

PROGETTO CORSO SICUREZZA DEL SOFTWARE

## Offuscatore per il linguaggio Python

Candidati:

**Giovanni Bellorio**

Matricola VR419955

**Kevin Costa**

Matricola VR424301

**Alessandro Cosma**

Matricola VR420117

## INDICE

---

1	INTRODUZIONE	3
2	BACKGROUND	4
2.1	Offuscatore	4
2.1.1	Impossibilità di offuscare un programma	5
2.1.2	Valutare le trasformazioni offusanti	5
2.2	Tecniche di offuscamento del codice	6
2.2.1	Layout Obfuscation	6
2.2.2	Control Flow Obfuscation	7
3	OFFUSCATORE PER PYTHON	8
3.1	Scelte progettuali	8
3.2	Algoritmo e codice	8
3.2.1	Codice di Layout Obfuscation	9
4	ESEMPIO DI FUNZIONAMENTO	10
	Bibliografia	10

## INTRODUZIONE

---

Lo scopo di questo progetto è realizzare un offuscatore per il linguaggio Python. Il programma che implementa l'offuscatore sarà realizzato anch'esso in Python e prenderà in considerazione le seguenti tipologie di offuscamento del codice:

- **Layout obfuscation**
- **Data obfuscation**
- **Control Flow obfuscation**

Nel capitolo 2 daremo una panoramica generale sui concetti legati all'offuscamento del codice, spiegando cos'è formalmente un offuscatore, quali sono le sue caratteristiche, i suoi pregi e i suoi difetti, infine spiegheremo nel dettaglio le varie tecniche di offuscamento che andremo ad utilizzare.

Nel capitolo 3 verrà presentato il nostro programma per l'offuscamento del codice. Elencheremo le varie scelte progettuali effettuate in fase di progettazione (3.1) e successivamente presenteremo passo passo il codice che implementa l'algoritmo (3.2).

Infine, nel capitolo 4 mostreremo un semplice esempio del suo funzionamento accompagnato da alcuni test.

## BACKGROUND

---

Quando si considera un software sviluppato e distribuito, la maggior parte del suo “know-how” risiede nel prodotto stesso. Risulta quindi essenziale la protezione del suo codice e della sua proprietà intellettuale.

Attacchi di *reverse-engineering* hanno l’obiettivo di attuare analisi statiche e dinamiche del codice, al fine di capire il funzionamento interno di un programma proprietario di interesse. La protezione è necessaria ad ogni livello di funzionamento del programma, a partire dal codice sorgente, fino ad arrivare al codice macchina, passando anche per le informazioni di interesse che il programma da proteggere scambia con l’ambiente di esecuzione.

Esistono varie tecniche di protezione del codice con differenti obiettivi:

- *Misure legali*: leggi, copyright, patenti, brevetti e licenze ideate per proteggere la “forma” e l’idea di un programma.
- *Offuscamento*: rendere difficile il reverse-engineering del programma.
- *Watermarking del software*: inserire una firma o un riconoscimento contro il furto del programma.
- *Tamper-proofing*: rilevare violazioni contro l’integrità del codice o modifiche illegali.

Essendo il nostro progetto mirato alla realizzazione di un offuscatore per codice Python, descriveremo ora in dettaglio il concetto di offuscatore e presenteremo alcune delle principali tecniche utilizzate.

### 2.1 OFFUSCATORE

Sia:

$$P \xrightarrow{T} P'$$

una trasformazione di un programma sorgente  $P$  in un programma  $P'$  con  $P, P' \in \text{Programs}$ , cioè l’insieme dei programmi.

$P \xrightarrow{T} P'$  è una trasformazione di offuscamento se  $P$  e  $P'$  hanno lo stesso *comportamento osservabile*.

Più precisamente, affinché  $P \xrightarrow{T} P'$  sia una trasformazione di offuscamento legale, devono valere le seguenti condizioni:

1. Se  $P$  non riesce a terminare o termina in una condizione di errore, allora  $P'$  può o non può terminare.
2. Altrimenti,  $P'$  deve terminare e produrre lo stesso output di  $P$ .

Il *livello di sicurezza* rispetto al reverse-engineering che un offuscatore aggiunge ad un dato programma dipende da vari fattori: raffinatezza della trasformazione di offuscamento, potenza del deoffuscatore, quantità di risorse (tempo e memoria) disponibili al deoffuscatore.

### 2.1.1 Impossibilità di offuscare un programma

Una trasformazione di offuscamento non potrà mai proteggere completamente un programma. Fred Cohen, il primo ad introdurre la diversità dei programmi come difesa contro gli attacchi automatici ai sistemi operativi, affermava che:

*“Any protection scheme other than a physical one depends on the operation of a finite state machine, and ultimately, any finite state machine can be examined and modified at will, given enough time and effort. The best we can ever do is delay the attack by increasing the complexity of making desired alterations (security through obscurity)”*

[inserire risultati paper “On the impossibility of code obfuscation”]

### 2.1.2 Valutare le trasformazioni offuscanti

Una trasformazione offuscante è valutata in base alle seguenti proprietà:

- **Potenza:** quanto più difficile è comprendere il codice offuscato rispetto a quello originale.
- **Resilienza:** misura quanto una trasformazione regge l’attacco di un deoffuscatore automatico.
- **Costo:** misura quanto overhead computazionale (tempo e spazio) viene aggiunge all’applicazione offuscata.
- **Furtività:** misura quanto bene il codice nuovo introdotto con la trasformazione si integra con il codice originale.

**POTENZA** Sia  $T$  una trasformazione che preserva il comportamento, tale che  $P \xrightarrow{T} P'$  trasformi un programma  $P$  in un programma  $P'$ . Sia  $E(P)$  la complessità di  $P$ .

$T_{pot}(P)$ , la potenza di  $T$  rispetto ad un programma  $P$ , è una misura del grado con cui  $T$  cambia la complessità di  $P$ .

$$T_{pot}(P) = E(P')/E(P) - 1$$

$T$  è una trasformazione di offuscamento potente se  $T_{pot}(P) > 0$ .

**RESILIENZA** Sia  $T$  una trasformazione che preserva il comportamento, tale che  $P \xrightarrow{T} P'$  trasformi un programma  $P$  in un programma  $P'$ .  $T_{res}(P)$  è la resilienza di  $T$  rispetto ad un programma  $P$ .

$T_{res}(P) = one - way$  se l’informazione è rimossa da  $P$  tale che  $P$  non può essere ricostruito da  $P'$ .

$$T_{res} = Resilience(T_{Deobfuscator\_effort}, T_{Programmer\_effort})$$

**COSTO** Il costo di una trasformazione offuscante è il tempo di esecuzione (o la quantità di spazio occupato) del programma offuscato rispetto a quello originale.

$T_{cost}(P)$ , cioè il costo di un programma  $P$ , può essere classificato su una scala di quattro punti come segue:

- **caro:** se l’esecuzione di  $P'$  richiede esponenzialmente più risorse di  $P$ .

- **costoso**: se l'esecuzione di  $P'$  richiede  $O(n^p)$ ,  $p > 1$  risorse più di  $P$ .
- **economico**: se l'esecuzione di  $P'$  richiede  $O(n)$  risorse più di  $P$ .
- **gratuito**: se l'esecuzione di  $P'$  richiede  $O(1)$  risorse più di  $P$ .

**FURTIVITÀ** Mentre una trasformazione resiliente potrebbe non essere suscettibile agli attacchi di deoffuscatori automatici, potrebbe comunque essere suscettibile agli attacchi degli umani.

In particolare, se una trasformazione introduce un nuovo codice che differisce ampiamente da ciò che è presente nel programma originale, sarà facile individuare per un reverse engineer. Tali trasformazioni non sono furtive (a.k.a. *unstealthy*).

La furtività è una nozione sensibile al contesto. Il codice può essere nascosto in un programma ma estremamente visibile in un altro.

## 2.2 TECNICHE DI OFFUSCAMENTO DEL CODICE

In questa sezione andremo a descrivere a livello teorico le tecniche di offuscamento che saranno utilizzate successivamente all'interno del nostro offuscatore.

### 2.2.1 *Layout Obfuscation*

L'obiettivo del *Layout Obfuscation* è cambiare o rimuovere le informazioni utili dal codice senza influire sulle istruzioni reali.

Tecniche principali utilizzate per questo tipo di offuscamento:

- **Rimozione commenti**: vengono rimossi i commenti e i docstring presenti nel codice.
- **Rinominazione degli identificatori**: i nuovi nomi possono utilizzare diversi schemi, numeri, caratteri non stampabili o caratteri invisibili. Inoltre i nomi possono essere riutilizzati, purché usati in ambiti diversi.

Queste sono trasformazioni *one-way* in quanto la formattazione originale non può essere ripristinata.

Vantaggi:

- potente contro l'attacco umano
- per quanto riguarda i costi è gratuito.
- è molto utile per offuscare *authorship* del codice.

Svantaggi:

- Ha una bassa potenza, in quanto nella formattazione c'è poco contenuto semantico.

### 2.2.2 *Control Flow Obfuscation*

Il *Control Flow Obfuscation* trasforma un control-flow ben strutturato di un programma eseguibile in una struttura difficile da analizzare da un programma che rileva le trasformazioni del control-flow. Tale offuscamento può ostruire e fermare gli attacchi statici al control-flow del codice eseguibile sotto attacchi di tipo white-box. Questa tecnica costringe l'attaccante ad eseguire attacchi dinamici per ottenere il control-flow, in questo modo diventa molto più difficile da ottenere e aumenta significativamente lo sforzo dell'attacco.

Tecniche principali utilizzate per questo tipo di offuscamento:

- **Predicati opachi:** sono espressioni di valore booleano per le quali il difensore sa se restituiranno true, false o talvolta true e talvolta false
- **CFG Riducibili:** sono grafi che possono essere ridotti a un singolo nodo mediante una sequenza di applicazioni di due regole
- **Predicati opachi dinamici:** una famiglia di predicati opachi correlati, che valutano tutti lo stesso risultato ad ogni esecuzione, ma in diverse esecuzioni possono valutare risultati diversi

Vantaggi:

- potente contro l'analisi statica
- difficili da valutare dall'attaccante per la complessità esponenziale
- è molto utile per offuscare *authorship* del codice.

Svantaggi:

- Vulnerabile all'analisi dinamica

## OFFUSCATORE PER PYTHON

---

### 3.1 SCELTE PROGETTUALI

### 3.2 ALGORITMO E CODICE

Viene ora presentato il codice che implementa l'offuscatore.

Il codice sorgente è composto da un metodo `main()` che rappresenta l'entry point del nostro programma e da una serie di funzioni e metodi che vengono invocate all'interno di tale metodo per svolgere le funzioni di offuscamento.

```
def main():

    print("-----")
    print("OBFUSCATION STARTED\n")

    name_src = sys.argv[1] # name of the source file, passed as argument
    name_dest = name_src+"_OBFUSCATED.py" # name of the destination file

    file_SRC = open(name_src, "r")
    file_DEST = open(name_dest, "w")

    # Call 'remove_comments_and_docstrings()' function on the source file object
    # which it is first converted to a string through the read() method.
    # 'out' contains a string with the entire code
    out = remove_comments_and_docstrings(file_SRC.read())

    # Call 'opaque_predicate()' function
    out = opaque_predicate(out)

    # Call 'encoding_literal_data()' function
    out = encoding_literal_data(out)

    # Call 'obfuscate_variables()' function
    out = obfuscate_variables(out)

    # Call 'obfuscate_functions()' function
    out = obfuscate_functions(out)

    # Write the result into file_DEST
    file_DEST.write(out)
    file_DEST.close()
    file_SRC.close()

    print("\nOBFUSCATION ENDED")
    print("-----")

if __name__ == '__main__':
    main()
```

All'inizio dell'esecuzione del programma, viene letto il nome del file contenente il software Python da offuscare e salvato nella variabile `name_src`: questa informazione deve essere passata come argomento di input all'offuscatore, con una sintassi del tipo:



```
python3 offuscatore.py <nome_file_da_offuscare>.py
```

dove `offuscatore.py` è il nome dell' offuscatore e `<nome_file_da_offuscare>` è il nome del file di input.

Successivamente viene aperto in sola lettura il file sorgente (variabile `file_SRC`) e viene creato un nuovo file, chiamato come il precedente file di input ma con l'aggiunta della suffisso "OBFUSCATED" e salvato nella variabile `file_DEST`: esso rappresenta l'output del nostro programma cioè il software offuscato.

In seguito vengono chiamate in sequenza le seguenti funzioni:

- **`remove_comments_and_docstrings()`**: esegue un *layout obfuscation* rimuovendo i commenti e la documentazione;
- **`opaque_predicate()`**: esegue un *control flow obfuscation*, inserendo predicati opachi;
- **`encoding_literal_data()`**: esegue un *data obfuscation*, codificando stringhe, array e interi;
- **`obfuscate_variables()`**: esegue un *layout obfuscation*, rinominando i nomi di variabili;
- **`obfuscate_functions()`**: esegue un *layout obfuscation*, rinominando i nomi di funzione e il relativo "corpo".

Ognuna di queste funzioni riceve in input il programma (variabile `out`) trasformato dalla funzione di offuscamento precedente, vi applica un certo insieme di trasformazioni offusanti e successivamente restituisce un output trasformato, che viene poi dato in input alla funzione di offuscamento successiva.

Alla fine del metodo `main()`, viene scritto nel file di output il programma offuscato e vengono chiusi i file di input e output precedentemente aperti.

### 3.2.1 Codice di Layout Obfuscation



## BIBLIOGRAFIA

---