Network Censorship

Jingbo Cui (A paper written under the guidance of Prof. Raj Jain)

Abstract

In recent years, countries and companies use network censorship technology to censor websites, historical information, and data from people. Although network censorship can maintain national stability, it also raises privacy concerns, hence the emergence of different anti-censorship technologies. This report starts with the contribution of Privacy Enhancements and Assessments Research Group (PEARG) of IETF to network privacy technology and discusses the invasion of Privacy by Pervasive Monitoring. Also, the report analyzes various network censorship technology and anti-network censorship technology. Finally, discuss the range of network censorship from a personal point of view.

Keywords:

Network Censorship, PEARG, Anti-network Censorship, DPI, Filtering, Tor

---

Table of Contents:

---

1 Introduction

Network censorship refers to countries and companies using network censorship technologies to censor the browser websites, histories, and data from people. It raises privacy concerns. Therefore, the Network Censorship Technology and Anti-network Censorship Technology proliferate and compete with each other.

---

2 PEREAG and Pervasive Monitoring

This section will introduce the Privacy Enhancement and Evaluation Study Group (PEARG), and its effort for privacy. Also, it will talk about one common attack on Internet privacy called Pervasive Monitoring (PM).

2.1 PEARG

Whether people support network censorship or not, privacy is a major concern when people use a network. To discuss and review related privacy technologies, the IETF established the PEARG). The PEARG is a general forum and dedicated to maintaining the desired privacy attributes for the network.

While discussing the records of existing privacy enhancement technologies, PEARG will also find and record new privacy enhancement technologies from open sources or academic communities. PEARG also provides a forum to discuss cryptographic and practical aspects of privacy protocols [pearg].

2.2 Pervasive Monitoring

Attacks on people's privacy are everywhere when they use a network. PM is one of these attacks. Through the intrusive collection of protocol artifacts, including application content or protocol metadata, PM enables undifferentiated and widespread surveillance [rfc7258].

Although PM is beneficial in some respects, such as filtering violent elements, anti-spam, the IETF has a clear view of PM as an attack on Internet privacy. Therefore, the IETF works to mitigate PM attacks, thinking that the goal is to increase the estimated cost or make the attacks detectable by making PM expensive through protocols or technologies.

In a word, nowadays people's privacy is under attack everywhere, and PM is one of them. It implements undifferentiated and widespread surveillance. On the other hand, IETF established PEARG to contribute to privacy by establishing forums and introducing new privacy enhancement technologies, and more.

---

3 Network Censorship Technology

In this section, deep packet inspection (DPI), IP Filtering, DNS Filtering, and Keyword Filtering network censorship technologies will be discussed.

3.1 Deep Packet Inspection

DPI is an in-depth detection technology based on data packets. It can detect different network application layer payloads (such as HTTP and DNS) at key points on the network, such as backbone network. The traffic on the link is collected and identified using a predefined policy to detect the payload and determine the validity of the packet [Wagner09]. The data range that DPI technology can detect is shown in Figure1.

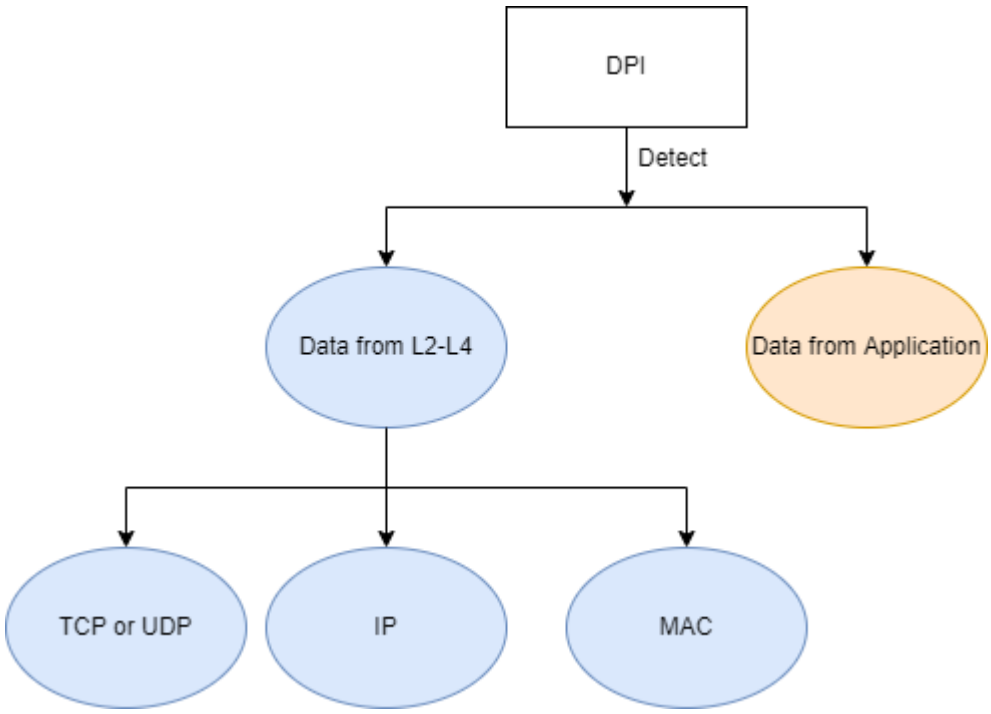

Figure1. Data that DPI can Detect

Although DPI can manage P2P, VoIP, and streaming media, review information security, and monitor public opinion, it infringes users' privacy in these services.

3.2 IP Filtering, DNS Filtering, and Keyword Filtering

Filtering is another common network censorship technology, it contains IP filtering, DNS filtering, and keyword filtering. IP filtering technology can be configured by configuring an IP packet filtering table or proxy server to restrict access and visitors to a specific range. DNS filtering is to specify specific websites and applications at the DNS level so that users cannot access them. Keyword filtering is the setting of a specific keyword value. When information is transmitted, a pre-programmed procedure is used to check whether any keyword is matched, and if so, the transmission is blocked. For example, intelligent moderation will be conducted after the blog is published, and the blog will be blocked if it contains keywords.

Of the three filtering methods, IP filtering is the least expensive, but it is also the least accurate, as it may inadvertently block sites containing valuable sites. Keyword filtering is the most expensive, but at the same time, it has the best filtering accuracy [Leberknigh10].

Filtering is a common method among network censorship technologies. It contains IP Filtering, DNS Filtering, and Keyword Filtering and IP Filtering is the most popular filtering method.

---

4 Anti-network Censorship Technology

This section will talk about several anti-network censorship technologies, including Network Traffic Obfuscation, ScrambleSuit, Browser-based Proxies, User-Generated Content, Infranet, and iCloud Private Relay.

4.1 Network Traffic Obfuscation

Censorship-circumvention system is a general term for traffic disguising technologies that help Internet users circumvent online censorship. When users use a virtual private network (VPN) to communicate, they can use traffic obfuscation technology to hide abnormal traffic from normal traffic, making it difficult to distinguish abnormal traffic [Dixon16].

To be detailed, It can modify multiple traffic characteristics containing traffic content to hide the type of network traffic of the underlying network protocol exchanged between endpoints, such as IP package content, IP package sizes, traffic patterns, protocol behavior, and more [Mazurczyk16].

4.2 ScrambleSuit

Philipp Winter, Tobias Effects, and Juergen Fuss have proposed a low-cost polymorphic network protocol to circumvent censorship called ScrambleSuit. It is applied over TCP to obfuscate transmitted application data by using morphing techniques and a secret exchanged out-of-band. This allows users to defend against active detection and other fingerprint technologies, such as protocol classification and regular expressions, while browsing [Winter13]. Therefore, users can use the ScarmbleSuit based on the Tor to obfuscate the data. The architecture is shown in the figure2 below.

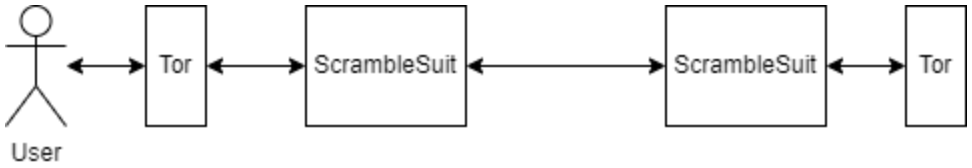

Figure2. ScrambleSuit Architecture

4.3 Browser-based Proxies

When some websites are blocked, people often use proxies outside the censorship zone to get around the censors. But these proxies can be easily stopped if they are discovered. David Fifield, Nate Hardison, Jonathan Ellithorpe, Emily Stark, Dan Boneh, Roger Dingledine, and Phil Porras address this problem by proposing a browser-based proxy creation system that generates many short-lived proxies. The system can seamlessly jump from one agent to the next as the client uses these browser-based agents to appear and disappear [Fifield12].

4.4 User-Generated Content

Sam Burnett, Nick Feamster, and Santosh Vempala explore use the vast deployment of websites that host user-generated content to circumvent network censorship. They developed Collage, which allows users to send data to websites through hidden channels. Using a large number of websites where users can exchange information and a variety of ways information can be hidden, it is difficult for censors to monitor or block such information [Burnett10].

4.5 Infranet

Nick Feamster, Magdalena Balazinska, Greg Harfst, Hari Balakrishnan, and David Karger came up with the Infranet system to allow users to view moderated content through collaborative Web servers distributed across the global Internet. Infranet uses a tunneling protocol to establish a communication channel between clients and servers to provide users with access to censored sites [Feamster02].

4.6 iCloud Private Relay

The iCloud Private Relay is a new way for Apple to protect users' privacy, to ensure that no one knows the website and user's identity when users browse the website. Requests are sent over two separate Internet relays, the first provided by Apple and the second by a third party. During the request, DNS is encrypted, and the IP address passes through the network provider and the first relay to generate a temporary IP from the second relay. At the same time, the second relay is responsible for resolving the site name and connecting to the website [HT212614]. The process is shown in figure3 below.

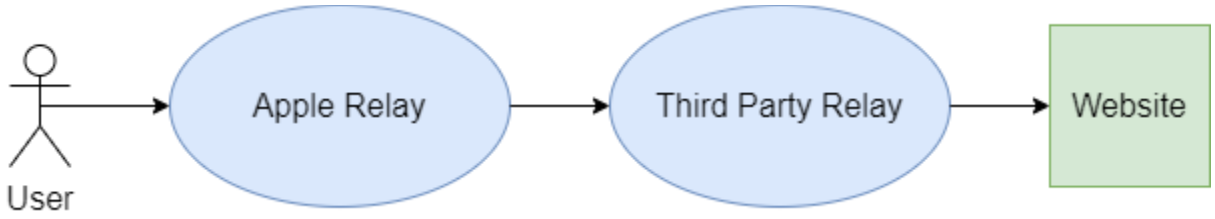

Figure3. Request Process using iCloud Private Relay

5 Competition Between Network Censorship Technology and Anti-network Censorship Technology

Network censorship technology and anti-network censorship technology compete with each other. Whenever a new development is made on one side, the other side is likely to develop new technologies to counter it. This section will discuss the Onion Router (Tor) first. Then mention that China can block the Tor. Finally, talk about CloudTransport to protect privacy.

5.1 Tor

The Tor, for example, is sponsored by The US Naval Research Laboratory, allows users to communicate anonymously over the Internet. Tor can prevent traffic filtering and sniffer analysis and implement anonymous external connections and anonymous hidden services. Tor is encrypted at the application layer of the five-layer protocol stack. The structure is the same as that of the Onion. That is, the transmission between routers is encrypted using the symmetric key, forming a hierarchical structure. After running onion proxy, users can communicate with other tor, thus forming a virtual circuit in the tor network, as shown in figure 4 [wikipedia].

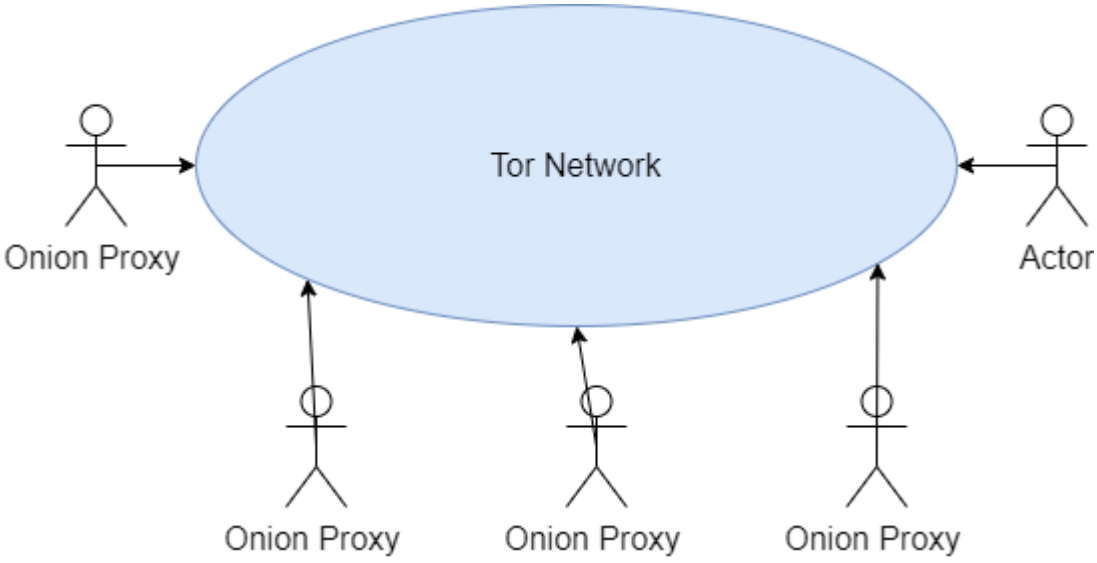

Figure4. Tor Network

5.2 Great Firewall of China Is Blocking Tor

However, the Great Firewall of China can block regular tor. The bridges and relays can be detected and be blocked. Philipp Winter and Stefan Lindskog made an experiment and found that the GFC blocking relays and bridges by IP: port tuples and scan for keywords in inbound and outbound traffic [Winter12]. Figure5 shows the bridge and relay are detected.

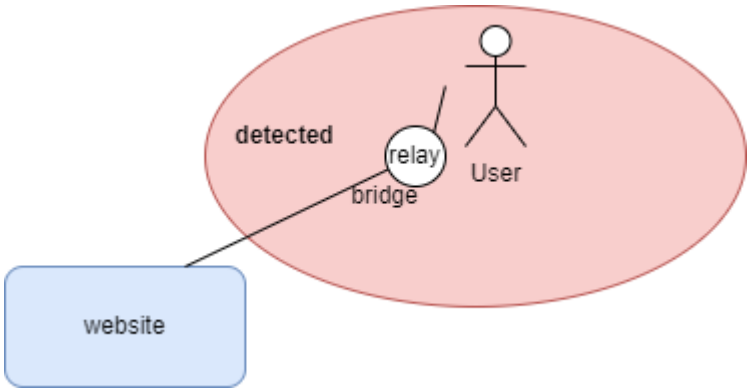

Figure5. Bridge and Relay are Detected

5.3 CloudTransport

Since the traffic generated by using the Onion network is separated from the normal network traffic, it is vulnerable to network-level filtering. To solve this, Chad Brubaker, Amir Houmansadr, and Vitaly Shmatikov came up with CloudTransport, which uses cloud storage services like Amazon S3 to hide users' network traffic. CloudTransport increases the cost of network censorship to protect user privacy, forcing censors to use more expensive forms of network filtering, such as mass traffic analysis [Brubaker14].

In short, technology is evolving, Whenever there is a new development on either side of the technology, the other will try to solve it.

---

6 Future Considerations and Discussion

In some people's opinion, network censorship can check violence, crime, illegal money transactions, and other activities to maintain social stability. In other people's opinion, network censorship violates user privacy rights. As a result, new types of network censorship and anti-network censorship technologies are constantly emerging.

At the same time, each country has a different institutional context, and the situation is constantly changing, new technologies are constantly emerging.

---

7 Summary

Network censorship infringes users' privacy while maintaining social stability, so whether to support network censorship has been debated and new network censorship technologies and anti-network censorship technologies appear constantly. IEFT established PEARG to maintain the desired privacy attributes for the network and to alleviate Pervasive Monitoring. This report discusses Deep Packet Inspection, IP Filtering, DNS Filtering, and Keyword Filtering network censorship technologies. Network Traffic Obfuscation, ScrambleSuit, Browser-based Proxies, User-generated Content, Infranet, and iCloud Private Relay anti-network censorship technologies are discussed. Tor, Great Firewall of China, and CloudTransport are taken as examples to analyze the competition between the two kinds of technologies. Whenever one side has an advantage, the other side tries to solve it.

---

8 References

[pearg] "Privacy Enhancements and Assessments Research Group (pearg)", https://datatracker.ietf.org/rg/pearg/about/ [The background, objectives, service, and collaborations of pearg]

[rfc7258] https://datatracker.ietf.org/doc/html/rfc7258 [The definition of Pervasive Monitoring and the IETF will work to mitigate Pervasive Monitoring]

[Wagner09] B. Wagner, "Deep Packet Inspection and Internet Censorship: International Convergence on an'Integrated Technology of Control'", SSRN, 2009, pp. 3-7, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2621410

[Leberknigh10] C. Leberknigh, M. Chiang, H, Poor and F. Wong, "A taxonomy of Internet censorship and anti-censorship", Fifth International Conference on Fun with Algorithms, 2010, pp. 52-64, http://www.princeton.edu/~chiangm/anticensorship.pdf

[Dixon16] L. Dixon, T. Ristenpart and T. Shrimpton, "Network Traffic Obfuscation and Automated Internet Censorship," IEEE Security & Privacy, Nov.-Dec. 2016, vol. 14, no. 6, pp. 43-53, https://ieeexplore.ieee.org/abstract/document/7782699

[Mazurczyk16] W. Mazurczyk, S. Wendzel, S. Zander, A. Houmansadr and K. Szczypiorski, "Traffic Type Obfuscation," Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures, IEEE, 2016, pp.117-138, https://ieeexplore.ieee.org/document/7440960

[Winter13] P. Winter, T. Pulls, and J. Fuss, "ScrambleSuit: a polymorphic network protocol to circumvent censorship", Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society (WPES '13), 2013, pp. 213-224, https://dl.acm.org/doi/abs/10.1145/2517840.2517856

[Fifield12] D. Fifield, N. Hardison, J. Ellithorpe, E. Stark, D. Boneh, R. Dingledine and P. Porras, "Evading censorship with browser-based proxies", International Symposium on Privacy Enhancing Technologies Symposium, 2012, pp. 239-258, https://link.springer.com/chapter/10.1007/978-3-642-31680-7_13

[Burnett10] S. Burnett, N. Feamster and S. Vempala, "Chipping Away at Censorship Firewalls with User-Generated Content", USENIX Security Symposium, pp.

	463-468, 2010, https://www.usenix.org/legacy/events/sec10/tech/full_papers/Burnett.pdf
[Feamster02]	N. Feamster, M. Balazinska, G. Harfst, H. Balakrishnan and D. Karger, "Infranet: Circumventing Web Censorship and Surveillance", USENIX Security Symposium, 2002, pp. 247-262, https://www.usenix.org/legacy/event/sec02/full_papers/feamster/feamster_html/
[HT212614]	"About iCloud Private Relay", https://support.apple.com/en-us/HT212614 [What is iCloud private relay and how do it protect privacy]
[wikipedia]	"Tor", https://en.wikipedia.org/wiki/Tor_(network) [The definition of Tor]
[Winter12]	P. Winter and S. Lindskog "How the Great Firewall of China Is Blocking Tor", USENIX Free and Open Communications on the Internet (FOCI 12), 2012, pp. 1-7, https://www.usenix.org/conference/foci12/workshop-program/presentation/winter
[Brubaker14]	C. Brubaker, A. Houmansadr and V. Shmatikov, "Cloudtransport: Using cloud storage for censorship-resistant networking", International Symposium on Privacy Enhancing Technologies Symposium, 2014, pp. 1-20, https://link.springer.com/chapter/10.1007/978-3-319-08506-7_1

List of Acronyms

PEARG	Privacy Enhancement and Evaluation Study Group
PM	Pervasive Monitoring
DPI	Deep Packet Inspection
VPN	Virtual Private Network
Tor	Onion Router

Last modified on December 15, 2021
This and other papers on recent advances in networking are available online at
http://www.cse.wustl.edu/~jain/cse570-21/index.html
Back to Raj Jain's Home Page