SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA
FACULTY OF ELECTRICAL ENGINEERING AND INFORMATION TECHNOLOGY

Registration number: FEI-5382-5982

SECURE IMPLEMENTATION OF MCELICE CRYPTOSYSTEM

DIPLOMA THESIS

2015 **Martin Orem**

SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA
FACULTY OF ELECTRICAL ENGINEERING AND INFORMATION TECHNOLOGY

Registration number: FEI-5382-5982

SECURE IMPLEMENTATION OF MCELICE CRYPTOSYSTEM

DIPLOMA THESIS

Study Programme:	Applied Informatics
Field Number:	2511
Study Field:	9.2.9 Applied Informatics
Training Workplace:	Institute of Computer Science and Mathematics
Supervisor:	doc. Ing. Pavol Zajac, PhD.
Consultant:	Ing. František Uhrecký

Bratislava 2015 **Martin Orem**

Slovenská technická univerzita v Bratislave
Ústav informatiky a matematiky

Fakulta elektrotechniky a informatiky
Akademický rok: 2012/2013
Evidenčné číslo: FEI-5382-5982

STU FEI

ZADANIE BAKALÁRSKEJ PRÁCE

Študent: **Michal Ližičiar**
ID študenta: 5982
Študijný program: Aplikovaná informatika
Študijný odbor: 9.2.9 aplikovaná informatika
Vedúci práce: Ing. Matúš Jókay, PhD.

Názov práce: **Anonymizácia internetového prístupu**

Špecifikácia zadania:

Cieľom práce je vytvoriť zásuvný modul pre internetový prehliadač, ktorý bude schopný buď náhodne alebo selektívne meniť informácie používané na identifikáciu používateľa pri jeho prístupe na cieľový server.

Úlohy:
1. Analyzujte dostupnosť a funkčnosť podobných modulov.
2. Analyzujte informácie používané na identifikáciu používateľa pri prístupe na stránku.
3. Navrhnite, implementujte a otestujte anonymizačný modul pre zvolený internetový prehliadač.

Zoznam odbornej literatúry:

1. YARDLEY, G. Better Privacy. [online]. 2012. URL: http://nc.ddns.us/BetterPrivacy/BetterPrivacy.htm.
2. ECKERSLEY, P. A Primer on Information Theory and Privacy. [online]. 2010. URL: https://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy.

Riešenie zadania práce od: 24. 09. 2012
Dátum odovzdania práce: 24. 05. 2013

L.S.

Michal Ližičiar
študent

prof. RNDr. Otokar Grošek, PhD.
vedúci pracoviska

prof. RNDr. Gabriel Juhás, PhD.
garant študijného programu

SÚHRN

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Študijný program:	Aplikovaná informatika
Autor:	Martin Orem
Diplomová práca:	Bezpečná implementácia McEliece kryptosystému
Vedúci záverečnej práce:	doc. Ing. Pavol Zajac, PhD.
Konzultant:	Ing. František Uhrecký
Miesto a rok predloženia práce:	Bratislava 2015

Práca sa zaoberá vytvorením zásuvného modulu pre internetový prehliadač, ktorý modifikuje informácie používané na identifikáciu používateľa pri prístupe na server. V prvej časti práce sa nachádza prehľad metód, ktoré zvyšujú anonymitu pri prehliadaní webových stránok. Práca tiež obsahuje zoznam dnes najpoužívanejších rozšírení, ktorých úlohou je zmena niektorých identifikačných prvkov prehliadača alebo anonymizácia pomocou špeciálnych techník. V ďalšej časti sa nachádza prehľad charakteristík prehliadača. Kombináciou týchto charakteristík sa dá s vysokou mierou úspešnosti identifikovať používateľ, ktorý danú stránku navštívil. Posledná časť práce obsahuje návrh, implementáciu a testovanie rozšírenia vytvoreného pre internetový prehliadač Mozilla Firefox. Popisuje zdrojový kód rozšírenia, súvislosť medzi charakteristikami prehliadača, zistené obmedzenia a postup riešenia. Výsledné rozšírenie zvyšuje anonymitu používateľa modifikáciou niektorých charakteristických prvkov prehliadača alebo blokovaním odosielania prvkov, ktoré nie je možné v rámci rozšírenia zmeniť. Na rozdiel od dnes najpoužívanejších modulov dokáže rozšírenie okrem modifikácie HTTP hlavičky, meniť aj charakteristiky zisťované pomocou JavaScript príkazov.

Kľúčové slová: anonymizácia, identifikácia používateľa, zásuvný modul, Mozilla Firefox, internet

ABSTRACT

SLOVAK UNIVERSITY OF TECHNOLOGY IN BRATISLAVA
FACULTY OF ELECTRICAL ENGINEERING AND INFORMATION TECHNOLOGY

Study Programme:	Applied Informatics
Author:	Martin Orem
Diploma Thesis:	Secure implementation of Mcelice Cryptosystem
Supervisor:	doc. Ing. Pavol Zajac, PhD.
Consultant:	Ing. František Uhrecký
Place and year of submission:	Bratislava 2015

The bachelor thesis is about creating of a plugin for web browser, that modifies information used to identification of user during accessing a server. There is an overview of methods that increase anonymity during browsing websites, in the first part. The thesis also contains a list of the most used extensions nowadays, that function is a change of some identification components of browser or special ways of anonymization. In the next part of the thesis is an overview of the characteristics of web browser. By combination of these characteristics we can with high level of success identify a user, who have visited the web site. The last part of thesis contains project, implementation and testing of extension created for the web browser Mozilla Firefox. There is also description of source code of extension, the link between the characteristics of web browser, detected limitations and way how to solve them. The resulting extension increases anonymity of user by modification of some characteristic components of web browser or by blocking sending components, that can not be in extension changed. In comparison with most used modules nowadays, this module can modify HTTP headers including characteristics detected by JavaScript commands.

Keywords: anonymization, identification of user, plugin, Mozilla Firefox, internet

Declaration

I declare that I developed this diploma thesis myself with listed references.

Acknowledgments

I would like to express my deepest gratitude to my supervisor, doc. Ing. Pavol Zajac PhD., for his support and guidance.

Contents

List of Figures and Tables

List of Abbreviations and Symbols

WWW - World Wide Web

List of Algorithm

Introduction

In today's world, cryptography has found its place in many areas of ordinary living and it is important to understand its limits. We have learnt the meaning of the word privacy, especially on the internet. We distribute private information on web sites, we save confidential information on our computers, we pay through internet banking believing and expecting that all of this is adequately defended. As time goes by have to realised that existence of a quantum computer is not any more just a dream. Existence of quantum computer may be a breakthrough in current cryptography, regarding its enormous power. We are facing a hard question. What would be in post-quantum world enough secure? ....Tu popisem kapitoly snad

1 Preliminaries

The security of many cryptosystems relies on three hard problems: the integer factorization problem, the discrete logarithm problem or the elliptic curve discrete logarithm problem. However, these problems can be efficiently solved by a quantum computer using Shor's algorithm. [Postquantum crypto, D.J. Bernstein] Post-quantum cryptography refers to cryptographic algorithms that are meant to be secure against an attack by the quantum computer. Nowadays many cryptographers are designing and reviewing algorithms, striving for the best candidate for post-quantum world. One of the most reviewed candidate is McElice cryprosystem, which is described more in detail in the following section.

1.1 McElice cryptosystem

McElice cryptosystem was proposed by R. J.McEliece in 1978. [**?**] The cryptosystem belongs to a public key cryptography family of protocols, it basically means that two different keys are used for encryption and decryption. The most common public-key scheme used today is RSA. Security of RSA has been reviewed more in detail than any other public-key scheme, so that's why may be considered to be more secure. Due to fact that RSA uses shorter keys, we can find just rare implementations of McElice PKC in practice. However, McElice PKC provides much more faster encryption and decryption process of messages. [referencia] The original construction of McElice cryptosystem is based on Goppa codes, which seems to be resistant against cryptoanalysis with the right choice of parameters. Goppa codes are well suited for cryptographic application due to its generator matrix, which is hardly to be distinguished from a random binary matrix and also for their high error-correcting capabilities. Many other variants of the cryptosystem using various linear codes have been proposed over the years, but the most of them were subsequently proven to be insecure by researchers. [referencia] McElice cryptosystem is considered to be one of the best candidate for post-quantum cryptography, which causes a growing interest in implementation and cryptoanalysis. Security of McElice cryptosystem relies on a decoding problem, which is known to be NP-hard. [referencia] The most important part of secret key is without any doubts the description of the structured linear code, created by an irreducible polynom in key generation process. An efficient decoding algorithm for the chosen linear-code is required for successful decryption of messages. It is clear that the knowing the structure of the underlying linear code provides a way for fast decryption. McElice cryptosystem also takes an advantage from randomness. A public key is !"permuted" and "varied" form of chosen-linear code (secret key), which should be

hardly distinguished from a completely random linear code. Now we can formally define McElice cryptosystem.

1.1.1 Key generation

Generovanie kľúčového páru Alg. 1 shows a process of generation of key pair. In order to generate key pair, we have to define Goppa code, which is created over irreducible polynom. Pre nájdenie daného polynómu môžeme použiť algoritmus z [**?**]. Algoritmus testuje ireducibilnosť náhodne zvoleného polynómu daného stupňa. Pre zostrojenie kontrolnej matice kódu je použitý algoritmus uvádzaný v [**?**]. Pomocou Gaussovej eliminačnej metódy [**?**] upravíme kontrolnú maticu na systematický tvar a následne je možné vytvoriť generujúcu maticu. Výstupom algoritmu je dvojica: privátny a verejný kľúč. Private key - S, G, P (random singular matrix, generation matrix, permutation matrix). Public key - $\widehat{G}, t$ (masked generation matrix and number of error, which is capable to correct).

Algorithm 1 Key generation

1. Pick a random irreducible polynom g over $GF(2^m)$ of degree t,
2. Compute a $k \times n$ generation matrix G, of goppa code $\Gamma = (\alpha_1, ..., \alpha_n, g)$, with dimension $k = n - td$,
3. Generate a random $k \times k$ singular matrix S,
4. Generate a random $n \times n$ permutation matrix P,
5. Compute a $k \times n$ matrix $\widehat{G} = SGP$,
6. Public key is pair of $(\widehat{G}, t)$, where t is maximum of corrected errors, private key is consisted of S, G, P.

1.2 Anonymná sieť

Anonymná sieť je sieť serverov, medzi ktorými dáta prechádzajú šifrované. V anonymných sieťach dáta prechádzajú z počítača používateľa, odkiaľ bola požiadavka poslaná, cez viaceré proxy smerovače, z ktorých každý správu doplní o smerovanie a zašifruje vlastným kľúčom. Cesta od ...

1.3 Funkcionalita

Rozšírenie tiež okrem splnenia špecifikácie malo pre prehľadnosť a overenie funkčnosti zobrazovať údaje, ktoré boli na server odoslané. Zoznam údajov odoslaných na server,

	Funkcia													
						Modifikácia								
Modul	zobrazenie hlavičky	blokovanie skriptov	zmena IP	zmena lokalizácie	zmazanie/blokovanie cookies	blokovanie trackerov	popis	používateľský agent	kódové označenie prehliadača	názov prehliadača	verzia prehliadača	platforma	výrobca prehliadača	označenie výrobcu prehliadača
User agent switcher							X	X	X	X	X	X	X	X
Ghostery					X	X								
Better privacy					X									
Anonymox			X	X	X		X	X						
Modify headers					X			X						
Request policy						X								
Live HTTP headers	X													
User agent awitcher for chrome							X	X						
Header hacker							X	X	X	X	X	X	X	X
Mod header							X	X	X	X	X	X	X	X
Script no		X												
No script		X												
Proxify it			X	X										
I'm not here				X										
Get anonymous personal edition		X	X	X	X	X								
Anonymous browsing toolbar			X	X										
Easy hide your IP and surf anonymously			X	X				X	X	X	X			

Table 1: Moduly a ich funkcie pri anonymizácii

sa mal ukladať do krátkodobej histórie, aby nemal používateľ k dispozícií len najnovšie údaje, ale aj údaje odoslané v nejakom časovom období.

1.3.1 Funkcionalita2

Samozrejmosťou bolo nastavenie zapnutia rozšírenia pri štarte, prípadne interval zmeny odosielaných údajov.

1.4 Vzhľad

Dôležitou požiadavkou kladenou na rozšírenie bolo príjemné používateľské rozhranie. Z tohto dôvodu malo rozšírenie obsahovať zoznam modifikovaných vlastností a tlačidlo pre prístup k nastaveniam rozšírenia v jednoduchej a praktickej forme. Predpokladaný vzhľad je zobrazený na obrázku č. 1. Dôležitou požiadavkou kladenou na rozšírenie bolo príjemné

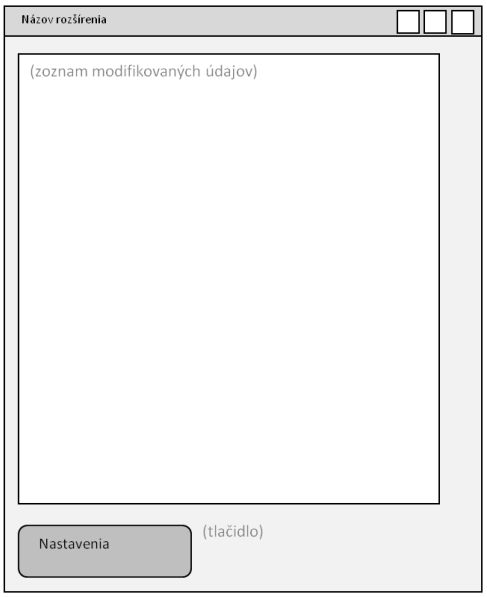

Figure 1: Predpokladaný vzhľad rozšírenia.

používateľské rozhranie.[?] Z tohto dôvodu malo rozšírenie obsahovať zoznam modifikovaných vlastností a tlačidlo pre prístup k nastaveniam rozšírenia v jednoduchej a praktickej forme. Predpokladaný vzhľad je zobrazený na obrázku č. 1.

Algorithm 2 Ukážka algoritmu

```
1  /* Hello World program */
2
3  #include<stdio.h>
4
5  struct cpu_info {
6      long unsigned utime, ntime, stime, itime;
7      long unsigned iowtime, irqtime, sirqtime;
8  };
9
10 main()
11 {
12     printf("Hello World");
13 }
```

Conclusion

Cieľom práce bola analýza anonymizačných modulov, identifikačných prvkov prehliadača a vytvorenie anonymizačného modulu pre internetový prehliadač.

Analýzou najpoužívanejších modulov a vlastností prehliadača, ktoré slúžia na identifikáciu používateľa, sme zistili aktuálny stav a funkcionalitu rozšírení, ktorými je možné anonymizovať prístup na internet. Väčšina týchto rozšírení modifikuje len časť vlastností prehliadača, ktoré sú odosielané na server, alebo úplne blokuje ich odosielanie. Nami vytvorené rozšírenie dokáže modifikovať väčšinu identifikačných prvkov rozšírenia, pričom dodržiava súvislosti medzi vlastnosťami (používateľský agent odosielaný v hlavičke dopytu je totožný s používateľským agentom zisťovaním pomocou JavaScript príkazu, súvislosť medzi šírkou a dĺžkou rozšírenia obrazovky). Dokáže blokovať údaje, ktoré sú posielané v otvorenej podobe na server a obsahujú informácie o identifikačných údajoch prehliadača, ktoré sa nedajú na úrovni rozšírení modifikovať.

Testovanie rozšírenia nám overilo funkčnosť a správnosť implementácie. Rozšírenie dokáže buď vždy, alebo v časových intervaloch modifikovať väčšinu charakteristických prvkov prehliadača odsielaných na server, a tým zvyšuje anonymitu používateľa.

Resumé

Ciel'om práce bolo zmapovat' súčasný stav v oblasti...

Appendix

A Structure of attached medium

\
\Bakalarska_praca.pdf
\FEIk_Identuty.xpi
\FEIkIdentity
\FEIkIdentity\chrome.manifest
\FEIkIdentity\install.rdf
\FEIkIdemtity\content
\FEIkIdemtity\content \function.js
\FEIkIdemtity\content \options.xul
\FEIkIdemtity\content \overlay.xul
\FEIkIdemtity\content \window.js
\FEIkIdemtity\content \window.xul
\FEIkIdemtity\defaults
\FEIkIdemtity\defaults\preferences
\FEIkIdemtity\defaults\preferences \prefs.js
\FEIkIdemtity\locale
\FEIkIdemtity\locale \sk-SK
\FEIkIdemtity\locale \sk-SK\options.dtd
\FEIkIdemtity\locale \sk-SK\window.dtd
\FEIkIdemtity\skin

B Algoritmus

Algorithm B.1 Ukážka algoritmu

```
1  /* Hello World program */
2
3  #include<stdio.h>
4
5  struct cpu_info {
6      long unsigned utime, ntime, stime, itime;
7      long unsigned iowtime, irqtime, sirqtime;
8  };
9
10 main()
11 {
12     printf("Hello World");
13 }
```