Summer 8-2018

Building Test Anonymity Networks in a Cybersecurity Lab Environment

John Schriner
CUNY Queensborough Community College, jschriner@qcc.cuny.edu

Building Test Anonymity Networks in a Cybersecurity Lab Environment

John Schriner

John Jay College of Criminal Justice

City University of New York

Author Note:

This is a capstone thesis project towards a Master of Science in Digital Forensics and Cybersecurity.

Correspondence concerning this project should be addressed to John Schriner, Department of the Library, Queensborough Community College, Bayside, Queens 11364

Contact: jschriner@qcc.cuny.edu

Abstract

This paper explores current methods for creating test anonymity networks in a laboratory environment for the purpose of improving these networks while protecting user privacy. We first consider how each of these networks is research-driven and interested in helping researchers to conduct their research ethically. We then look to the software currently available for researchers to set up in their labs. Lastly we explore ways in which digital forensics and cybersecurity students could get involved with these projects and look at several class exercises that help students to understand particular attacks on these networks and ways they can help to mitigate these attacks.

Keywords: anonymity networks, Tor, I2P, digital forensics, cybersecurity

Anonymous Communication Networks (ACNs) have been an essential tool for Internet users wishing to keep their traffic hidden from their ISP, third-party entities, or nation states. Tor Project is a non-profit that develops Tor and the Tor Browser--a hardened browser based on Firefox that limits browser fingerprinting and tracking. Succinctly, using onion routing, Tor routes encrypted traffic over a circuit of three hops to its final destination: no one hop (or node) knows the full picture of the service request. I2P (the Invisible Internet Project) uses garlic routing, which is a variant of onion routing in its method of routing that bundles several messages together. These ACNs are similar in that they are built atop the Internet, but whereas Tor has a centralized directory and is meant to be used to visit clearnet sites and Onion Services (née hidden services), I2P was not designed for exit to the clearnet but rather meant to route to internally-hosted "eepsites" and other I2P services like chat or file-sharing. This is a very large design difference and one we will revisit throughout this paper.

Building test ACNs in a cybersecurity lab environment is essential for the student that needs to know how Tor and I2P work, how they can improve these networks, and how they can test attacks and defense methods in a safe lab environment without affecting the anonymity of real users of the networks.

Tor and I2P are Research-Driven

Research portals for both Tor Project and I2P describe how academic research ought to be conducted to protect users from de-anonymization. Working with the Tor Research Safety Board, a researcher submits answers to the following questions:

> What are you trying to learn, and why is that useful for the world? That is, what are the hoped-for benefits of your experiment?

What exactly is your plan? That is, what are the steps of your experiment, what will you collect, how will you keep it safe, and so on.

What attacks or risks might be introduced or assisted because of your actions or your data sets, and how well do you resolve each of them? Use the "safety guidelines" above to help in the brainstorming and analysis.

Walk us through why the benefits from item 1 outweigh the remaining risks from item 3: why is this plan worthwhile despite the remaining risks? [1]

We discuss the technical options for test networks below, but it is important to note that researchers of the Tor network should work closely with the Tor Research Safety Board. For both Tor research and I2P research, we are asked to use a test network first, and if that's not possible, then to collect our own data and attack our own traffic. Both projects have research teams that work with the researcher in scope and user privacy.

There has been a great deal of research on Tor since 2002, and although this research benefits I2P development and the strength of ACN's in general, I2P project notes that there is a great need for I2P-focused research [2]. Both projects note that although it is enjoyable to figure out offensives against the software and network, more research is needed in defense.

At the time of writing there are 6429 active relays in the Tor network [3] and currently 2,190,301 users [4]. The number of relays has tripled since 2011, when metrics start in the portal [5]. To gather I2P metrics, one has to visit *stats.i2p*, a site only accessible via I2P [6]. The Tin Hat, a known pseudonymous I2P researcher, worked on mapping the I2P network and notes that *stats.i2p* estimates that there are 25,000 routers on the network at any given time [7].

There has been much research comparing Tor and I2P: from the I2P project's perspective [8]; a comparative study [9]; focusing on research highlighting defenses and offenses against both [10];

sophisticated and reproducible traffic classification of both networks [11]; and weighed factors contributing to informed threat modeling [12]. This paper acknowledges that in a cybersecurity lab environment both ACN's ought to be available to the student to study and improve.

Combatting Intrusive Research

In early 2014, the Software Engineering Institute ("SEI") of Carnegie Mellon University (CMU) compromised the Tor network by running malicious relays that manipulated user traffic and it was, according to Tor Project, for the purpose of deanonymizing Tor users and hidden services. The vulnerability was said to be able to unmask new hidden services within two weeks and it led to CMU being subpoenaed by law enforcement for the IPs they collected [13].

We see that the Tor Research Safety Board, in light of the Carnegie Mellon problem, wishes to help researchers by working closely with them along the way and assuring ethical and non-intrusive research:

> **"Can't I just run Tor relays and do my experiment without telling you?** Please don't! The directory authority operators have been much more conservative lately (after the CMU incident in particular) in terms of looking for suspicious patterns or behavior, and removing suspicious relays from the network. If the directory authority operators know about you, understand your research, and can read about why the benefits are worth the risks in your case, they will likely leave your relays in place, rather than surprising you by kicking your relays out of the network mid experiment." [14]

There are worries among researchers of darknet markets that behavior like the quasi-

departmental SEI may lead to a mistrust of researchers from Tor users. Nick Mathewson, a co-founder of the Tor Project, said of the CMU compromise:

> If you're doing an experiment without the knowledge or consent of the people you're experimenting on, you might be doing something questionable—and if you're doing it without their informed consent because you know they wouldn't give it to you, then you're almost certainly doing something wrong. Whatever you're doing, it isn't science [15].

A cybersecurity lab environment with a close connection to the Tor Research Safety Board and I2P developers, alongside an assurance of responsible disclosure, would help cybersecurity students to understand the framework of these networks. It would also be the foundation for ethical research, including attacks and defenses of the networks using ethical methods and reproducible results.

Test Network Software

A lab that wishes to do non-intrusive research with Tor and I2P needs to have a lab environment that either simulates the network, emulates a test network in real time, or runs a parallel private network.

In [16], Shrazi et al. describe the categories of experimentation techniques: a) theoretical modeling (the foundation and necessary component of Tor experimentation) , b) private Tor networks, c) distributed overlay network deployments, d) simulation, and e) emulation. A precise model, such as the one designed in [17] is necessary in order to incorporate the Directory Authorities, relays, bridges, selection of guard nodes, and exit nodes. Sharazi et al. looked specifically at the feasibility and resource requirements of Shadow, TorPS, and ExperimentTor.

Private Tor networks may be deployed using Chutney (currently in alpha), which helps to build and configure the topology of a Tor test network [18]. This requires physical machines or virtual machines so it has limitations in scale. This project is promising, however, as it's actively developed collaboratively with Tor Project.

Some Tor researchers have used distributed overlay networks for Tor research such as Princeton University's PlanetLab and the University of Utah's EmuLab. PlanetLab currently has 1353 nodes across the planet and hosts projects like the Open Observatory for Network Interference [19][20] that measures network censorship globally, and at least two Tor experimentation projects. As noted above, there are over 6000 Tor relays currently, and given the limited resources of shared nodes in the PlanetLab ecosystem and as noted by Shrazi et al. [16], it would be difficult to reproduce results and scale properly using this method. Another network testbed is EmuLab [21] and although it too has been used for Tor research, it suffers the same limitations of resources and scalability.

Shadow with the Tor plugin was first released in 2011 by Jansen and Hopper [22] to efficiently and accurately simulate (or “shadow”) a Tor test network for experimentation on one machine. Shadow is an event simulator with virtual nodes, virtual CPU's with processing delays to mimic real world processing, and virtual cryptographic processing to save expensive cryptographic operations and decrease the experiment's runtime. The Scallion plugin is critical to simulating the Tor network: this plugin intercepts and modifies certain aspects of the network such as state registration and the Tor socket function wrapper, and it changes jobs that would normally spawn new processes for the CPU into events that then uses a single-threaded process. Scallion also uses a set of scripts integral to the live Tor network called TorFlow to measure bandwidth on the network, and Scallion manipulates the bandwidth rate sent to the Directory Authorities to simulate better path selection [22].

Developers of Shadow were able to successfully simulate the live Tor network—in 2011—using consensus data for relay bandwidth from the Directory Authorities while also simulating

geographic location of nodes and their latency from PlanetLab tests they had done previously [22]. As the number of Tor non-bridged users and the number of Tor relays has doubled since Shadow development began, it's essential to re-assess our tools. Tor network bandwidth is currently over 125 Gbit/s but was 7 Gbit/s in 2011 when this software was developed [23]. We will discuss possible class exercises and experimentations below, but certainly updates to our model reflecting the number of Tor users as well as geolocational and bandwidth data would be a necessary experiment for researchers desiring to update our tools for accurate experiments today.

ExperimenTor uses network emulation as a technique for Tor experimentation. ExperimentTor is based on FreeBSD v6.3 or Ubuntu 11.04, both quite outdated. In fact, ExperimenTor has largely been replaced by Scalable Network Emulator for Anonymous Communications (SNEAC) developed in 2014, and similar to ExperimenTor, it requires at least two physical or virtual machines [16]. Recall that emulation methods operate in real time on virtual nodes so these hardware resources may be prohibitive for many labs: in [16] researchers note that Singh's experiment [24] used 8 machines, at least 1 TB of RAM, 80 CPU cores, and 40 Gigabit ethernet interfaces. The clear advantages of using SNEAC are that we a) use unmodified Tor software, b) operate in real time and thus this method may lead to better reproducibility.

As noted above, Tor has dominated the research focus of anonymity network researchers and there is a real dearth of research in test I2P networks. There are two current methods: I2P has a *MultiRouter* mode that may be used on a single machine to virtualize test routers, or a researcher could choose to enable virtual network mode that disables all traffic to focus only on testing the router. Using the live network, Crenshaw in [25] was able to correlate an I2P eepsite with a clearnet version using banner-grabbing. Similarly for the Tor network, misconfigured or leaky web servers may in the future be checked with the OnionScan tool [26]: OnionScan developers are working on supporting the scanning of I2P eepsites, which suffer from many of the same issues as Tor in this regard. The live I2P

network was also used for research in [27] by placing floodfill routers on the network and logging all new leaseset store requests. This one-week experiment lead to statistical data about traffic type and the identification of 181 eepsites and 1350 I2PSnark torrent clients.

From the above detailed methods and software, researchers using their university's cybersecurity laboratories would need to weigh their options. For Tor, given the high hardware requirements of SNEAC, researchers may opt for simulation via Shadow, or even with its limitations of scale, distributed overlay networks like PlanetLab or EmuLab. For I2P, researchers can choose to virtualize routers, or they can work with I2P developers to experiment on the live network safely. We may now turn to experiments that students of cybersecurity, and those interested in anonymity network research in particular, may perform in a test anonymity network environment.

Class Guidelines and Lesson Plans

In this section we'll look into exercises that may be conducted in a laboratory environment with the purpose of discovering how these networks work, how these attacks work, and how attacks are mitigated.

Viewing and compiling code

A cybersecurity lab is a good place to learn how Tor and I2P networks are built. Using versions for various operating systems could help students to identify new software vulnerabilities or view patches for known vulnerabilities of older versions. Students could install from source and review the source code to demystify the software.

Both Tor Browser and I2P are open source so their code is readily available to view. Tor is

written in C and Tor Browser uses a hardened Firefox. I2P is written in Java.

Laboratory experiments in a test anonymity network environment

To those students new to the protocol, viewing network traffic via Wireshark would help them to identify Tor or I2P traffic on a network. Researchers could work on pluggable transports, which are methods for obfuscating Tor traffic by looking like other protocols.

From there students could focus on DoS attacks on critical aspects of the Tor network such as the Directory Authorities, known entry nodes, or discovered bridges. For I2P, Kack [28] demonstrated a variant of the *slowloris* attack known as *darkloris* which initiates many resource-draining requests and quickly uses up all of the server's sockets, rendering the eepsite non-responsive to other users. Simple python scripts like this could be put to the test in a laboratory environment as DoS attacks outside of a lab environment are prone to prosecution under the Computer Fraud and Abuse Act in the United States.

Researchers could test the Onion services for misconfigurations and server leaks using OnionScan [20]. Given a virtualized full-scale Tor test network, researchers may want to focus on de-anonymization attacks via javascript or canvas fingerprinting when users switch to full screen or when they have installed plugins. In a test environment, researchers could run malicious nodes along the circuit without doing real users harm. Exit nodes in a test network could be "bad actors" and log traffic with an effort to de-anonymize—and of course work on mitigations. Ultimately, researchers would join Tor developers to strengthen Tor and provide valuable insight. We want to build Tor test networks so students can learn to attack and defend the network in an effort to strengthen the network and the software that makes it possible.

Router families and attack mitigation

Both Tor and I2P have protections against users' routers/nodes connecting to other nodes in the same /16 network. In Tor, the operator of a node would add a *MyFamily* configuration option [29] so that these nodes will not connect in a single circuit. If two nodes are "too close," then the default configuration is set to *EnforceDistinctSubnets* [30]. I2P introduced Router Family configuration in 2016 and the I2P project notes that having this option has two good effects: it allows researchers to publicly identify their routers, and it helps I2P project to know that the researchers are not running an attack on the network:

> It also will prevent other routers from including multiple routers of the family in a single tunnel, which could lead to de-anonymization. Routers that appear to be colluding but do not have a declared family may be assumed to be an attack on the network, and may be blocked. The best way to ensure the success of your research project is to work with us directly [1].

Students in an anonymity network class would work on identifying family routers on the network and those that collude to de-anonymize users by trying to run their own nodes in a circuit.

Sybil attacks on I2P

Similarly, a test I2P network would allow researchers to look into Sybil attacks as described by Timpanaro et al. in [31]. They found that to successfully place malicious peers next to a particular key, an attacker would need to generate 12K fake routing keys to properly perform the attack, computed in just a few minutes with moderate hardware. The researches offer improvements to netDB including

increasing the replica set from 3 to 10 peers making an Eclipse attack exponential more costly in terms of processing time.

User agents and canvas fingerprinting

The user agent of a browser in the I2P network is spoofed to the same Firefox user agent as Tor Browser for outproxying [32][33] and "MYOB/6.66 (AN/ON)" for internal eepsites [32]. Leaving users the choice of browser presents a whole set of issues around errant javascript, installed plugins, use of a particular browser over time, and canvas fingerprinting. Researchers in a laboratory environment could set up eepsites and determine if a visitor's user agent or unique attributes set them apart. Similarly to how Tor addresses canvas fingerprinting linkability [34], researchers of both I2P and Tor could take into account fingerprinting methods such as HTML 5 Canvasing: Tor Project says it is "the single greatest fingerprinting threat browsers face today" [34] because even subtle differences in video card, font packs, and library versions rendered by WebGL could be hashed and provide a unique identity for a machine with the user unaware. As a browser can leak screen resolution to a server, Tor Browser warns the user not to maximize their window. Laboratory researchers could use the Electronic Frontier Foundation's Panopticlick [35] tool to look into HTML 5 Canvasing and other fingerprinting methods.

I2P forensics research

There has been some research into forensic analysis of I2P activities in [36] focusing on peer-to-peer (p2p) file-sharing and the differences from clearnet p2p protocols and traditional forensics work. Besides artifacts and detection of I2P software via known hash sets or comparisons of possibly

unique *addressbooks*, the authors note the difficulties present in forensics work. Bazli, Wilson, and Hurst expanded on this work in [37] noting that attacks on the network could originate with taking over existing registers like 'NO.I2P' which functions as a domain name register node. The authors suggest this method as well as mirroring other eepsites and collecting data on visitors. Clearly, these methods fail to respect user privacy if they are misleading users to visit errant sites.

Researchers in an I2P test laboratory could work on mirroring eepsites and working with I2P developers and registrars to make malicious spoofing/cloning of websites more difficult to accomplish. Researchers could also work with I2P developers and name resolution registers to have better methods of establishing trust and consensus on Base32 addresses so that users are directed to the correct destination.

Tor Project currently offers a few research ideas that will help the project [38] and help cybersecurity researchers to get involved.

Future work and conclusions

Future work in this area will include updating our tools and models with current numbers of users and relays/routers in these networks. A tool like SNEAC looks promising and we look forward to more research using this tool for emulation of the whole Tor network. Future work will include emulating and simulating the I2P network so fewer researchers use the live network for their attack experiments. As researchers in anonymity tools move to compartmentalization the secure integration of tools onto one machine such as Qubes [39] or SecureDrop [40], we will see more scalable tools on one machine that could be deployed in a laboratory with little overhead.

Laboratory administrators and students should take into consideration the above options for test networks and create something useful for their continuing research. By working closely with Tor

Project's Research Safety Board and I2P developers, researchers can connect with others doing similar work and working through scale or reproducibility issues. In close cooperation with these projects we can be assured to do research that respects user privacy and leads to better and more secure software.

References

[1] Tor research safety board. (n.d.). Retrieved July 28, 2018, from https://research.torproject.org/safetyboard.html

[2] Academic research - I2P. (n.d.). Retrieved July 28, 2018, from https://getI2P.net/en/research

[3] Tor Atlas. (2018, July 17). There are currently 6429 #Tor relays running providing 31.7 GiB/s total bandwidth. https://metrics.torproject.org/networksize.html …pic.twitter.com/WqObNPUAAL [Tweet]. Retrieved July 17, 2018, from https://twitter.com/TorAtlas/status/1019174047723261953
n.b. These statistics can also be found at Tor Metrics and by viewing the daily CSV file: https://metrics.torproject.org/networksize.html

[4] Users – Tor metrics. (n.d). Retrieved July 17, 2018, from https://metrics.torproject.org/userstats-relay-country.html

[5] Servers – tor metrics. (n.d.). Retrieved July 28, 2018, from https://metrics.torproject.org/networksize.html?start=2011-01-01&end=2018-07-17

[6] Stats (n.d.) Retrieved July 17, 2018, from http://stats.I2P/cgi-bin/dashboard.cgi

[7] Through a network, darkly | a geographic look at I2P. (n.d.). Retrieved July 28, 2018, from https://thetinhat.com/blog/thoughts/i2p-survey.html

[8] I2P compared to Tor - I2P. (2016, November). Retrieved July 17, 2018, from https://getI2P.net/en/comparison/tor

[9] Ali, Khan, Saddique, Pirzada, Zohaib, Ahmad, & Debnath. (2016). TOR vs I2P: a comparative study. *Industrial Technology (ICIT), 2016 IEEE International Conference on,* 1748-1751.

[10]Haughey, Epiphaniou, & Al-Khateeb. (2016). Anonymity networks and the fragile cyber ecosystem. *Network Security, 2016*(3), 10-18.

[11]Montieri, Ciuonzo, Aceto, & Pescape. (2017). Anonymity services Tor, I2P, JonDonym: classifying in the dark. *Teletraffic Congress (ITC 29), 2017 29th International, 1*, 81-89.

[12]Shahbar & Shirazi. (2014). Weighted factors for measuring anonymity services: a case study on Tor, Jondonym, and I2P | faculty of computer science. (n.d.). Retrieved July 17, 2018, from https://www.cs.dal.ca/research/techreports/cs-2017-01

[13]Cox, J. (2016, February 24). Confirmed: Carnegie Mellon University attacked Tor, was subpoenaed by feds. Retrieved June 8, 2018, from https://motherboard.vice.com/en_us/article/d7yp5a/carnegie-mellon-university-attacked-tor-was-subpoenaed-by-feds

[14]Tor research safety board. (n.d.). Retrieved July 18, 2018, from https://research.torproject.org/safetyboard.html

[15] Cox, J. (2015, November 12). Academics “livid,” “concerned” over allegations that CMU helped FBI attack Tor. Retrieved June 8, 2018, from https://motherboard.vice.com/en_us/article/8q899v/academics-livid-concerned-over-allegations-that-cmu-helped-fbi-attack-tor

[16] Shirazi, F., Goehring, M., & Diaz, C. (2015). Tor experimentation tools. Security and Privacy Workshops (SPW), 2015 IEEE, 206-213.

[17] Methodically modeling the tor network | Usenix. (n.d.). Retrieved July 20, 2018, from https://www.usenix.org/conference/cset12/workshop-program/presentation/jansen

[18] Chutney: unofficial Git repo. (2018). Python, Tor Project — Unofficial repositories. Retrieved from https://github.com/torproject/chutney (Original work published 2013)

[19] Projects | planetlab. (n.d.). Retrieved July 20, 2018, from https://www.planet-lab.org/db/pub/slices.php

[20] Ooni probe - m-lab. (n.d.). Retrieved July 20, 2018, from https://www.measurementlab.net/tests/ooni/

[21] Emulab. Net - emulab - network emulation testbed home. (n.d.). Retrieved July 20, 2018, from https://www.emulab.net/

[22] Jansen, R., & Hopper, N. (2012). Shadow: running tor in a box for accurate and efficient experimentation. Presented at the Symposium on Network and Distributed System Security (NDSS), U.S. Naval Research Laboratory. Retrieved from https://www.nrl.navy.mil/itd/chacs/jansen-shadow-running-tor-box-accurate-and-efficient-experimentation

[23] Traffic – tor metrics. (n.d.). Retrieved July 29, 2018, from https://metrics.torproject.org/bandwidth.html?start=2012-01-01&end=2018-07-29

[24] Singh, S. (2014). Large-scale emulation of anonymous communication networks. Retrieved from https://uwspace.uwaterloo.ca/handle/10012/8642

[25] Darknets and hidden servers: identifying the true IP/network identity of I2P service hosts. (2011). Retrieved July 28, 2018, from https://www.irongeek.com/i.php?page=security/darknets-I2P-identifying-hidden-servers

[26] Onionscan. (n.d.). Retrieved July 28, 2018, from https://onionscan.org

[27] Timpanaro, J., Isabelle, C., Olivier, F. Monitoring the I2P network. [Research Report] RR-7844, INRIA. 2011. Retrieved July 27, 2018, from https://hal.inria.fr/hal-00653136/document

[28] Kejsarmakten | Layer 7 DOS against I2P darknet. (2016, October 12). Retrieved July 28, 2018, from https://web.archive.org/web/20161012150751/blog.kejsarmakten.se/all/projects/2012/09/11/dark-loris.html
n.b. the original website is not available but it was archived by the Internet Archive

[29] Tor Project. (n.d.). Tor project: faq. Retrieved July 28, 2018 from

References

https://www.torproject.org/docs/faq.html.en#MultipleRelays
[30] Tor Project. (n.d.). Tor Project: manual. Retrieved July 28, 2018, from https://www.torproject.org/docs/tor-manual.html.en
[31] Timpanaro, J., Cholez, T., Chrisment, I., & Festor, O. (2015). Evaluation of the anonymous I2P network's design choices against performance and security. *Information Systems Security and Privacy (ICISSP), 2015 International Conference on,* 1-10. Retrieved July 26, 2018 from https://ieeexplore.ieee.org/document/7509929/
[32] 2163 (Expose user-agent strings for HTTP proxy in Tunnel Manager configuration) – I2P bugtracker. (n.d.). Retrieved July 29, 2018, from https://trac.I2P2.de/ticket/2163
[33] Darknets and hidden servers: Identifying the true IP/network identity of I2P service hosts. (n.d.). Retrieved July 29, 2018, from https://www.irongeek.com/i.php?page=security/darknets-i2p-identifying-hidden-servers
[34] The design and implementation of the tor browser [draft]. (n.d.). Retrieved July 29, 2018, from https://www.torproject.org/projects/torbrowser/design/#fingerprinting-linkability
[35] Panopticlick. (n.d.). Retrieved July 29, 2018, from https://panopticlick.eff.org/
[36] M. Wilson and B. Bazli, "Forensic analysis of I2P activities," *2016 22nd International Conference on Automation and Computing (ICAC)*, Colchester, 2016, pp. 529-534. doi: 10.1109/IConAC.2016.7604974 Retrieved July 28, 2018 from https://ieeexplore.ieee.org/document/7604974/
[37] Behnam Bazli, Maxim Wilson & William Hurst (2017) The dark side of I2P, a forensic analysis case study, Systems Science & Control Engineering, 5:1, 278-286, DOI: 10.1080/21642583.2017.1331770 Retrieved July 28, 2018 from https://www.tandfonline.com/doi/abs/10.1080/21642583.2017.1331770
[38] Tor research: research ideas. (n.d.). Retrieved July 27, 2018, from https://research.torproject.org/ideas.html
[39] Qubes OS: A reasonably secure operating system. (n.d.). Retrieved July 30, 2018, from https://www.qubes-os.org/
[40] The road towards an integrated SecureDrop Workstation. (n.d.). Retrieved July 29, 2018, from https://securedrop.org/news/road-towards-integrated-securedrop-workstation/