Proceedings of Informing Science & IT Education Conference (InSITE) 2015

Cite as: Chrane, C., & Kumar, S. A. (2015). An examination of tor technology based anonymous internet. *Proceedings of Informing Science & IT Education Conference (InSITE) 2015,* 145-154. Retrieved from http://Proceedings.InformingScience.org/InSITE2015/InSITE15p145-153Chrane1636.pdf

An Examination of Tor Technology Based Anonymous Internet

Colton Chrane and Sathish Alampalayam Kumar
Coastal Carolina University, Conway, SC, USA

ctchrane@g.coastal.edu, skumar@coastal.edu

Abstract

The concept of Anonymous Internet is getting traction in the wake of recent privacy related NSA (National Security Agency) privacy allegations. Based on our initial findings, Tor appears to be a solution for this and taking control of the Internet and the User’s privacy. Our study reveals that Tor’s power and future ability to thrive revolves around its expansion. Tor needs to grow in size specifically in nodes as well as in software (Torrenting). With the increase in servers and relays in the system as well as few tweaks including a constant shuffling of servers, the more protected a user would be. We plan to put further research and development efforts in Tor to ensure that Tor becomes a viable source for anonymous Internet as well as popular mainstream browser.

Keywords: Anonymous Internet, Tor Browser, Torrent, Information Privacy

Introduction

Internet is one of the greatest and latest technological revolution that we are currently experiencing. Cyberspace has enveloped our lives with the exponential growth in the technology. At the same time, this has caused people to question trust of the government as well as others due to the information security and assurance issues and the rapid proliferation of Information Technology in our day to day activities.

One of the ways to protect information is to keep the information in the Internet anonymous. By anonymous Internet, we mean that the ability to be online in the Internet in a private manner. Tor browsers are growing fast and are at the forefront of anonymous Internet. It uses onion routing technology. The onion routing software helps to keep the information private. Ironically the Tor browser’s inception was due to the efforts of the United States Navy. This eventually led to commercialized use and is now an open-source software for everyone to use. According to Syverson (2005), Onion Routing prevents the transport medium from knowing who is communicating with whom, the network knows only that communication is taking place. Basically what happens in the Internet is a communication between servers. Although in Tor, we see that users are redirected through nodes which are other servers to disguise their IP address so when data is sent between servers your IP address is disguised and thus makes you basically anonymous. Although Tor is not completely anonymous and precautions have to be taken before using and while using to keep your identity hidden. Tor has

Editor: Eli Cohen

obvious weaknesses that must be taken with precaution. According to Johnson, A et al., (2013), Tor is known for vulnerabilities against an adversary that can observe a user's traffic entering and exiting the anonymity network. Quite simple and efficient techniques can correlate traffic at these separate locations by taking advantage of identifying traffic patterns. As a result, the user and their destination may be identified, completely subverting the protocol's security goals.

Basically when the information enters the Tor nodes, information is unencrypted as when the information leaves the Tor nodes, which leaves the information vulnerable. Some fixes include a VPN where instead of an IP; one can use original server and be encrypted by it using a server somewhere else. This can also help one circumvent censorship. Although this is appealing and liberating, Tor has problems with vulnerability to malware, hackers, and compromising one's identity, if one don't follow rules.

The concept of Tor Browser is growing exponentially and hence security concerns are growing as well. This has opened up the community to very liberating experience that we are not used to. Tor Browser can be used for legal and illegal purposes. The user community uses it legally to keep their document and communications to themselves. On the other hand we have people who use it for drug trafficking and child-porn purposes. Tor is a great technology, but it must be applied carefully for whatever reason we use this. According to Misata (2013), citizens are willing to reconsider civil right and liberties in regards to the recent NSA accusations from an anonymous Internet context.

The Tor community is often portrayed in the media as being comprised only of immoral, unjust, and malicious individuals. This could be true considering the borderless cyber world we live in today, and Tor technology is available open source and free. Like other open-source technologies, anyone is free to download Tor. However, we firmly believe that the bad actors in this arena are few and do not make up Tor's core user community. Tor community consists of a wide variety of people, groups, and organizations that all share a common vision: Privacy is important and anonymity has a place in daily life. Journalists often use Tor to communicate more safely with whistleblowers and dissidents. Non-governmental organizations (NGOs) use Tor to allow their employees to connect securely and privately while they're in a foreign country, without notifying everybody nearby who they're working for. Activist groups recommend Tor as a mechanism to maintain civil liberties online; for example, the Electronic Frontier Foundation (EFF) is an open supporter of The Tor Project. Corporations see the value in Tor to conduct competitive analysis safely, protect sensitive procurement patterns from eavesdroppers, and, in some cases, replace traditional VPNs.

Tor needs to be examined to address if Tor is a viable and safe technology for anonymous Internet. Also another question that needs to be examined is does pitfalls of the Tor technologies outweigh its benefits? Tor, although being out only for a decade now, is still young and growing and has to rapidly keep up with the Internet. It is essential that alternatives to torrenting and other ways that may give away your IP needs is to be tested and evaluated. With the growth for a need in anonymous browsing in the private and public sector, this may become a way normal browsers operate such as Internet Explorer and Google Chrome. Another reason for the adoption of the Tor technology could be in countries where Internet censorship is being infringed on the rights of people and they can use this technology and separate themselves, while exploring the open web. This can be achieved through a proper Tor design and infrastructure.

Based on our initial findings, Tor appears to be a solution to the recent NSA allegations and take control of the Internet and the User's privacy. Further study also reveals that Tor's power and future ability to thrive revolves around its expansion. Tor needs to grow in size specifically in nodes as well as in software (Torrenting). With the increase in servers and relays in the system the more protected a user is and also with a few tweak including a constant shuffling of servers.

In order to be taken seriously as a browser and fulfil demographics, Tor must be able to download and use add-ons like BitTorrent and Java.

This paper is organized as follows: the next section provides the background and motivation for our research objective to address the privacy related concerns in the Internet. In the third, we provide our review of literature review of related work. The fourth section provides our research objective, and the fifth section describes our methodology that we have developed for examining the anonymous Internet. The sixth section describes our findings and results. The seventh section provides our reflections on the lessons learned. In the eighth section we provide our plans for the future work. Finally the last section presents the conclusion and summary of the work.

Background and Motivation

The desired properties of the Tor system are as follows:

- Anonymity: The source, destination, and service of any packet should be hidden, except that the first hop ISP will know that it is accepting the packet from/delivering it to one of its customers.
- Censorship-resilience: Neither the system nor any part of it should be censorable. This includes specific services/destinations, ISPs, and any control plane mechanisms like name resolution.
- Net-neutrality: ISPs should not be able to discriminate against a specific source or destination.
- DoS-resilience: Even when DoS attacks take down specific nodes and links, end hosts should be able to communicate with each other. Not only is this a nice property, it is necessitated by the above goals— DoS is a potential tool for censorship, and one would expect that anonymity makes DoS attacks easier.
- Decentralization: The system should not rely on or trust any single point of weakness. This is also necessitated by the above properties, since centralized solutions are easily censorable and doable.
- Minimal Disruption: The system should have minimal impact on the current view of the Internet. For example, path dilation should be small, policy control should be available, and pricing should be similar to the current economic model.

This is a perfect outline of what to expect from Tor and what is perceived to stand in the way of this in the future is congestion and not enough broadband.

Following are some of the safety tips while using and downloading the Tor browser. It is advisable not to torrent over the Tor browser. File sharing through torrenting may cause the application to ignore proxy server settings, which is how Tor hides IP address. This causes people to be able to see one’s IP address thus making one not anonymous. Also another main pitfall is using plugins which can be altered to give away one’s IP address. This would mean one cannot stream videos, music, or play games. So one should never use or install browser plugins basics like Flash and QuickTime. This is due to the fact they can be altered or manipulated into giving away one’s IP address. It is a limitation for the Tor since the commercial Internet use has evolved and leaned more towards the entertainment realm. To address these concerns, Tor and YouTube have released beta versions, that work along with Tor to keep one’s privacy intact. It is also advised not to open or download documents through the browser specifically DOC or PDF files. It is the same method as torrenting as it can cause one’s IP address to be vulnerable and if one were to do it, one should use a 3rd party (non-torrent) application. Another way to increase its security is to build the Tor network a larger network will make it harder for attackers to find a user and thus creating a better anonymous community and avoid Internet censoring. It has been observed that there are numerous loopholes in the Tor technology that can cause eavesdropping and expose one's non-Tor IP address. We must first see its weaknesses and how the infrastructure can be altered as well to further advance this technology.

Review of Related Literature

There are quite a few methods in the literature that address the issue of Anonymous Internet. According to Clark et al., (2007), users inexperienced with Tor will have difficulty with at least one of the core Tor tasks no matter which current deployment option they choose. This causes the most dangerous pitfall in Tor's anonymity to be the user him/herself. Tor should not be taken lightly and it should be researched thoroughly before its use.

Another realm of Tor and its allegations of weakness come from the use on not enough nodes. Nodes are what are used to keep anonymity by relaying you through random servers (nodes) so one's Tor IP is not actually for them and the user is disguised. Although problems arise when not enough nodes are active and use more broadband slowing or causing failure in the system. This is clearly outlined by Liu et al., (2011).

The need for the methods to lead to an ideal Tor browser have been outlined clearly in the literature and the answer of decongestion and broadband control arises multiple times in the literature. First examination of this is outlined by Liu et al., (2011) where they state in order to make this design of the Tor browser more concrete, resource allocation, congestion control, and the interface to higher levels need to be addressed. As per literature, the research shows that problems will arise in Tor's growth if Tor can't keep up with its growth and will implode. Another similar process is to limit broadband usage as it has been termed by Moore et al., (2011) as a "Universal Rate Limit." It would simply give everyone a set broadband limit such that Tor relays aren't overpowered. Through findings, it has been determined that the broadband limit has to be so large that it won't make a difference. Else, it would be lower and the higher broadband user would either have to contribute to the network to get higher broadband usage or use their own relays. This obviously would not be an option to novice Tor users, which could hurt its viability. Although gloomy outcome is discovered by Johnson et al., (2013), who states that the longer you use Tor the more likely you will be compromised. This can be due to reallocating bandwidth to different servers as well as human error. To address these issues, they also propose a solution where users can choose to limit which relays their client will select using manual configuration options (EntryNodes, ExitNodes, ExcludeNodes, etc.). While this does break the uniformity of the path selection among clients, it may be a worthwhile risk tradeoff for these users. Software for the Tor has been released to expand the Tor and help the user community to reach the goal of free and secure Internet. For instance, Mobile OS software as well as software for USB has been released to make Tor portable. Also they have released a software for the cloud storage system so other users can tap into Tor's anonymous Internet and other means to circumvent censorship. This is clearly outlined by Misata, K. (2013).

As seen in Table 1 our review on the related work in the area of Anonymous Internet outlines the issues the related work addresses along with the solutions and limitations of the related work.

Table 1: Related Work on Anonymous Internet

Author/ Source	Issues It Addresses	Solutions	Limitations
Clark, J., Van Oorschot , P. C., & Adams, C. (2007)	Novice users as well as poorly configured Firefox extensions make it difficult to prevent error	Get rid of technical jargon and make a simpler user interface to warn users of Tor dangers	Difficulty for Novice user
Liu, V., Han, S., Krishnamurthy, A., & Anderson, T. (2011)	Can Tor replace IP?	The idea to provide many properties: anonymity, censorship resistance, network neutrality, DoS resilience, decentralization, and consistency with the business structure of the Internet	To make this design more concrete, resource allocation, congestion control, and the interface to higher levels must be discussed, and they leave much of these for future work
Moore, W., Wacek, C., & Sherr, M. (2011)	How to control congestion in Tor bandwidth	Universal Rate Limit	Universal Rate Limit Software isn't compatible with existing infrastructure
Johnson, A., Wacek, C., Jansen, R., Sherr, M., & Syverson, P. (2013)	How congestion and increase in traffic can compromise your anonymity	Manual configuration options to determine node path to keep it original and untraceable	Relies on manual configuration and not automated configuration

Research Objective

Our findings reveal that Tor has severe pitfalls and holes that could compromise one's identity. The purpose of this research is to examine Tor, understand its weaknesses and strengths as well as its future as a browser. Particularly, our research answers the question: Is Tor a viable source for anonymous browsing and could its continued growth along with its already found holes make this a questionable technology for mainstream usage.

Methodology

Following is the methodology that we used to examine the anonymous Internet. In the Figure 1, background research indicates the analysis of the prior experiments and test results that we used to research the nodes in Tor and their usage for anonymous Internet. In addition, they were used to perform the Tor anonymity test and identify the current research pitfalls in Tor. Data collection and analysis is then used to examine and present our findings of the Anonymous Internet using Tor technology. We collected the Tor usage data from the Internet based CollecTor service. We used the data to research the Tor nodes and their usage of the resources

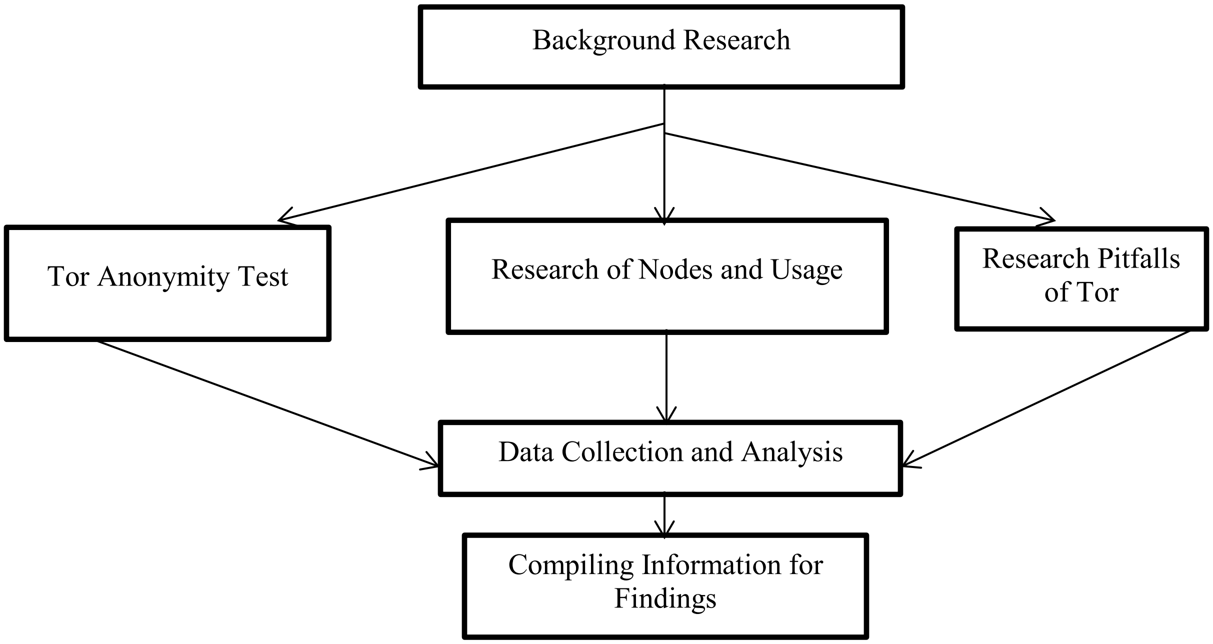

Background Research
Tor Anonymity Test
Research of Nodes and Usage
Research Pitfalls of Tor
Data Collection and Analysis
Compiling Information for Findings

Figure 1. Methodology to examine anonymous Internet using Tor technology

Data Collection and Analysis

To obtain the empirical data we used CollecTor service as well as Tor Metrics services. These services collect data stored by Tor from the users. We utilized the data from these services to quantify Tor's growth, efficiency, as well as bridge and relay descriptions. Analyzing bridge, relay, and Tor population growth gave us an idea of how the growth of Tor directly influences its strength of keeping users anonymous.

Figure 2 indicates the growth of Tor bridges and relays in the last few years. Bridges and relays are integral part of the Tor node system. Relays are the parts of the Tor nodes that keep one anonymous and can be ran from any computer. Bridges are used to circumvent IP addresses and are used in countries like China where relay IP addresses are blocked. As indicated in Figure 3, the population of Tor users is directly influential, because every user goes through the relays and bridges, nodes, to be on the Tor network.

As seen in Figure 2 and 3, in 2015 there was eight thousand relays and four thousand bridges compared to over two million users and each user runs through three relays to be in the network. Although growth is steady and promising the number of bridges and relays are far inferior. This means that it is easier for someone to compromising one's IP address because of a small amount of relays a user can run through. In order for Tor to be viable and used without compromising anonymous security needs, there needs to be a larger pool of relays to increase the list of IP addresses that can be used to keep users unidenifiable.

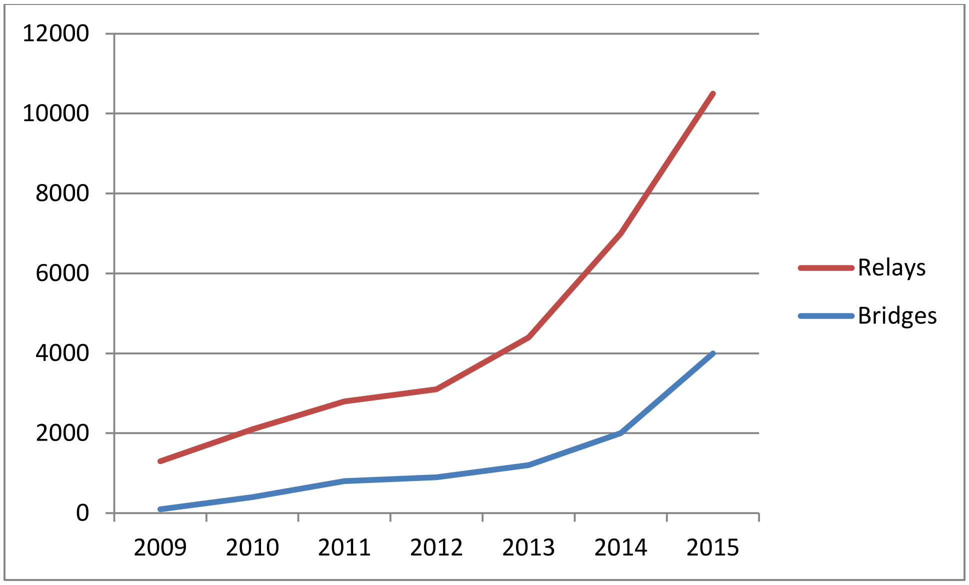


Figure 2. Growth of Tor Relays and Bridges

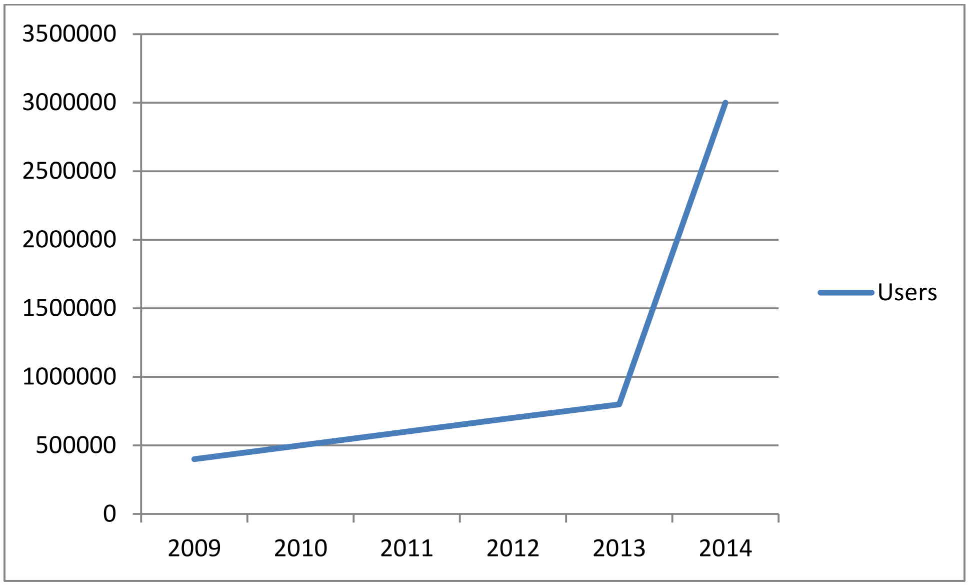


Figure 3. Number of users connected to Tor network over last few years

Findings

Based on our preliminary research and experimentation, Tor has been found to be an anonymous browser, and can have a viable and a strong presence in the future. While experimenting with Tor we found its technological limitations. Tor is dealt with the challenge of growing and fixing its problems when it's ever expanding and growing. Following are our findings, in order for the Tor to serve as an anonymous Internet and for its future as a popular browser:

- Tor must provide consistent anonymity to its user
- Tor must rid of Internet censorship.
- Every device connected to Internet has equal demand and equal priority

- Tor is a great use to stay private in messaging as well as discovering censored resources in the Internet.
- Tor can be used on all levels from the private to the public sector
- To keep Tor running smoothly and to keep bandwidth restrictions there must be as much nodes as possible, which implies the rapid expansion of the Tor network

Lessons Learnt

We found that considering this topic being fairly new, the information and literature on the topic was very low. Also due to controversy and speculations of malicious content we were very cautious on selecting the websites for the experimentation. Although we were cautious, we didn't take right precautions and had to run malware protection on the computer we were experimenting. Although these limitations may have set us back but they ultimately helped us with insights towards the results and findings.

Recommendations for Future Work

In the future, we would like to investigate to incorporate the resource allocation, congestion control features in Tor and better interface based on automated configuration, such that it is accepted as a popular browser by the general public. We would like to experiment more on the effects of a lack of nodes on the bandwidth. In addition, we would like to experiment how torrent affects anonymity as well.

Conclusion

Tor could be a credible Internet browser as well as an anonymous networking tool, if it meets the criteria related to anonymous Internet. To be more viable for a popular browser, Tor browser needs to support a growing demand for plug in support and a novice friendly user interface. This could be the future of the Internet and a solution for the users who allege that NSA is infringing on the citizens' rights. Our background research and experimentations demonstrate that the Tor is an up and coming source in the future of browsing. Our studies demonstrate that Tor is a viable anonymous browser, but lack an infrastructure and R&D efforts that are needed to be a popular browser. Studies indicate that the expansion of the number of nodes using the Tor system would result in a better anonymous Internet experience. We compiled our findings based on the literature review and experimentations related to the anonymous Internet using Tor browsers and their future success. International usage of this system with a global interface would increase the number of nodes and improve the stability of the system. Tor browser has a strong potential for a powerful browser in the future and a strong source for anonymous Internet in the future if it grows faster, optimizes the node server system, and becomes user friendly with a plug in system and user friendly interface.

References

Brookshear, J., & Smith, D. (2012). Networking and the Internet. In *Computer science: An overview* (11th ed.). Boston: Addison-Wesley.

Clark, J., Van Oorschot, P. C., & Adams, C. (2007). Usability of anonymous web browsing: an examination of Tor interfaces and deployability. In *Proceedings of the 3rd symposium on Usable privacy and security* (pp. 41-51).

Johnson, A., Wacek, C., Jansen, R., Sherr, M., & Syverson, P. (2013). Users get routed: Traffic correction on Tor by realistic adversaries. In *Proceedings of the 20th ACM Conference on Computer and Communications Security*, 337-350.

Liu, V., Han, S., Krishnamurthy, A., & Anderson, T. (2011). Tor instead of IP. In *Proceedings of the 10th ACM Workshop on Hot Topics in Networks* (p. 14).

Misata, K. (2013). The Tor project: An inside view. *ACM XRDS: Crossroads*, The ACM Magazine for Students, 45-47.

Moore, W., Wacek, C., & Sherr, M. (2011). Exploring the potential benefits of expanded rate limiting in Tor: Slow and steady wins the race with Tortoise. In *Proceedings of 2011 Annual Computer Security Applications Conference*, 12-12 (ACSAC'11).

Syverson, P. (2005). *Onion routing*. Retrieved November 28, 2014, from http://www.onion-router.net/

Tor Exit Nodes Mapped. (2014). Retrieved November, 2014, from http://hackertarget.com/tor-exit-node-visualization/

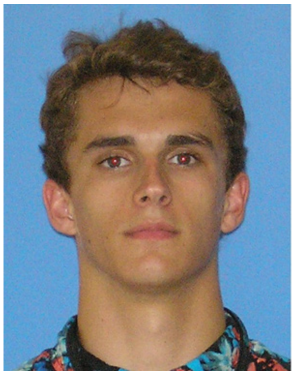
Tor Metrics. (n.d.). Retrieved Feb, 2015, from https://metrics.torproject.org/

Tor research data collection. (2014). Retrieved Feb 2014 from https://collector.torproject.org/index.html#formats

Tor: Overview. (2014.). Retrieved Nov, 2014, from https://www.torproject.org/about/overview.html.en

Welcome to new era of computer hacking basics & much more. (2014). Retrieved Nov, 2014, from http://beginerhack.blogspot.com/2013/08/ultimate-way-to-use-torrent-in-cyberoam_27.html

Biographies



Colton Chrane is a student in Coastal Carolina University, Conway, SC, USA. His research interests are in the field of cybersecurity especially in the area of anonymous and private Internet. He is interested in pursuing research in the area of Information Security and Privacy.

Sathish Alampalayam Kumar received his PhD in Computer Science and Engineering from University of Louisville in 2007. He is currently an Assistant Professor of Computer Science and Information Systems at the Coastal Carolina University, Conway, SC USA. Dr. Kumar's research interests are in the area of information security and data analytics He has published several papers in conference proceedings and journals in the areas of cybersecurity and data analytics.