UNIVERSITÉ
Concordia
UNIVERSITY

Security Evaluation of Censorship Evasion Tools

(INSE 6150 - Security Evaluation Methodologies)

Submitted to
Prof. Jeremy Clark

Submitted by
Pranesh Sekar (40195581)
Kimia Ghasemi (40224378)

Table of Contents

ABSTRACT **3**

INTRODUCTION **3**

VARIOUS CENSORSHIP EVASION TOOLS **3**

VPNs 3
Proxy Servers 4
Smart DNS services 4
Using the site's IP address directly 5
TOR 5

USABILITY, DEPLOYABILITY AND SECURITY EVALUATION **6**

Usability 6
Deployability 7
Security 8

REFERENCES **10**

Abstract

The increasing use of censorship by governments and other organizations has led to the development of various tools and techniques for evading censorship. However, the security of these tools has not been widely evaluated. This paper seeks to fill this gap by providing a complete evaluation of popular censorship evasion tools encompassing the usability, deployability and security properties.

Introduction

First, we review the most common censorship evasion tools, including virtual private networks (VPNs), proxy servers, smart DNS, and Tor. We then evaluate their security properties, including the level of encryption, the use of secure protocols, and the ability to protect against traffic analysis.

Next, we conduct a thorough analysis of the security risks associated with using censorship evasion tools, including the risk of malware infection, the potential for government surveillance, and the possibility of interception by third-party actors.

Finally, we provide recommendations for maximizing the security of censorship evasion tools, the implementation of security best practices, and the selection of reputable and trustworthy providers. Overall, this paper provides a practical resource for people and organizations seeking to evade censorship while maintaining the security of their online activities.

Various Censorship evasion tools

VPNs

A virtual private network (VPN) is a software tool that allows users to securely access the internet while hiding their online activities from others. VPNs work by encrypting the user's internet connection and routing it via a secure server in another location, effectively masking the user's true IP address and location. This allows users to access blocked content and protect their privacy online.

VPNs also provide a high level of security for online activities. By encrypting the user's internet connection, VPNs protect against hackers and other cybercriminals who may try to intercept sensitive information such as passwords and credit card numbers. This makes VPNs particularly useful for accessing public Wi-Fi networks, where the risk of cyber-attacks is higher.

Another benefit of VPNs is the ability to access content that is restricted by location. Many streaming services, such as Netflix and Hulu, have different content libraries for different regions. With a VPN, users can access content that is only available in other countries by connecting to a server in that location.

There are some potential drawbacks, such as slower internet speeds and the need to trust the VPN provider, the benefits of using a VPN far outweigh the risks.

Proxy Servers

Proxy servers act as intermediaries between clients and servers. When a client device, such as a computer or a mobile phone, requests a server, the proxy server intercepts the request and delivers it to the server on behalf of the client. This allows the client to access resources on the server without directly connecting to it.

There are several benefits to using a proxy server. One of the most crucial is that it can improve the security of a network by acting as a barrier between the client and the server. The proxy server can screen incoming requests and block any that are deemed to be malicious or unwanted. This helps to protect the client and the server from cyberattacks and other threats.

Another advantage of using a proxy server is that it can help improve a network's performance. When a client requests a resource from a server, the proxy server can cache the response so that if another client makes the exact request in the future, the proxy server can quickly return the cached response instead of forwarding the request to the server again. This reduces the load on the server and can enhance the overall pace and responsiveness of the network.

Additionally, a proxy server can be used to enhance privacy and anonymity on the internet. When a client connects to a server via a proxy, the server only visits the IP address of the proxy, not the IP address of the client. This can help to protect the client's privacy and anonymity, as their real IP address is hidden from the server.

There are various attacks on proxies such as session hijacking, where attackers steal victims' sessions and redirect data traffic; malicious mobile node flooding, where victims are flooded with packets or network traffic is redirected to malicious nodes; replay attack, where data is passively captured and retransmitted to produce unauthorized results; man in the middle attack, where the attacker places themselves in the middle of data transmission between two parties; insider attack, where a system user misuses resources; modification attack, where the authentication message of the mobile access gateway or mobile node is modified; eavesdropping, where session data is stolen between a mobile device and its home agent; and stolen verifier, where the attacker steals a verification table from the authentication system.

Smart DNS services

A Smart DNS is also useful for users who want to protect their online privacy. When a user accesses a website using a traditional DNS, their internet service provider (ISP) can see the websites they are visiting. This can be a problem for users who want to keep their online activities private. With a Smart DNS, the user's DNS queries are routed through a different server, which means that the ISP cannot see the websites that the user is accessing.

In some countries, the government may block certain websites or types of content by blocking their domain name and not the IP address of the server. By using a Smart DNS, users can access these websites by getting the IP address of the server while posing as a user from another country.

There are four major types of attacks which can happen in smart DNS services: DDoS, DNS amplification, DNS hijacking, and DNS tunneling. DDoS attacks use a botnet to run malicious queries in the background to flood a target's network. DNS amplification attacks use publicly accessible open DNS servers to flood a target's DNS response traffic with spoofed source addresses. DNS hijacking can occur when an attacker modifies a DNS nameserver to one they control, changes a domain's IP address to redirect it to their own, or compromises an organization's router to change the DNS server pushed down to devices. DNS tunneling uses the DNS protocol to tunnel information through the network. To mitigate these attacks, organizations can use DNS security measures such as firewalls, rate limiting, and DNS security protocols.

Using the site's IP address directly

It is possible to evade censorship by using an IP address directly. Censorship typically works by blocking access to certain websites based on their domain name. By using the IP address of a website instead of its domain name, it may be possible to bypass censorship and access the website.

Nevertheless, there are a few disadvantages to this approach. First, not all websites have a static IP address that never changes. In these cases, using the IP address to access the website may not work, as the IP address may have changed since the censorship was implemented.

Second, censorship may still be effective even if a website has a static IP address. Many censors can block access to websites based on their IP address and blocking access based on their domain name.

Therefore, while using an IP address to evade censorship is a potential option, it is not a reliable or foolproof method.

TOR

Tor is a free and open-source software that enables anonymous communication. It is a network of virtual tunnels that allows people to browse the internet privately and securely. Tor is short for The Onion Router, named after the onion routing technique, that it uses to encrypt data and protect users' privacy.

In TOR, the user first establishes a connection with an onion router. The user then sends their message, which is encrypted and wrapped in multiple layers of encryption. The outermost layer is peeled off by the first onion router, revealing the next layer of encryption. This process continues as the message is passed from one onion router to the next, with each router peeling off a layer of encryption until the innermost layer is reached. The final onion router then sends the decrypted message to its destination. The use of multiple layers of encryption and multiple onion routers makes it difficult for anyone intercepting the message to determine its sender, recipient, or contents.

One of the main limitations of Tor is that it can slow down your internet connection. This is because your traffic is being routed through multiple servers. Additionally, the website itself will still be able to see your real IP address since java script is enabled in your browser. And also, certain forms of surveillance, such as traffic analysis, can still potentially be used to deanonymize Tor users.

Tor was initially developed by the U.S. Navy for protecting government communications, but it is now used by a wide range of people, including journalists, activists, and ordinary citizens who want to keep their online activities private.

Usability, Deployability and Security Evaluation

Usability, deployability, and security evaluation are all important factors to consider when designing and implementing a software system. Usability refers to the ease with which users can learn and use the system, deployability refers to the ease with which the system can be deployed in different environments, and security evaluation is the process of assessing the security of a system to identify potential vulnerabilities and protect against malicious attacks. Together, these factors help ensure that a software system is effective, efficient, and secure.

The following table list all the possible properties in a censorship evasion tool.

Usability	**Deployability**	**Security**
Ease of Use	Handle a lot of traffic	Encryption Used
Speed and Performance	Availability in user location	Protocols Supported
Device Compatibility	Easy Setup	No log Policy
Customer Support	Software Upgradation	Kill Switch
Pricing and Value for money	Simultaneous connections	Leak Protection
Flexibility		Audited Security
		Reputation

Usability

Ease of Use

Users must be able to use the application with a clean UI and must be able to navigate the app with ease.

● - Easy to use

◕ - Require help from experts to work with

○ - Bad to use for everybody

Speed and Performance

The application/service must be fast and must not affect your day-to-day activities.

● - Faster and efficient

○ - Slower and Resource Hogging

Device Compatibility

The application must be usable in all devices and platforms / Operating Systems.

● - Can be used in all devices

◕ - Requires extra work in some platforms

○ - Can be used in only one device / platform

Customer Support

The product must have a 24x7 customer service via channels like phone, chat UI or at least email.

● - Excellent Customer service

◕ - Customer service behind paywall / community support only

○ - No customer service

Pricing and Value for money

The product must have a decent pricing plan or at least a free plan with limited number of features.

● - Free all the time

◕ - Free with paid plan options

○ - Paid plan only

Flexibility

The application should adapt to the user's needs. For example, the application should use browser traffic when the user is using browser and the application traffic when the user is using an application/software

● - Flexible with wide range of user’s applications

○ - Can be used only with a certain type of application

Deployability

Handle a lot of traffic

The server of the tools must handle a lot of traffic when many people start using it.

● - The server can scale up to meet with the load

○ - The server can only serve a small amount of people

Availability in user location

Even though the tool can circumvent censorship, the application should not be blocked from the user to be downloaded and installed.

● - The availability of the tool cannot be blocked by outsiders

◕ - Can be blocked but downloadable from illegal means

○ - Can be easily blocked and made inaccessible to the users

Easy Setup

The application must be able to be installed in a proper and usual way.

● - Easily installable

◕ - Easily installable in some platforms but difficult in other platforms

○ - Not easily installable

Software Upgradation

The application must be easily upgradable when needed through self-update or through app stores.

● - Easily updatable

◕ - Easily updatable in some platforms but difficult in other platforms

○ - Not easily updatable

Simultaneous connections

The application must be usable on multiple devices of the user.

● - Usable in multiple devices

○ - Can be used in one device only

Security

Encryption Used

The application must use proper encryption with at least 128 bit entropy.

● - Only the best encryption is used

◕ - Supports encryption but not turned on by default

○ - Does not encrypt

Protocols Supported

The application must support multiple protocol so that it is compatible with all platforms and backwards compatible

● - Supports many protocols

○ - Supports only one single protocol

No log Policy

The application must not log user content on their server. It leaves the user vulnerable when the sell the data or give it to the authorities

● - Nothing is logged
◕ - Can be logged by the owner/service provider of the tool
○ - Always logged

Kill Switch

The application must have a kill switch to immediately stop all traffic or block all content to the server when the user detects something fishy is going on.

● - Provides kill switch
◕ - It’s up to the service provider
○ - No way to implement kill switch

Leak Protection

Other applications must not find a way around the tool to get the real details of the user.

● - All the user traffic must follow the application’s protocol
◕ - Apps can bypass the tool’s features
○ - Easily leakable

Audited Security

The application must be audited by security personnel to ensure they have no loopholes or security vulnerabilities.

● - Always audited
◕ - up to the service provider
○ - Never audited

Reputation

The application must have a reputation among popular users and experts.

● - Highly reputable
○ - Can never be trusted

	VPN	Proxy	Smart DNS	IP Address	Tor
Usability					
Ease of Use	●	◕	◕	●	◕
Speed and Performance	○	○	○	●	○
Device Compatibility	◕	●	●	●	○
Customer Support	◕	◕	◕	NA	◕
Pricing and Value for money	◕	◕	◕	NA	●
Flexibility	●	○	○	○	○
Deployability					
Handle a lot of traffic	●	●	●	NA	○
Availability in user location	●	●	●	●	◕
Easy Setup	●	◕	◕	NA	◕

Software Upgradation	●	○	●	NA	◕
Simultaneous connections	●	●	●	NA	NA
Security					
Encryption Used	●	○	◕	○	●
Protocols Supported	●	○	○	NA	○
No log Policy	◕	◕	◕	○	●
Kill Switch	●	●	○	○	●
Leak Protection	●	○	●	○	●
Audited Security	◕	◕	◕	NA	●
Reputation	●	●	●	○	○

Table: Showing Usability, Deployability and Security Evaluation

- *= Valid, Positive result.* ◕ *= Valid result with certain conditions.* ○ *= Invalid, Negative result. NA = Not applicable.*

References

[1] M. Z. M. B. S. H. W. H. &. K. T. Alizadeh, "Security and Privacy Criteria to Evaluate Authentication Mechanisms in Proxy Mobile IPv6.," *Jurnal Teknologi,* vol. 72, no. 5, 2015.

[2] A. J. A. M. S. Rahel A. Fainchtein, "User Perceptions of the Privacy and Usability of Smart DNS," in *ACSAC*, Austin, TX, USA, 2022.

[3] M. C. H. V. P. F. W. Christopher S Leberknight, "A Taxonomy of Internet Censorship and Anti-Censorship," *ResearchGate,* 2012.

[4] D. Price, "How to Bypass Blocked Sites and Internet Restrictions," MakeUseOf, 14 April 2022. [Online]. Available: https://www.makeuseof.com/tag/how-to-bypass-internet-censorship/.