry blokowe

2.3 Szyfry strumieniowe

2.4 Funkcja skrótu

2.5 Kod uwierzytelnienia wiadomości

2.6 MAC bazujący na funkcji skrótu

2.7 Funkcje typu „key stretching”

2.8 Pojęcia entropii

3 Kryptografia w praktyce

3.1 Pojęcia pomocnicze

3.1.1 Kodowanie transportowe

Kodowanie Base64

Kodowanie Base32

3.1.2 Czas uniksowy

3.1.3 Ujednolicony Identyfikator Zasobów

3.2 Hasło jednorazowe

3.3 Interfejs „Windows Data Protection”

4 Ataki na mechanizm OTP

4.1 Atak urodzinowy

4.2 Atak przez powtórzenie

4.3 Atak „Man in the middle”

4.4 Phishing

5 PicnicAuth

5.1 Architektura projektu

5.2 Generowanie OTP po stronie użytkownika

5.3 Przechowywanie sekretu użytkownika

5.4 Przykład użycia projektu

5.5 Planowane ulepszenia

6 Zakończenie

6.1 Podsumowanie i wnioski

6.2 Podziękowania

7 Spis literatury

[1] text1

[2] text2

Wyrażam zgodę na udostępnienie mojej pracy w czytelniach Biblioteki SGGW w tym w Archiwum Prac Dyplomowych SGGW.

. . . . . .

(czytelny podpis autora pracy)