R210 Essay: Anonymity Systems

Chongyang Shi (*cs940*)

February 16, 2018

1 Summaries of research

Danezis et al. [1] developed the Mixminion anonymous mailing protocol, building on earlier protocols including Mixmaster [2] and Babel [3]. Mixminion implemented several highly influential features present in future anonymity systems, such as indistinguishable message types, TLS-based forward anonymity, key rotation, and centralised directory servers. After discussing de-anonymisation attacks enabled by pitfalls in predecessors' designs, the authors set out how they designed Mixminion in accordance with their new security and usability goals, most notably the use of a crossover header swap to counter active tagging attacks. Further considerations were given regarding Mixminon's abuse mitigation features and the positive and negative impacts of centralising information distribution through directory servers. The authors concluded with suggestions on future work, some of which have been undertaken by the Tor project as followed.

Designed by Dingledine et al. [4], Tor is an improved version of the Onion Routing anonymity protocol, which utilises multiple layers of encryption and hash checking to maintain authenticity and privacy during multi-hop routing. Rather than specialising for mailing anonymity, Tor is a generic protocol which can efficiently anonymise most TCP applications with minimal interfacing. In comparison with Onion Routing, Tor further implements perfect forward secrecy against replay attacks, allows hidden services to be hosted through in-network rendezvous, and is more resilient against de-anonymisation and denial-of-service active attacks by designating Guard Nodes and throttling. The Tor Browser Bundle provides excellent usability and additional protections against information leak to end users. The authors also noted the wider social impacts of anonymity systems. As an updated technical report, more up-to-date evaluations on network performance would have been a useful addition.

Murdoch [5] introduced a covert channel attack based on clock skews caused by actively induced changes in system temperature. The temperature-sensitive nature of clock crystals in modern computers was utilised as side-channel information in this attack, which characterised constant and varying clock skews through linear fitting on data points obtained from TCP timestamps. Tested to be effective in identifying servers ultimately hosting hidden services, the attack can also be generalised for use against other anonymity systems. Murdoch also examined the possibility of facilitating across-air-gap information leakage and geolocation fixing with this attack's methodology. Finally, Murdoch concluded with discussions on possible mitigations and future work. While the Tor network did not directly influence components in the experiment, possible CPU interference from running periodic-task-heavy directory servers on the same hardware as Tor nodes, and more complex conditions in the noisy public network (e.g. BGP) could affect the accuracy of this attack in a real environment.

2 Key themes of research

2.1 Active attacks pose a more tangible threat to anonymity systems

While the threat models of both Mixminion and Tor explicitly accept the inevitable feasibility of passive traffic-confirmation attacks by adversaries with sufficiently large surveillance power, extensive countermeasures had to be implemented in the protocols to protect against active attacks. Danezis et al. [1, Sec. 2] considered possible attacks from compromised nodes in prior protocols, and designed Mixminion to be resilient against tagging and replay attacks. Similarly, key rotation and designated Guard Nodes formed parts of an imperfect solution to active attacks in Tor [4, Sec. 7], still requiring additional tools to ensure anonymity. Some active attacks over unconventional channels can be even harder to mitigate, such as the clock skew-inducing attack by Murdoch [5].

2.2 Usability is the key to the success of an anonymity system

A consensus among anonymity system developers is that it must be sufficiently easy for users to adapt to an anonymity system, and for node operators to minimise their risk from abuse. This was ingrained in Mixminion [1, Sec. 3] as a design goal, and was achieved in Tor through its browser bundle [4, 4.5]. Customisable exit policies to reduce abuse complaints are present in both systems [1, 5.3][4, 6.2]. Prohibitive cost of more stable OCXO clocks [5, 4.2] hinders a possible mitigation of Murdoch's attack. Additionally, good usability for both clients and node operators can encourage popularisation of the anonymity system, which may be important to security as discussed below.

2.3 Anonymity through herd effect

By design, anonymity of clients within such a system depend on significant variance in possible routes a connection can take, which requires large numbers of nodes and peers to be present in the network. It would be significantly easier for both passive and active attackers to de-anonymise users or disrupt operation in a smaller-than-designed network, as seen in Mixminion through low crossover depth [1, 4.3], and in Tor through compromised entry nodes [4, Sec. 7]. Significant variance in routes may also complicate practical deployments of Murdoch's attack [5].

3 Ideas in current context

Website fingerprinting was raised by Dingledine et al. [4, Sec. 7] as a significant passive attack threat to Tor. The feasibility of website fingerprinting was systematically confirmed by Wang and Goldberg [6] recently, following a long trail of researches in this area. Relatively effective server-side and client-side countermeasures to Tor website fingerprinting attacks have been developed by Cherubin et al. [7]. This new arms race attracts further research.

Tor introduced the capability for services with undisclosed origins to be hosted and accessed anonymously [4, Sec. 5]. In addition to its intended use, the capabilities of hidden services led to various illicit websites being hosted within the Tor network. The most famous case was Silk Road, an illegal substance trading platform facilitated through cryptocurrencies. The platform was eventually took down and its owner arrested, however not due to effective attacks on the Tor network or even covert channel attacks like Murdoch's [5], but rather through social engineering [8]. The ethics of provisioning hidden service technologies is under debate.

Also designed to be a counter-censorship tool, the Tor network contains unannounced bridge nodes, whose connections can be obfuscated via pluggable transport (PT) tools [4, p. 17], which apply pseudo-random transformation or protocol mimicry to Tor traffic. A number of PT tools have been deployed and integrated into the browser bundle. However, Wang et al. [9] demonstrated that all deployed PT's traffic can still be identified by censors with relatively trivial effort and false positive rate. My ongoing MPhil project looks further into the quality of PT obfuscations, and generalises attacks against these obfuscations.

4 Literature review

In addition to Tor [4] itself, the design of Mixminion [1] has had lasting impact on many other anonymity systems and adversary researches thereof. Hopper et al. [10] noted some advantages of high-latency systems headed by Mixminion comparing to low-latency systems, as well as further efforts to improve their security. Danezis and Mittal [11] later developed an algorithm to label nodes in a Mixminion-style network for likelihoods of control by an active attack adversary. Mixminion was also suggested by Ben-Sasson et al. [12] as a possible additional anonymity layer in their anonymous Bitcoin ledger system.

Dingledine et al. [4] very comprehensively considered possible attacks against Tor in their initial publication. New attacks within Tor's threat model emerged during more than a decade of use, including shared-path congestion analysis by Murdoch and Danezis [13], its bandwidth amplification variant by Evans et al. [14], as well as a compromised exit node attack by Ling et al. [15]. Other suggested uses for Tor's protocol design include anonymised malware infection reporting by Gu et al. [16].

Murdoch's covert channel attack [5] headed a set of side-channel active attacks against anonymity systems, as summarised by Zander et al. [17]. Eckersley [18] studied how measurable subtle variations exploited by these attacks can also be used for web browser fingerprinting. In developing wireless fingerprinting techniques, Desmond et al. [19] considered intentionally altering processor temperature as a mitigation to Murdoch's attack, conceptualising mitigations for other covert channel attacks.

(1202 words according to texcount.)

References

[1] G. Danezis, R. Dingledine, and N. Mathewson, "Mixminion: Design of a type iii anonymous remailer protocol," in *Security and Privacy, 2003. Proceedings. 2003 Symposium on.* IEEE, 2003, pp. 2–15.

[2] U. Möller, L. Cottrell, P. Palfrader, and L. Sassaman, "Mixmaster protocol—version 2," *Draft, July*, vol. 154, p. 28, 2003.

[3] C. Gulcu and G. Tsudik, "Mixing e-mail with babel," in *Network and Distributed System Security, 1996., Proceedings of the Symposium on*. IEEE, 1996, pp. 2–16.

[4] S. M. P. S. Roger Dingledine, Nick Mathews, "Tor: The second-generation onion router," Tor Project, Tech. Rep. DRAFT v1, January 2014.

[5] S. J. Murdoch, "Hot or not: Revealing hidden services by their clock skew," in *Proceedings of the 13th ACM conference on Computer and communications security*. ACM, 2006, pp. 27–36.

[6] T. Wang and I. Goldberg, "On realistically attacking tor with website fingerprinting," *Proceedings on Privacy Enhancing Technologies*, vol. 2016, no. 4, pp. 21–36, 2016.

[7] G. Cherubin, J. Hayes, and M. Juarez, "Website fingerprinting defenses at the application layer," *Proceedings on Privacy Enhancing Technologies*, vol. 2017, no. 2, pp. 186–203, 2017.

[8] N. Popper, "The tax sleuth who took down a drug lord," December 2015. [Online]. Available: https://www.nytimes.com/2015/12/27/business/dealbook/the-unsung-tax-agent-who-put-a-face-on-the-silk-road.html

[9] L. Wang, K. P. Dyer, A. Akella, T. Ristenpart, and T. Shrimpton, "Seeing through network-protocol obfuscation," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015, pp. 57–69.

[10] N. Hopper, E. Y. Vasserman, and E. Chan-Tin, "How much anonymity does network latency leak?" *ACM Transactions on Information and System Security (TISSEC)*, vol. 13, no. 2, p. 13, 2010.

[11] G. Danezis and P. Mittal, "Sybilinfer: Detecting sybil nodes using social networks." in *NDSS*. San Diego, CA, 2009, pp. 1–15.

[12] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," in *Security and Privacy (SP), 2014 IEEE Symposium on*. IEEE, 2014, pp. 459–474.

[13] S. J. Murdoch and G. Danezis, "Low-cost traffic analysis of tor," in *Security and Privacy, 2005 IEEE Symposium on*. IEEE, 2005, pp. 183–195.

[14] N. S. Evans, R. Dingledine, and C. Grothoff, "A practical congestion attack on tor using long paths." in *USENIX Security Symposium*, 2009, pp. 33–50.

[15] Z. Ling, J. Luo, W. Yu, X. Fu, D. Xuan, and W. Jia, "A new cell counter based attack against tor," in *Proceedings of the 16th ACM conference on Computer and communications security*. ACM, 2009, pp. 578–589.

[16] G. Gu, P. A. Porras, V. Yegneswaran, M. W. Fong, and W. Lee, "Bothunter: Detecting malware infection through ids-driven dialog correlation." in *USENIX Security Symposium*, vol. 7, 2007, pp. 1–16.

[17] S. Zander, G. Armitage, and P. Branch, "A survey of covert channels and countermeasures in computer network protocols," *IEEE Communications Surveys & Tutorials*, vol. 9, no. 3, pp. 44–57, 2007.

[18] P. Eckersley, "How unique is your web browser?" in *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, 2010, pp. 1–18.

[19] L. C. C. Desmond, C. C. Yuan, T. C. Pheng, and R. S. Lee, "Identifying unique devices through wireless fingerprinting," in *Proceedings of the first ACM conference on Wireless network security*. ACM, 2008, pp. 46–55.