Extended Abstract: Enabling Limited Identity Recovery in Anonymity Networks

Eric Wagner
RWTH Aachen University
eric.michel.wagner@rwth-aachen.de

1 Introduction

In 2013, Edward Snowden showed the world that governments never abandoned their stance against strong encryption for the public [1]. In the past, governments attempted to dictate backdoors or outright ban strong encryption. Over the years, the focus of this war on cryptography shifted towards finding and integrating weaknesses in widely deployed cryptographic protocols. These efforts were conducted behind closed doors, such that the public's awareness of these practices only started rising after Snowden's revelations [2]. This public awareness led to a steady increase in the use of encryption on the Internet. As a consequence, voices about law enforcement agencies (LEAs) being ineffective at fighting crimes (*e.g.,* terrorism and child pornography), due to the use of cryptography, rise again.

In actuality, it is doubtful that governmental backdoors into encryption protocols would help to significantly reduce such illegal activities while these do significantly reducing everyone's privacy. However, there is nevertheless some merit to the positions that some form of *exceptional data access* for LEAs could significantly benefit society, as long as large-scale surveillance is prevented. Hence, one has to wonder if there can exist technical solutions that benefit both sides of this debate. "Exceptional data access" is here used as the general term that comprises all methods that allow accessing data in exceptional cases that would otherwise remain hidden; these methods include, but are not limited to, backdoored encryption. By analyzing current research in this domain, we conclude that backdooring encryption for in-transit data is not feasible. However, we show that integrating exception data access into anonymity networks offers a novel and compelling target for such mechanisms. In the end, such measures could even increase the privacy of honest people.

Anonymity networks obscure the origin of Internet traffic and thereby provide anonymity to their users. Tor [3] is the most popular anonymity service and attracts many users, which in turn boosts the anonymity of each participant [4]. Tor is a crucial tool for privacy-aware citizens, journalists, whistleblowers, and the military, which proves the importance of keeping such networks alive [5]. Unfortunately, this strong anonymity also attracts criminals. Anonymity networks like Tor escalate the power of encryption because, in addition to hiding what is communicated, they also conceal who is talking to whom. Tor hence also serves as the primary catalyst for illegal activities on the Internet [6]. This association with illegal activities damages the image of Tor, which, in turn, holds honest citizens back from using the network. A mechanism for restricted identity recovery in exceptional cases could remedy this situation by preventing crime and making such networks more attractive for honest users. Anonymity networks offer an excellent target for exception data access for another reason; criminal organizations can hardly spin up a custom solution because the network's effectiveness scales with the number and diversity of its participants [4].

One of our main contributions is the design of an anonymous authentication protocol, which we integrated into a novel anonymity network. This protocol establishes threshold-encrypted identities for circuits in a decentralized fashion whenever a client uses the network. The encrypted identities are only accessible through the collaboration of a trusted consortium, that has to approve each request by LEAs, and the exit relays of Twisd. This consortium is assembled of governments, privacy advocates, and cooperation, which prevents collusion and enables proper public oversight. Utilizing a consortium instead of cryptographic puzzles adds flexibility beyond rate-limiting to this process, which is crucial to protect high-profile individuals from deanonymizations. Technical oversight is nonetheless still necessary to assure that this consortium acts in the public's interest. However, mission-critical data has to stay confidential to not interfere with ongoing investigations. To address this problem, we introduce the concept of translucent blockchains. Translucent blockchains permit temporal confidentiality for both immutable storage and distributed computations, while still allowing the revelation of selected data and statistics in real-time.

2 Major Requirements for Exceptional Data Access

Several exceptional data access mechanisms with three major targets for governments were proposed over the years. First, there is backdoored access to in-transit data, which gives governments the ability to decrypt and listen in on encrypted communications. Offering governments with such tools have already been discussed in the 1990s, but eventually, their realization was abandoned by governments due to public opposition [7]. Approaches to limiting access to this data rely either on governments solving cryptographic puzzles for each data access [8] or on probabilistically limiting the amount of data the government has access to [9]. However, the necessary building blocks for secure communications are in the public domain, which makes it easy for well-funded terrorist organizations to forgo the risk of being spied upon [1]. As a result, any general backdoor into cryptography will rather be a tool for (large-scale) surveillance instead of uncovering illegal activities, especially since it is practically impossible to build a secure solution at the necessary scale [7].

A second, more recent, research topic is governmental access to data at rest[10, 11]. This covers the ability of LEAs to unlock, e.g., mobile phones, in exceptional cases. A major advantage of targeting hardware with exceptional data access is that data access is easily limited and transparent by requiring physical access to the device. In the end, having access to a device also unlocks access to the communications done with this device, thus not limiting the amount of information that can be retrieved from a targeted individual. Current proposals in this domain demand prolonged device access by LEAs in combination with an external confirmation of the lawful device access, either by the device's manufactures [10], or by other device owners [11]. The main limitation of this approach is that suspect devices first have to be identified and located, which can be non-trivial.

A third approach for exceptional data access is restricted identity recovery in anonymity networks. Despite criminals clearly abusing anonymity on the Internet, thus far, hardly any research has been conducted in this domain. The little work that has been published [12, 13, 14] is not sufficiently protecting the privacy of law-abiding citizens and offers limited scalability. The privacy risks in the current solutions stem from limited oversight, not enforcing an ethical target selection, not protecting adequately against collusion attacks, and exposing the network operators to political pressure. This lack of adequate solutions to this problem emphasizes that providing LEAs with tools to prosecute criminals without impairing law-abiding citizens is a challenging problem.

Overall, we can say that current solutions towards exceptional data access lack at least one of two crucial features: (1) translucency towards outside observers or (2) enabling the public, but not individuals, to abandon them. If one of these features is missing, governments can abuse the system to enable large-scale surveillance. Because anonymity networks received hardly any attention in the context of exceptional data access, current proposals are lacking, although such a network could even boost the effective privacy of the ordinary Internet user.

3 Our proposal: Twisd

To remedy the current lack of research on anonymity networks with exceptional data access, we propose Twisd — Tor with Integrated Selective Deanonymization — an anonymity network based on Tor that enables the recovery of client identities in justified cases. Twisd is not meant as a replacement for Tor, but rather as an alternative that could be deployed alongside Tor. Such a deployment would offer those people that currently shy away from using Tor, due to its association with criminal activities, a tool to also gain anonymity on the Internet. Twisd has however, the potential to attract many more users than Tor, which means that it could offer better anonymity due to its larger user base [4]. Thus, Twisd could also attract

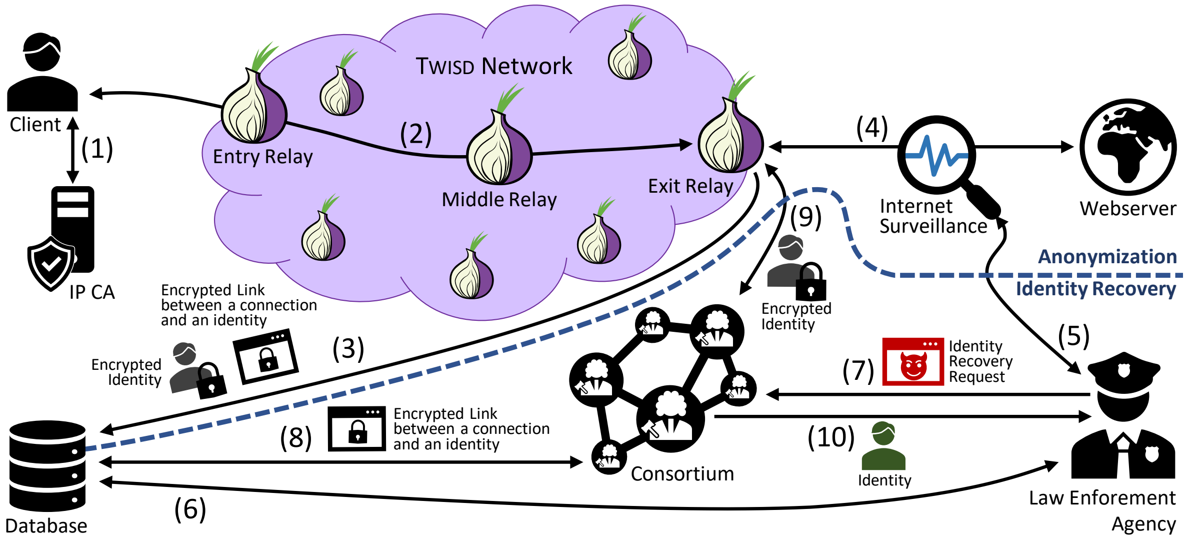

Figure 1: An overview of TWISD at work. (1) A client obtains an IP certificate if a new one is required. (2) He then establishes a new TWISD circuit. (3) The exit relay externally stores encrypted information linking the client's identity to its traffic. (4) The client connects to the Internet through the anonymity network. (5) This traffic is analyzed by LEAs for suspicious behavior. (6) A LEA can link an intercepted packet to one of the stored flows. (7) Then, it requests the identity of the traffic's origin from the consortium. (8+9) The consortium, in collaboration with the exit relay, can link the flow to an encrypted identity. (10) Finally, the identity can be recovered such that only the LEA learns it.

honest users from Tor and thus weaken the anonymity in Tor. This has two consequences : (1) TWISD would facilitate the work of LEAs even without banning other anonymity networks, and (2) TWISD has to be securely usable for all current Tor users as long as they do not engage in activities risking public safety. In particular, this means that TWISD has to offer anonymity to high-profile individuals and people using anonymity service to escape an oppressed Internet.

3.1 Using the TWISD Network

Figure 1 shows an overview of TWISD's architecture. TWISD identifies clients based on their IP addresses at the time of connecting to the network. When a client first connects to the network, it has to request an IP certificate from a certificate authority (CA). Such a certificate proves the TWISD users' ability to sent and receive from a certain IP address and thus makes exactly the anonymization offered by TWISD revocable. Afterward, when establishing a new TWISD circuit, the client executes an anonymous authentication protocol with the relays to generate an encrypted client identity. Encrypted identities allow the identification of clients or pinpointing misbehavior to one of the relays in the circuit. Because we can probe a relay's honesty under normal circumstances, we can make the reasonable assumption that a relay would only act maliciously while directly colluding with the client. This assumption, in turn, means that an identified malicious relay is as valuable to LEAs as the client's identity. A client's encrypted identity and metadata of established connections are then stored in a state-sponsored database, while the client can use his circuit.

3.2 Accessing Anonymized Identities in Exceptional Cases

During the usage of TWISD, encrypted identities of all users are stored in a state-sponsored database. These identities are however not retrievable by governments at will; Instead, access to this data is protected behind several layers of security. As a first step to provide security, the identities are threshold-encrypted, such that a majority of members of a trusted consortium have to agree on an identity recovery. We propose to assemble such a consortium from governmental representatives for their legal expertise, privacy-advocates to bring trust, and privacy-protecting cooperation for their ability to resist governmental pressure. A second

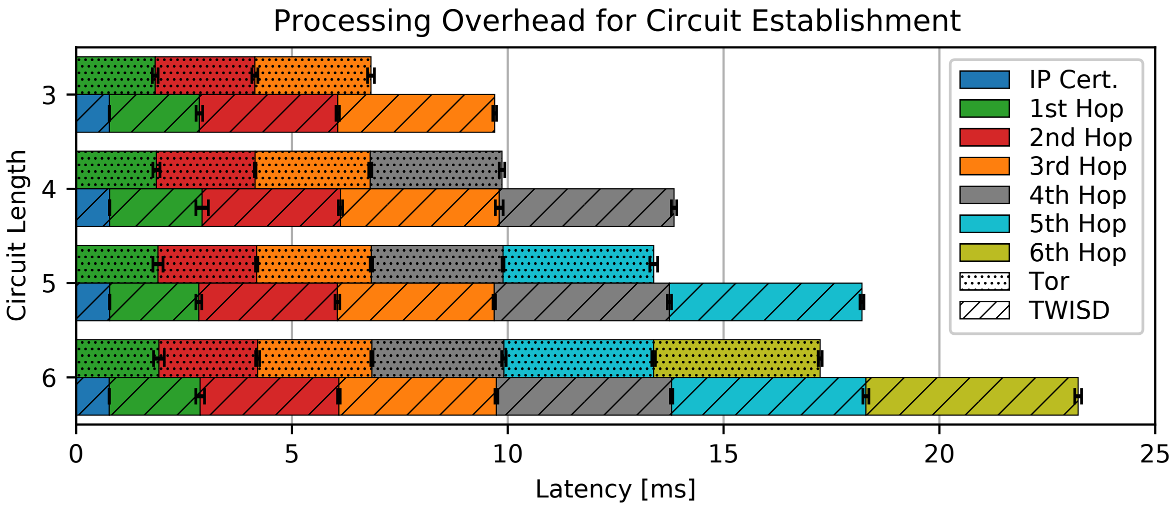

Figure 2: Bar plot of the average latencies to establish a circuit for a given length in Tor and in TWISD. The bars are dissected to display the latencies of each circuit extensions individually. Error bars show 95 % confidence intervals.

layer of security comes from including the exit relays of a circuit into the identity recovery process. Most of the security in Tor comes from the exit relay and by integrating it into the identity recovery process. Thus, we only have to select a consortium that is more trustworthy than two randomly selected relays (*i.e.*, the entry and middle relay), in order for the identity recovery process in TWISD to be less vulnerable than a collusion attack in Tor. The final core protection mechanism comes from the eventual transparency of identity recovery attempts, for the realization of which we propose translucent blockchains. This eventual transparency allows us to not base TWISD's security on blind trust, but on the assumption that consortium members are honest as long as dishonest behavior is eventually uncovered. We can also think of additional protection mechanisms against mass surveillance (*e.g.*, only probabilistically storing identity recovery information, or integrating cryptographic puzzle into identity recoveries).

4 Performance Evaluation

We built a prototype of TWISD by extending the Tor codebase as previously discussed, while also adding some additional features. Tor was used as a baseline because it is the most popular and best-performing anonymity network. Usually, Tor is evaluated via simulations in *Shadow* [15]. However, this abstracts cryptographic processing away and is thus not suitable for us [15]. Instead, we used a local testbed, consisting of nine TWISD relays (one directory authority, three exit relays, and five non-exit relays) and one TWISD client. As our target host for connection establishments we run an *apache2* HTTP web server. Additionally, a local IP CA and a *MongoDB* database process ran on our server.

In Figure 2, we compare the latency to extend a circuit by one hop at a time. The x-axis shows the elapsed time, while the different horizontal bars represent circuits of various lengths in TWISD or Tor, respectively. The length of the full bars represents the total time to establish a circuit. We subdivide these bars on the basis of when the different hop extension complete. Thus, the green bar represents the time from the client selecting the first hop in the circuit until it received a Created2 cell from this relay. Together, the green, red, orange (and blue) bars represent the total time from the client initiating the circuit establishment until this circuit includes three relays, which is the default circuit length in Tor. Overall, we can observe a latency increase between 2.9 ms and 5.97 ms, depending on the established circuit's length. For connection establishments (not shown in this figure) the overhead is even smaller, with an average overhead of 1.3 ms. In a real deployment, the network latencies between relays contribute orders of magnitude more latency and uncertainty into this process. All in all, we can say that processing and latency overheads are barely perceivable and thus not a problem for TWISD in comparison to Tor.

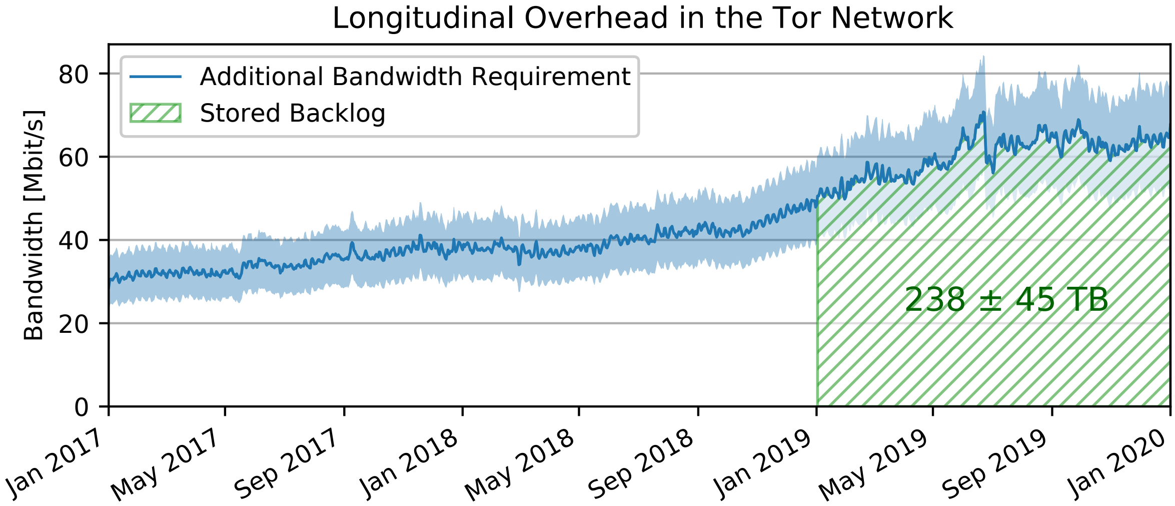

Figure 3: An worst-case estimation of the additionally required exit bandwidth if a Tor-size TWISD network would be deployed. The blue curve estimates the additionally consumed bandwidth by all exit relay over time. The green area estimates ow much data would be retained in the state-sponsored databases. The light blue area show 95 % confidence intervals for the consumed bandwidth.

In reality, the additional data that is transferred and stored by TWISD risks to become the real bottleneck. Therefore, we quantify the impact of the data transfer and storage for a real-world deployment. Estimations of the bandwidth consumption of TWISD also allow us to estimate the processing overhead that TWISD adds to its exit relays. Recent measurements by Mani et al. allow us to predict the requirements of a Tor-sized TWISD network. According to Mani et al., an average of 2.1 billion exit streams were created every 24 hours in April 2018, with an average amount of 20 streams per circuit [16]. Over the same period, the Tor Project reported an average of 111.55 Gbit/s of consumed bandwidth by the Tor network [17]. For our estimations, we make the worst-case assumption that the relationship between the amount of consumed bandwidth and the amount of opened exit streams is constant over the last three years. Figure 3 quantifies the bandwidth overhead of TWISD in a Tor-sized network according to these estimations. Here, the blue line shows the combined bandwidth consumption by all exit relays to write data into the state-sponsored database. In January 2020, all Tor exit relays combined would thus consume 67.7 Mbit/s to write identity recovery data to the state-sponsored database. These data transfers however, only increase the consumed exit bandwidth of TWISD by 0.11% in comparison to Tor. Our estimations also mean that an exit relay advertising 50 Mbit/s of exit bandwidth has to, on average, verify 385 ed25519 signatures, compute 18 hybrid threshold encryptions, and insert 403 elements into its local database per second. This processing overhead is low enough to be hardly noticeable for exit relays. Figure 3 also highlights the amount of data that would be stored in the state-sponsored database, in case identity recovery data should be retained for one year after the traffic was sent. This storage requirement is shown by the green, hatched area in the figure. For data retention of a year, the governments would thus have to store 234 TB of identity recovery data. A database that fulfills these bandwidth and storage requirements can be set up even by the governments of poorer countries.

5 Conclusion

Unreasonable demands for governmental access to hidden data became more frequent over the last years. We analyze current proposals to limits such data access to exceptional cases and come to the conclusion that none of the current proposals satisfy all necessary requirements towards such a system. We also identify anonymity networks as a known enabler of criminal activities, which, however, received little attention in this debate. Therefore, we analyze the feasibility of integrating limited identity recovery into an anonymity network and propose

Twisd as a result. Twisd forces all users to execute an anonymous authentication protocol that allows the exit relay to store encrypted identities of all users to a state-sponsored database. When necessary, a consortium of trusted parties, in cooperation with the exit relay of a circuit, can recover a user's identity. All such identity recovery attempts become public eventually. We show that Twisd does neither have significant latency or processing overhead compared to Tor, nor does Twisd produce unreasonable amounts of data. Twisd could even attract many more users than Tor because it would not be associated with criminal activities. Thus, Twisd could even offer better anonymity than Tor for honest citizens.

References

[1] D. Lyon, *Surveillance After Snowden.* John Wiley & Sons, 2015.

[2] U. Gasser *et al.*, "Don't Panic: Making Progress on the "Going Dark" Debate," 2016.

[3] R. Dingledine *et al.*, "Tor: The Second-generation Onion Router," tech. rep., Naval Research Lab Washington DC, 2004.

[4] R. Dingledine and N. Mathewson, "Anonymity Loves Company: Usability and the Network Effect," in *WEIS 2006*.

[5] The Tor Project, Inc., "Who uses Tor?." Last accessed: August 9,2020.

[6] D. Moore and T. Rid, "Cryptopolitik and the Darknet," *Survival*, vol. 58, no. 1, pp. 7–38, 2016.

[7] H. Abelson *et al.*, "Keys under doormats: mandating insecurity by requiring government access to all data and communications," *Journal of Cybersecurity*, vol. 1, no. 1, pp. 69–79, 2015.

[8] C. Wright and M. Varia, "Crypto Crumple Zones: Enabling Limited Access Without Mass Surveillance," in *IEEE EuroS&P 2018*.

[9] M. Bellare and R. L. Rivest, "Translucent Cryptography—An Alternative to Key Escrow, and Its Implementation via Fractional Oblivious Transfer," *Journal of cryptology*, vol. 12, no. 2, pp. 117–139, 1999.

[10] S. Savage, "Lawful Device Access without Mass Surveillance Risk: A Technical Design Discussion," in *ACM CCS 2018*.

[11] S. Servan-Schreiber and A. Wheeler, "Judge, Jury & Encryptioner: Exceptional Access with a Fixed Social Cost," *arXiv:1912.05620*, 2019.

[12] M. Backes *et al.*, "BackRef: Accountability in Anonymous Communication Networks," in *ACNS 2014*.

[13] A. Greenberg, "The Father of Online Anonymity Has a Plan to End the Crypto War," 2016. Last Accessed: 20/10/2019.

[14] Y. Zhang *et al.*, "Onionchain: Towards Balancing Privacy and Traceability of Blockchain-Based Applications," *arXiv:1909.03367*, 2019.

[15] R. Jansen and N. Hopper, "Shadow: Running tor in a box for accurate and efficient experimentation," in *NDSS 2012*.

[16] A. Mani *et al.*, "Understanding Tor Usage with Privacy-Preserving Measurement," in *IMC 2018*.

[17] The Tor Project, "Tor—Metrics," 2020. Last accessed: August 9, 2020.