UNIVERSITÀ DEGLI STUDI GUGLIELMO MARCONI
FACOLTÀ DI SCIENZE E TECNOLOGIE APPLICATE

CORSO DI LAUREA MAGISTRALE IN
INGEGNERIA INFORMATICA

Tesi di Laurea

CRITTOGRAFIA CLIENT-SIDE: ANALISI DELLO STATO DELL'ARTE E PROPOSTA DEL TOOL PROTOTIPALE CRYPTOFILE

Relatore
Prof. Paolo Bocciarelli

Candidato
Alessandro Cacciotti
Matricola: STA06814/LM32

Anno Accademico 2015/2016

INDICE

ABSTRACT

Negli ultimi anni, l'avvento dell'informatica e la nuova rivoluzione digitale, hanno portato all'utilizzo sempre più diffuso dei computer e degli altri dispositivi elettronici nella vita di tutti i giorni. Un crescente numero di persone sono solite custodire informazioni, documenti, foto o altri dati sensibili all'interno dei suddetti dispositivi, incuranti dei rischi in cui potrebbero incorrere nel caso questi cadessero nelle mani di qualche malintenzionato. L'importanza che assumono oggi alcune manciate di byte è impressionante: dati bancari, documenti top secret o semplicemente file contenenti dati sensibili la cui divulgazione comprometterebbe la privacy delle persone. Per questo motivo, la corretta protezione dei dati deve essere un obiettivo da raggiungere nel migliore dei modi. Sono quindi necessarie tecniche di Sicurezza Informatica in grado di proteggere la privacy degli utenti, mettendo al sicuro i dati strettamente riservati ad essi appartenenti.

La principale tecnica per la protezione dei dati è la Crittografia. Questa tecnica consente di trasformare i dati in modo tale da non rendere disponibili agli utenti non autorizzati le informazioni in essi contenute. Poter proteggere quindi i propri file attraverso un'applicazione che consenta di crittarli, tenendoli lontani da occhi indiscreti, è diventata ormai una necessità di primaria rilevanza per chiunque utilizzi un computer. Una volta messa in evidenza l'importanza che assume la crittografia nella protezione dei dati, è stata effettuata un'analisi di alcuni dei migliori sistemi attualmente disponibili che ne implementano le funzionalità. Tuttavia, la suddetta analisi, ha portato alla luce il fatto che non ne esiste uno che vada bene per qualsiasi tipologia di utente o che presenti tutte le migliori caratteristiche implementabili da un sistema crittografico. I sistemi di crittografia lato client attualmente disponibili presentano infatti, alcuni svantaggi, come la complessità di utilizzo, la scarsa

portabilità, la necessità di dover essere installati nel sistema, l'impossibilità di scelta dell'algoritmo di cifratura, la scarsa protezione o l'utilizzo di lunghe e complesse password da dover ricordare per la generazione delle chiavi. Le soluzioni attualmente disponibili presentano tuttavia anche interessanti caratteristiche, come consentire di cifrare file e cartelle, avere un'interfaccia grafica semplice e intuitiva, fornire servizi di compressione dei file, essere open source e fornire nuovi modi di generazione delle chiavi. Basandosi sui punti di forza evidenziati utilizzando ciascuno strumento, sono stati definiti i requisiti che un sistema di crittografia ideale dovrebbe soddisfare. Quest'ultimi, utilizzati come linee guida, hanno portato allo sviluppo del Tool Prototipale CryptoFile.

L'obiettivo che si pone questo progetto è quindi quello di realizzare un sistema di crittografia lato client che implementi la maggior parte dei punti di forza dei sistemi attualmente disponibili cercando di essere il quanto più possibile utilizzabile da ogni tipologia di utente. L'applicazione, che prende il nome di Cryptofile, si pone l'obiettivo di fornire un elevato livello di protezione, di consentire la scelta dell'algoritmo di cifratura, di non richiedere continuamente l'inserimento della chiave, di supportare l'utilizzo di algoritmi di cifratura in cascata, di essere compatibile con i principali sistemi operativi, di non richiedere installazione, di garantire semplicità di utilizzo, di presentare un'ottima interfaccia grafica, di fornire svariate funzioni per la protezione di file e cartelle, di utilizzare un modo alternativo per generare la chiave di cifratura e di consentire la possibilità di decifrare i file unicamente sul computer utilizzato per cifrarli.

Cryptofile implementa gli algoritmi di cifratura DES (Data Encryption Standard), Triplo DES, AES (Advanced Encryption Standard), Twofish e Serpent. L'utente può selezionare l'algoritmo che più si adatta alle proprie esigenze e la modalità con cui vuole inserire la chiave. Cryptofile consente di generare chiavi sia utilizzando la classica password, sia mediante un qualsiasi file (ad esempio un'immagine, un video, un documento ecc.) comportando così il doppio vantaggio di evitare che l'utente debba ricordare lunghe o complesse password per ottenere un buon livello di protezione e di consentire all'utente di portare con sé la chiave, ad esempio in una chiavetta USB, da tenere al sicuro dai malintenzionati. L'applicazione inoltre utilizza la compressione dei dati prima della cifratura per migliorare la resistenza alla crittoanalisi. Per poter offrire agli utenti la possibilità di decifrare i dati unicamente sul computer sul quale sono stati cifrati, Cryptofile, può cifrare i file utilizzando oltre alla chiave anche l'identificativo dell'hardware in esecuzione al momento dell'operazione di cifratura. Infine, l'interfaccia grafica è stata sviluppata in modo da risultare semplice e intuitiva, facendo sì che l'applicazione possa essere utilizzata facilmente da qualsiasi tipologia di utente.

Dai test effettuati, CryptoFile è riuscito a soddisfare tutti i requisiti proposti e si è quindi attestato come un ottimo strumento per aiutare qualsiasi tipologia di utente, dal più esperto al neofita, nell'arduo compito della protezione dei dati. Come possibile obiettivo futuro, sarebbe interessante rendere disponibile il programma agli utenti via internet e riuscire a svilupparne una versione utilizzabile dai dispositivi mobili, in modo da poter facilmente proteggere i dati anche su smartphone e tablet. Molti utenti infatti, memorizzano ogni giorno grandi quantità di dati e informazioni su questi dispositivi, incuranti dei rischi che possono correre nel caso che cadano in mani sbagliate. Il Tool Prototipale CryptoFile potrebbe facilmente essere trasformato in una applicazione Android o IOS per poter mettere

a disposizione le sue funzionalità anche per il mondo mobile.

BIBLIOGRAFIA

[1] Berardi Luigia, Beutelspacher Albrecht, *Crittologia come proteggere le informazioni riservate*, Franco Angeli, Milano, 2001

[2] Crittografia, *Treccani,* www.treccani.it/enciclopedia/crittografia/

[3] De Rosa Castello Antonio, *Sistemi di Cifratura*, Libreria Clup, Milano, 2004

[4] Ferguson Niels, Kohno Tadayoshi, Schneier Bruce, *Il Manuale della Crittografia: applicazioni pratiche dei protocolli crittografici*, Apogeo, 2011

[5] Ferguson Niels, Schneier Bruce, *Crittografia pratica,* Apogeo, 2005

[6] Languasco Alessandro, Zaccagnini Alessandro, *Manuale di Crittografia: teoria, algoritmi e protocolli*, Hoepli, 2015

[7] Pfleeger Charles P., Pfleeger Shari Lawrence, *Sicurezza in Informatica,* Pearson, 2008

[8] Stallings William, *Sicurezza delle reti*, Pearson, 2007

[9] Trappe Wade, Washington Lawrence C.*, Crittografia con elementi di teoria dei codici*, Pearson, 2009