**Czech University of Life Sciences Prague**

**Faculty of Economics and Management**

**Department of information Engineering**


Teze for Bachelor Thesis

# Authentication using one-time passwords

**Autor:** Timashev Roman
**Supervisor:** Ing. Josef Pavlicek, Ph.D

In this Bachelor thesis are explained the basic principles and improvements of one-time password authentication. I chose this topic because of its frequency of use in our days. Lots of different companies and banks successfully apply this technology to protect their clients from various attacks. Although the topic of passwords is not new to us, but most of the large companies such as Google or Facebook use authentication with one-time passwords, because they see a future in this system.

The main goals are:

1) To show the basic principles of work one-time passwords.
2) To find the safest method of delivering OTP to the user;
3) To find the best method of generating the OTP;
4) Try to find the possible causes of of hacking one-time passwords and try to improve this solution according to user requirements and convenience;
5) To design and implement this solution.

Partial goals of this work are:

1) To analyze the general types of authentication;
2) To show the advantages and disadvantages of OTP system;
3) To show methods of delivering, generating of one-time passwords.

In the theoretical part of thesis, we will describe the different types of authentication, methods of delivering OTPs, reasons of using these passwords and their types. In addition, we will consider the strengths and weaknesses of using OTP. We will describe the different methods of generating numbers for passwords using some different types of algorithms, the different type of tokens, which one is better for our solutions. In the end of this part, we will try to find the best algorithm of this system; the best delivering and generating methods of one-time passwords for web application. According to this knowledge, we will try to apply it in practice.

In the practical part of the work explains the principle of using OTP for web applcation using MultiOTP utility with PHP library. We will use different types software tokens on the Android system. In addition, I will try to improve the protection of using hardware tokens for internet banking to provide secure transaction.

Based on theoretical knowledge and the results of my solution, the conclusions of the thesis will be formulated.

There are many types of biometric data to protect the information. Each of them has its own security level. There are 2 types of biometric data: psychological and behavioral.

Fingerprint is unique for each person and its hard to forge. To authenticate the user does not need anything extra, except the user's finger, which is very convenient.

Voice is also unique for each user, easier to implement and is a cheaper option than fingerprint scanner.

According to certain conclusions from theoretical part, we can create the ideal degree of protection in using of internet banking.

Suppose we have some bank account, which use OTP sytem, we have hardware token that generates a password every 30-60 seconds using a built-in clock, login and our PIN. We enter your login, PIN and our token generates password for us, and we go into the system and can provide some transactions and make manipulation with our account, but your data can be stolen or you can lose your account.

To improve the system - we have to improve the way of protection. Changing of login and PIN does not make sense, because they can be changed only into the system.

We can improve our hardware token using biometric data of the person. We can integrate things like fingerprint scanners or second varinat – microphone (speech recognizer). As you know these two things are unique in each person.

The token does not turn up until the finger touches the scanner and starts comparing of public and private keys. If both key are the same, the display is switched on and the token generates a password that is only valid for 30 or 60 seconds, after that the screen automatically turns off again .To generate a password the user must touch the scanner again and the process repeats. All unsuccessful attempts will be stored on the server.

Another way of integration is the voice recognition via a microphone. The user needs to turn on the microphone using the switcher, then the user needs to say passphrase, which is stored on a server on the same principle compare two keys and the display turns on and generates a password.

The user enters their biometric data and waits for a response from the server. If his public key is the same as the key stored on the server (the private key, which user has to create, when he is creating own bank account), the token screen turns on and asks the server to generate the password. After this, server creates a password using the algorithm based on the time, token shows the password and after 30 or 60 seconds off, after that the process starts again.

One-time passwords are a good solution for authentication with public computers, on which can be installed a program to steal passwords. Authentication using sms messages is very popular among many companies and banks. This is because the mobile phone has almost everyone. Does not require additional resources and costs. However, this type protection is not ideal; in the mobile phone can be mounted virus. For example Viber or Facebook application automatically opens images from receiver, which can contain malware to steal accounts. Hardware tokens are very good solutions for online banking, however, they can be stolen. A decision, which I cited in the practical part, I think the ideal and very convenient for the protection of any information. I think in the near future, we will completely get rid of hackers attack using our own biometric data.

## List of books


ROEBUCK, Kevin. *OpenID: High-impact Strategies: What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors*. Queensland, Australia: Emereo Publishing, 2012. ISBN 9781743333037.

CHAKI, Nabendu, Natarajan MEGHANATHAN a Dhinaharan NAGAMALAI. *Computer Networks & Communications (NetCom): Proceedings of the Fourth International Conference on Networks & Communications*. New York: Springer Science & Business Media, 2013. ISBN 1461461545.

SLONE, John P. *Local area network handbook*. 6th ed. Boca Raton, Fla.: Auerbach, c2000, xiii, 676 p. ISBN 08-493-9838-X.

TODOROV, Dobromir. *Mechanics of User Identification and Authentication: Fundamentals of Identity Management*. Boca Raton, Florida: Auerbach, 2007. ISBN 9781420052206.

MAJOR, Peter. One-Time Passwords – HOTP and TOTP. In: *ForgeRock Community Blogs* [online]. 2014 [cit. 2015-02-16]. Dostupné z: http://blogs.forgerock.org/petermajor/2014/02/one-time-passwords-hotp-and-totp/