Università degli Studi di Salerno

Dipartimento di Informatica



Corso di Ingegneria Gestione ed Evoluzione del Software

SecureD

Test Plan

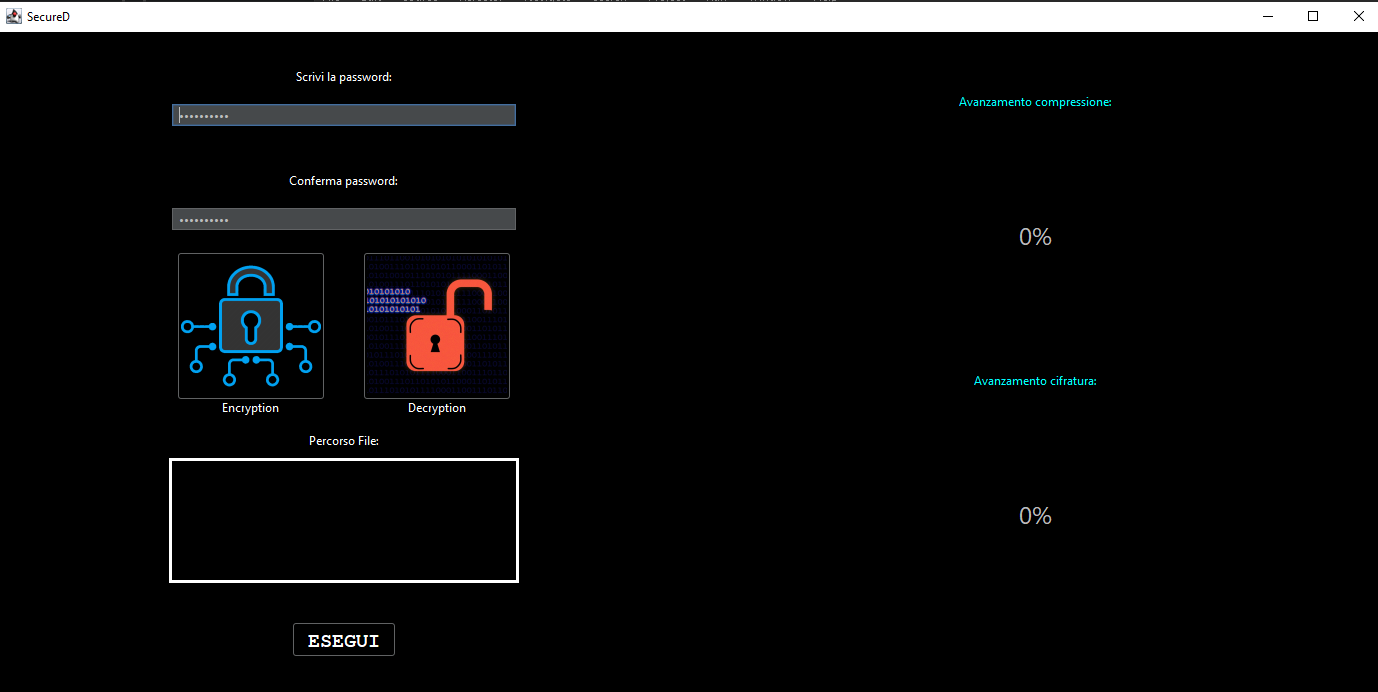
INTRODUZIONE

Lo scopo di questo documento è quello di analizzare pianificare e gestire lo sviluppo e le attività di testing del progetto SecureD.

Questa sessione di lavoro va ad verificare l’operato dell’applicazione SecureD in casi studiati per testare le funzionalità core, al fine di ottenere un corretto funzionamento.

Dai risultati ottenuti, se si dovessero evidenziare anomalie, saranno apportate modifiche atte a migliorare la stabilità del sistema.

PANORAMICA



SecureD è un’applicazione sviluppata per il sistema operativo Windows ed implementata in java che permette agli utenti di cifrare e decifrare file e cartelle.

Essendo costruita per essere usata anche da utenti non affini al mondo dell’informatica SecureD si contraddistingue per il suo funzionamento semplice, per questo motivo il layout principale è progettato per essere intuitivo usando immagini che richiamano l’attenzione dell’utente sulle operazioni di rilievo e che comunicano anticipatamente il significato dell’azione che si andrà a compiere.

FUNZIONALITA’ DA TESTARE

Nel testing si andranno a considerare la funzionalità principale di SecureD.

Le funzionalità che verranno testate sono:

* **Cifratura di file**

Funzionalità composta di più componenti

* Controllo password

Per stabilire se rispetta le specifiche

* Effettiva cifratura dei file

Per stabilire se il file cifrato viene effettivamente prodotto o meno

APPROCCIO

La sessione di testing di SecureD è svolta usando un’approccio di tipo **BLACK BOX**il quale prevede che i test vengano effettuati senza considerare l’implementazione delle funzionalità testate.

L’approccio della fase di testing si divide in due fasi:

* Testing sul sistema originale

Creazione test per verificare il controllo della password

* Testing sul sistema dopo il porting

Creazione test per verificare che i controlli di sicurezza sulla password siano equivalenti a quelli del sistema pre-porting

TEST CASES

Per sviluppare i test case sarà usato il metodo del **Category Partition**.

Questo metodo consiste nell’identificare, per ogni funzionalità da testare, dei parametri e per ogni parametro individuare delle categorie che saranno poi suddivise in scelte.

I test case verranno poi definiti nel documento di Test Case Specification.

SPECIFICA DEI TEST CASES

Cifratura file

#Parametro

Password

#Categorie

LPass

1 lunghezza 0-7. [error]

2 lunghezza 8-64 [property LUserOk]

3 lunghezza >8 [error]

#Parametro

Conferma Password:

#Categorie:

EQPasswordConfirm:

1 uguale a password [if LPassOk] [property EQPasswordConfirmOk]

2 diversa da password [error]

#Parametro

Percorso file

#Categorie

Validità

1 percorso file valido

2 percorso file non valido

RIFERIMENTI

Lunghezza massima password: https://cheatsheetseries.owasp.org/cheatsheets/Authentication\_Cheat\_Sheet.html