

Corso di Laurea in Ingegneria e Scienze Informatiche

# ClientShield: Implementazione di un Servizio Windows per la Sicurezza DNS

Tesi di laurea in:  
PROGRAMMAZIONE AD OGGETTI

*Relatore*

**Prof. Viroli Mirko**

*Candidato*

**Federico Diotallevi**

---

---

# Sommario

Lo sviluppo della tecnologia cresce sempre più velocemente e, con essa, anche i rischi che gli utenti corrono semplicemente navigando in rete. Questa tesi si inserisce nell'ambito dell'internet filtering, cioè la possibilità di filtrare il traffico in rete negando l'accesso a siti potenzialmente pericolosi.

L'obiettivo di questo progetto è lo sviluppo di un software che sia facilmente installabile su un dispositivo Windows e filtri tutte le richieste web effettuate. Si vuole offrire la possibilità ad un amministratore di rete di attivare e disattivare la protezione del dispositivo da remoto, decidendo eventualmente anche quali categorie di siti bloccare.

Per lo sviluppo è stata fondamentale la collaborazione con FlashStart, azienda di riferimento nel mercato italiano per quanto riguarda il filtraggio cro:DNSDomain Name System (DNS).

Il software è stato sviluppato in contesto aziendale come prototipo e sfrutta ampiamente le soluzioni di filtraggio aziendali. Ciò ha facilitato la gestione delle categorie e dell'effettivo filtraggio DNS, permettendo al progetto di focalizzarsi sulla cattura e redirectione del traffico internet del dispositivo verso i server gestiti da FlashStart.

---

---

*Optional dedication.*

---

---

# Indice

Sommario	iii
Introduzione	3
1 Contesto	5
1.1 Internet Filtering . . . . .	5
2 Contribution	7
	9
Bibliografia	9









---

# Introduzione

Navigare in rete è senz'altro una delle attività più diffuse al giorno d'oggi in tutto il mondo. La quantità di informazioni a cui si può accedere è pressoché infinita e, soprattutto, a disposizione di chiunque.

La digitalizzazione delle risorse è ormai diventata essenziale per qualsiasi realtà, dal settore pubblico a quello privato. Tuttavia, tale pratica espone inevitabilmente al rischio che documenti, dati e informazioni sensibili diventino obiettivo di attacchi informatici. A conferma di ciò, il recente rapporto [pISI24] evidenzia come gli attacchi informatici gravi a livello globale siano passati, in media, da 4.5 a 9 al giorno in soli cinque anni. Secondo il rapporto, gli incidenti critici sono aumentati dal 47% all'81% del totale e, in Italia, il 58% degli attacchi è costituito da malware, phishing e social engineering.

Con il recente e rapidissimo sviluppo delle *cro:AI*Intelligenza Artificiale (AI) il campo dell'Internet Filtering ha subito una vera e propria rivoluzione. I nuovi modelli di Machine Learning sono capaci di analizzare e identificare con precisione siti malevoli, grazie anche ai giganteschi volumi di dati di cui dispongono. Questi sistemi riescono a riconoscere tecniche di phishing e malware avanzate, anche quando progettate per eludere i metodi di rilevamento tradizionali.

Questa tesi si colloca in questo contesto e si propone l'obiettivo di sviluppare un software prototipale per il filtraggio internet sul computer di installazione. Il lavoro illustrerà dettagliatamente tutte le fasi di analisi, progettazione e sviluppo del progetto.

Data la necessità di interazione con componenti specifici del sistema operativo, il software è stato sviluppato esclusivamente per Windows, con l'obiettivo di creare un servizio di sistema.

**Struttura della Tesi** La tesi si articola in 4 capitoli principali, che descrivono le diverse fasi della realizzazione del progetto, in particolare:

- **Capitolo 1 (Contesto):** in questo capitolo si tratta in maniera approfondita il contesto aziendale e il problema affrontato dalla tesi. Viene analizzato il software attualmente presente in FlashStart e le motivazioni che inducono alla necessità di un nuovo sviluppo.
- **Capitolo 2 (Requisiti):** in questo capitolo vengono affrontati casi d'uso e requisiti, analizzando il funzionamento e la percezione del progetto dal punto di vista dell'utente.
- **Capitolo 3 (Tecnologie):** in questo capitolo vengono riportate le diverse tecnologie utilizzate e le scelte che hanno portato al loro impiego nel progetto.
- **Capitolo 4 (Analisi e progettazione):** in questo capitolo viene descritta la fase di analisi e progettazione del sistema, illustrandone in particolare l'architettura e i pattern utilizzati, evidenziando in che modo il software ne tragga guadagno.

---

# Capitolo 1

## Contesto

### 1.1 Internet Filtering

Il caso di studio oggetto di questa tesi è un software prototipale, che si inserisce nell'ambito dell'Internet Filtering. Per Internet Filtering si intende un sistema di monitoraggio, controllo e limitazione dell'accesso alle risorse online, basato su criteri predefiniti.

Una tecnologia di questo tipo risulta particolarmente utile ad aziende, scuole ed enti pubblici. Tramite questa pratica è infatti possibile effettuare controlli sul contenuto delle pagine web, limitando o impedendo l'accesso a siti contenenti malware o, eventualmente, contenuti indesiderati (ad esempio siti di scommesse, pornografia, droghe...). Risulta evidente fin da subito che per garantire un filtraggio di contenuti preciso ed efficace è necessaria un'attenta analisi delle pagine web, per evitare di correre il rischio di impedirne immotivatamente l'accesso.

Questa tesi è svolta come progetto in collaborazione con FlashStart, leader italiana per quanto riguarda il filtraggio Domain Name System (DNS). Un server DNS è un sistema che permette di tradurre nomi di domini leggibili da un uomo, in indirizzi interpretabili da dei computer per connettersi tra loro. Il filtraggio DNS si basa proprio su questo principio: quando si accede ad un sito web attraverso un browser qualsiasi, il computer interrogherà un server DNS per ottenere l'indirizzo attraverso cui sia possibile accedere al sito. FlashStart offre un servizio DNS configurabile, attraverso cui è possibile definire delle categorie di siti da bloccare.

I server dell'azienda aggiornano continuamente la lista delle categorie bloccate, facendo largo uso di Intelligenza Artificiale (AI) per garantire rapido aggiornamento (in risposta alla nascita di nuovi siti) ed alta precisione. Quando un utente, utilizzando un computer protetto dal servizio di FlashStart, tenta di accedere ad un sito appartenente ad una delle categorie bloccate, il DNS risponderà alla richiesta di risoluzione del nome con l'indirizzo di una pagina indicante i motivi del blocco, al posto di quella richiesta.







---

# Bibliografia

- [pISI24] Clusit Associazione Italiana per la Sicurezza Informatica. Rapporto clusit 2024 sulla sicurezza ict in italia - aggiornamento ottobre 2024. Rapporto di ricerca CLUSIT-2024-10, Clusit, ottobre 2024.



---

# Riconoscimenti

Optional. Max 1 page.