Universitatea Tehnică a Moldovei

Elaborarea unei aplicații de cifrare automată a documentelor

Developing an application for automatic file encryption

Student: **Creciun Nicu**

Conducător: **Catanoi Maxim**
lector universitar

Chișinău, 2020

MINISTERUL EDUCAȚIEI, CULTURII ȘI CERCETĂRII AL REPUBLICII MOLDOVA

Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică și Microelectronică

Departamentul Ingineria Software și Automatică

Admis la susținere:

Șef departament:

Fiodorov Ion, dr. conf. univ.

_____

“__” _____ 2020

Elaborarea unei aplicații de cifrare automată a documentelor

Teză de master

Student: **Creciun Nicu**

gr. SI-191M

Conducător: **Catanoi Maxim**

lector universitar

Chișinău, 2020

Adnotare

la teza de master cu tema
„**Elaborarea unei aplicații de cifrare automată a documentelor**„

a studentului gr. SI-191M, programul "Securitate Informațională",
Creciun Nicu

Teza de master este constituită din introducere, trei capitole, concluzii generale și recomandări, referințe bibliografice cu 19 titluri, 65 pagini de text de bază și 57 figuri.

Primul capitol constă din analiza domeniului de studiu, unde este descris scopul și obiectivele lucrării. Capitolul doi conține tehnologiile folosite pentru crearea scriptului de cifrare a informației și metodele de alipire a scriptului creat de document. Capitolul trei oferă o descriere detaliată a metodelor de cifrare automatăa documentelor. Se finisează teza de master cu concluzie asupra proiectului de teză efectuat.

Cuvinte cheie: cifrare automată, metode și sisteme de cifrare, scripturi, planificatorul de activități, aplicații de tip joiner.

Scopul tezei de cifrare automată a documentelor este de a sigura confidențialitatea, disponibilitatea și integritatea informatiei prezente în document.

Obiectivele generale ale lucrării sunt:

- analiza domeniului de cifrare a informației;
- analiza metodelor și sistemelor de cifrare a informației;
- alegerea metodei de creare a scriptului;
- elaborarea și alipirea scriptului de document;
- cifrarea automată a documentelor în caz de compromitere;
- formularea concluziei succinte cu privire la subiectul abordat.

Metodele aplicate: întotdeauna informaţia a însemnat putere, prin urmare dorinţa de a o proteja s-a pus din cele mai vechi timpuri. Din această cauză a fost propusă ideia de a cifra automat informația prezentă în documente. În baza studierii metodelor și sistemelor de cifrare a informației și a soluțiilor de cifrare automată a fost realizate două metode: folosirea task scheduler și aplicația de tip joiner. Pentru folosirea acestor metode este nevoie de scriptul powershell care va efectua cifrarea automată. În rezultat obținem că în caz de compromitere a informației documentul este cifrat.

Annotation

to the master's thesis with the topic

„ **Developing an application for automatic file encryption**„

master student gr. SI-191M, program “Information Security”,

Creciun Nicu

The master's thesis consists of an introduction, three chapters, general conclusions and recommendations, bibliographic references with 19 titles, 65 pages of basic text and 57 figures.

The first chapter consists of the analysis of the field of study, where the purpose and objectives of the paper are described. Chapter two contains the technologies used to create the information encryption script and the methods for join script to document. Chapter three provides a detailed description of the methods for automatically encrypting documents. The master's thesis is completed with a conclusion on the thesis project carried out.

Keywords: automatic encryption, encryption methods and systems, scripts, task scheduler, joiner applications.

The **purpose** of the automatic document encryption thesis is to ensure the confidentiality, availability and integrity of the information present in the document.

The general **objectives** are:

- analysis of the field of information encryption;
- analysis of information encryption methods and systems;
- choosing the method of creating the script;
- elaboration and attachment script to document;
- automatic encryption of documents in case of compromise;
- formulating the brief conclusion regarding the approached subject.

Applied methods: Information has always meant power, so the desire to protect it has been around since ancient times. For this reason, the idea of automatically encrypting the information present in the documents was proposed. Based on the study of information encryption methods and systems and automatic encryption solutions, two methods were developed: using task scheduler and joiner application. To use these methods is needed the powershell script which will perform automatic encryption. As a result we obtain that in case of compromise of the information the document is encrypted.

Cuprins

Introducere

Întotdeauna informaţia a însemnat putere, prin urmare dorinţa de a o proteja s-a pus din cele mai vechi timpuri. Primele texte cifrate descoperite până în prezent datează de circa 4000 de ani şi provin din Egiptul antic, dar existenţa acestora datează fără doar şi poate de la apariţia scrierii în toate civilizaţiile umane.

Cifrarea este procesul matematic de conversie a unui mesaj într-un formular care nu poate fi citit pentru toată lumea, cu excepția persoanei sau dispozitivului care are cheia de a „decripta” mesajul înapoi în formă lizibilă. Există multe metode de cifrare / decifrare, dar secretul datelor nu se bazează pe un algoritm secret, ci pe faptul că cheia de cifrare (parola) este cunoscută doar de persoanele de încredere.

Pentru că cifrarea să fie cu adevărat utilă, trebuie de gîndit la sistem, astfel încât utilizatorii să poată lucra cu acesta. Dacă angajații înțeleg cum să folosească toate acestea, iar cifrarea este transparentă și fără dificultăți tehnice, atunci protecția criptografică a informațiilor va funcționa cu adevărat.

Cifrarea este cea mai bună tehnologie disponibilă pentru a proteja datele de intruși, furnizori de servicii. În acest moment, a atins un astfel de nivel de dezvoltare încât, dacă este utilizat corect, este aproape imposibil spart. Deci cu toții producem, punem o mulțime de informații private pe internet în fiecare zi și trebuie să le asigurăm securitatea. Nu este nevoie să ne fie frică să nu utilizăm nici un serviciu pe internet, trebuie doar să luăm câțiva pași pentru a ne proteja.

Scopul cifrării automate a documentelor este de a sigura confidențialitatea, disponibilitatea și integritatea informatiei prezente în document. Confidenţialitatea, uneori numită secretizare, işi propune să interzică accesul neautorizat al persoanelor la informaţia care nu le este destinată. Ea reprezintă nivelul suprem al securităţii informaționale. Disponibilitatea garantează că utilizatorii autorizaţi au acces la informaţii şi la infrastructura asociată în momentul potrivit. Integritatea datelor este un proces care asigură că datele sunt corecte și coerente pe durata ciclului de viață.

Cifrarea automată semnifică un nivel mai înalt decît cifrarea obișnuită a documentelor fiindcă nu necesită mult timp și acțiuni din partea utilizatorului. Pentru realizarea acestui proiect se vac crea un script pentru cifrarea informației. Următorul pas va fi crearea sau folosirea unei aplicații de tip “joiner” care va alipi script-ul de document. După finisarea alipirii în caz de compromitere, documentul se va cripta automat.

Concluzii

Securitatea informațională este o problemă care devine tot mai strîngetă și mai actuală cu dezvoltarea rețelelor și industriei sistemului de calcul. Una din metodele de bază de asigurare a securității informaționale este metoda criptografică.

Cifrarea este procesul matematic de conversie a unui mesaj într-un formular care nu poate fi citit pentru toată lumea, cu excepția persoanei sau dispozitivului care are cheia de a „decripta" mesajul înapoi în formă lizibilă. Există multe metode de cifrare / decifrare, dar secretul datelor nu se bazează pe un algoritm secret, ci pe faptul că cheia de cifrare este cunoscută doar de persoanele de încredere.

În cadrul etapei de elaborare a tezei de master a fost studiată cu ajutorul resurselor electronice și a aplicațiilor propriu-zise tema criptării automate a documentelor. Analizînd diferite metode și sisteme de cifrare a informației a fost deduse două metode de elaborare a procesului: folosirea task scheduler și a aplicației de tip joiner. Informațiile accumulate au permis crearea scriptului powershell cu denumirea "FileCryptography.psm1" care va efectua cifrarea propriu-zisă. Dar pentru a efectua acest process în mod automat a fost creat alt script powershell cu denumirea "Crypt.ps1" care cu ajutorul cmdletului Test-Path va efectua verificarea locației fișirului. Ultimul pas fiind alipirea acestui script de către documentul pe care dorim să-l apărăm de compromitere.

Cifrarea este o componentă de bază, dar vitală, a confidențialității și securității datelor. După cum afirmă majoritatea specialiștilor din domeniul securității informației „Securitatea digitală devine din ce în ce mai importantă, pentru a ne proteja pe măsură ce efectuăm diferite operațiuni electronice. Iar la baza acestei securități se află cifrarea."

Bibliografie

1. IT Level. Lumea secretelor – coduri și criptografie [citat 15.09.2020]. Disponibil: https://www.itlevel.ro/cursuri-copii-bucuresti/
2. Ionut Morusan. Cifruri de substituție [citat 15.09.2020]. Disponibil: https://ionutmorosan.wixsite.com/encryptiondecryption/cifruri-de-descifrare
3. Infocad Blog. Criptosistemul Polybius [citat 17.09.2020]. Disponibil: https://infocadsite.wordpress.com/2016/08/27/criptosistemul-polybius/
4. Metoda Transpoziției [citat 19.09.2020]. Disponibil: https://fisieretextinfo.weebly.com/metoda-transpozitiei.html
5. Ignat Iurie. Sisteme criptografice [citat 20.09.2020]. Disponibil: http://www.security.ase.md/publ/ro/pubro23/pubro23.html
6. Metode moderne de cifrare [citat 22.09.2020]. Disponibil: https://polarize.ru/ro/programmy/primery-sovremennyh-algoritmov-shifrovaniya-osnovnye-sovremennye/
7. Algoritmul de cifrare DES [citat 25.09.2020]. Disponibil: https://www.securitatea-informatiilor.ro/solutii-de-securitate-informatica/algoritmul-de-criptografie-des/
8. Criptografie [citat 02.10.2020]. Disponibil: http://andrei.clubcisco.ro/cursuri/f/f-sym/5master/aac-criptografie
9. Cifrarea asimetrică [citat 05.10.2020]. Disponibil: https://ro.sawakinome.com/articles/technology/difference-between-symmetric-and-asymmetric-encryption.html
10. Elliptic curve cryptography [citat 12.10.2020]. Disponibil: https://avinetworks.com/glossary/elliptic-curve-cryptography/
11. Scripting: limbaj de programare [citat 20.10.2020]. Disponibil: https://ro.itpedia.nl/2018/07/24/scripting-scripttaal-is-iets-anders-dan-programmeertaal/
12. VBScript [citat 20.10.2020]. Disponibil: https://www.guru99.com/vbscript-tutorials-for-beginners.html
13. Jscript [citat 22.10.2020]. Disponibil: https://ru.bmstu.wiki/JScript
14. Shell Script [citat 25.10.2020]. Disponibil: https://www.hostinger.ru/rukovodstva/bash-skripty-rukovodstvo-po-funkcijam-bash-s-primerami/
15. C# [citat 25.10.2020]. Disponibil: http://progopedia.ru/language/csharp/

16. Asistență PowerShell [citat 27.10.2020]. Disponibil: https://docs.microsoft.com/ro-ro/power-platform/admin/powerapps-powershell
17. PS2EXE-GUI [citat 02.11.2020]. Disponibil: https://gallery.technet.microsoft.com/scriptcenter/PS2EXE-GUI-Convert-9b4b0493
18. Mscholtes/PS2EXE [citat 05.11.2020]. Disponibil: https://github.com/MScholtes/PS2EXE
19. File Joiner [citat 10.11.2020]. Disponibil: https://www.file-joiner.com/