

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

<b>1</b>	<b>Wstęp</b>	<b>9</b>
1.1	Cel pracy . . . . .	9
1.2	Pojęcie uwierzytelnienia wielopoziomowego . . . . .	9
1.3	Korzyści płynące z używania uwierzytelnienia wielopoziomowego . . . . .	9
<b>2</b>	<b>Elementy kryptografii</b>	<b>10</b>
2.1	Kryptografia symetryczna oraz asymetryczna . . . . .	10
2.2	Szyfry blokowe . . . . .	10
2.3	Szyfry strumieniowe . . . . .	10
2.4	Funkcja skrótu . . . . .	10
2.5	Kod uwierzytelnienia wiadomości . . . . .	10
2.6	MAC bazujący na funkcji skrótu . . . . .	10
2.7	Funkcje typu key stretching . . . . .	10
2.8	Pojęcia entropii . . . . .	10
<b>3</b>	<b>Kryptografia w praktyce</b>	<b>11</b>
3.1	Pojęcia pomocnicze . . . . .	11
3.1.1	Kodowanie transportowe . . . . .	11
3.1.2	Czas unixowy . . . . .	12
3.1.3	Ujednolicony identyfikator zasobów . . . . .	12
3.2	Hasło jednorazowe . . . . .	12
3.3	Interfejs Windows Data Protection . . . . .	12
<b>4</b>	<b>Ataki na mechanizm OTP</b>	<b>13</b>
4.1	Atak urodzinowy . . . . .	13
4.2	Atak przez powtórzenie . . . . .	13
4.3	Atak „Man in the middle” . . . . .	13
4.4	Phishing . . . . .	13
<b>5</b>	<b>PicnicAuth</b>	<b>14</b>
5.1	Architektura projektu . . . . .	14
5.2	Generowanie OTP po stronie użytkownika . . . . .	14
5.3	Przechowywanie sekretu użytkownika . . . . .	14
5.4	Przykład użycia projektu . . . . .	14
5.5	Planowane ulepszenia . . . . .	14
<b>6</b>	<b>Zakończenie</b>	<b>15</b>
6.1	Podsumowanie i wnioski . . . . .	15
6.2	Podziękowania . . . . .	15



## **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

Przed przystąpieniem do opisu praktycznych aspektów kryptografii użytych w projekcie, wymagane jest wyjaśnienie pojęć wykorzystywanych w mechanizmie haseł jednorazowych, lecz które nie są bezpośrednio związane z kryptografią.

#### 3.1.1 Kodowanie transportowe

Kodowanie transportowe wykorzystywane jest w przypadku, gdy zachodzi potrzeba transferu danych w środowiskach, które pozwalają na przesyłanie wyłącznie znaków ASCII.

Użycie kodowania transportowego jest konieczne w celu zachowania kompatybilności przy pracy z protokołami, które przystosowane są do pracy na danych 7-bitowych. W takim przypadku najstarszy bit jest zerowany, co mogłoby uszkodzić przesyłane dane. W przypadku przesyłania wyłącznie znaków ASCII zerowanie najstarszego bitu nie jest problemem, gdyż wszystkie znaki w podstawowej tablicy ASCII mają ten bit wyzerowany.

Bardziej współczesnym przykładem wykorzystania kodowania transportowego jest osadzanie danych graficznych bezpośrednio w kodzie HTML. Konieczne jest wówczas zakodowanie danych w celu wyeliminowania ryzyka pojawienia się znaków '<' oraz '>', które mogłyby być zinterpretowane jako tagi HTML.

Aby ujednolicić implementacje kodowania transportowego został stworzony dokument RFC 4648 [2], w którym opisany jest prawidłowy sposób implementacji oraz to jaki typ kodowania wybrać w zależności od nałożonych wymagań.

#### Kodowanie Base64

Najczęściej spotykanym typem kodowania transportowego jest kodowanie Base64. Kodowanie to konwertuje dowolny ciąg bajtów do postaci ciągu złożonego z małych i wielkich liter, cyfr oraz znaków '+' i '/'. Jeżeli po zakodowaniu końcowa część danych jest mniejsza niż 24 używany jest także znak '=' jako dopełnienie.

Sam proces kodowania polega na pobraniu 24 bitów danych a następnie podzieleniu ich na 4 grupy po 6 bitów. Każda z grup jest interpretowana jako indeks tablicy ustalonego alfabetu Base64. Dla każdej z grup za pomocą indeksu odczytywany jest znak a następnie dopisywany jest on do ciągu zakodowanego.

Istnieje również odmiana kodowania Base64

## Kodowanie Base32

### 3.1.2 Czas uniksowy

Czas uniksowy jest sposobem na reprezentację punktu w czasie, polegającym na mierzeniu sekund, które upłynęły od daty 1 stycznia 1970 (UTC). W systemach uniksowych zwykle reprezentowany jest w postaci 32-bitowej liczby całkowitej ze znakiem.

W przypadku architektur typu serwer-klient wskazane jest synchronizowanie czasu wykorzystując czas uniksowy, gdyż nie zależy on od lokalizacji w której jest mierzony. Właściwość ta eliminuje problem synchronizacji czasu pomiędzy strefami czasowymi.

### 3.1.3 Ujednolicony identyfikator zasobów

Ujednolicony identyfikator zasobów (ang. Uniform Resource Identifier, URI) jest ciągiem znaków jednoznacznie identyfikującym dany zasób.

Składnia identyfikatora jest wyrażana następująco:

schemat ":" ścieżka ["?" zapytanie] ["#" fragment]

Warto zauważyć, że składnia ta determinuje schemat (protokół), jaki wykorzystywany jest przy interakcji z identyfikowanym zasobem.

Przykłady identyfikatorów:

- ftp://randomftp.com/files/file.docx
- https://www.randomwebsite.pl/index.html
- mailto:jan.nowak@wp.pl
- tel:+48-25-123-88

Szczegóły dotyczące standardu URI są opisane w dokumencie RFC 3986 [1].

## 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 literary

- [1] T. Berners-Lee, R. Fielding, L. Masinter. *Uniform Resource Identifier (URI): Generic Syntax*.  
<https://tools.ietf.org/pdf/rfc3986.pdf>, 2005
- [2] S. Josefsson *The Base16, Base32, and Base64 Data Encodings*  
<https://tools.ietf.org/pdf/rfc4648>, SJD, 2006



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

.....  
(czytelny podpis autora pracy)