

In Pursuit of Privacy: An Introduction to Anonymization Technologies

Gunnar Wolf*

Department of Computer Science, Instituto de Investigaciones Económicas, Mexico

Received: 📅 October 01, 2018; Published: 📅 October 09, 2018

*Corresponding author: Gunnar Wolf, Department of Computer Science, Instituto de Investigaciones Económicas, Mexico

Short Communication

Privacy in the age of pervasive computing and networking is a very hard topic to fully grasp. Any serious attempt at discussing it must take many different angles into account. User interactions grow richer month after month, and due to Big Data techniques, more information about each individual is known to third parties than to the person in question themselves; this is illustrated in the concept of inverse privacy [4]. What is a user to do to keep at least a basic expectation of privacy? Due to the pervasive analysis, a user can only expect their actions to remain private by becoming anonymous-By incorporating into their everyday activities Privacy Enhancement Technologies (PETs) that avoid each of their actions to be linked into a wide-encompassing profile. Anonymity is often achieved via confusion and blending in the crowd: If a person wants their messages to be concealed, they usually first need to identify and use an active network carrying traffic in which to hide; implementations starting with Chaum's mix networks [2] expressly assume an existing level of traffic needed for anonymous messages to be hidden. Mix networks are based on public key cryptography, first delineated in 1976 [3]. In a nutshell, each message is encrypted with the public key of several intermediaries, forming a route that must be followed in order to reach its destination. That is, having users A, B, C, D and E, each of whom has an asymmetric key pair $\{K_A, K_A^{-1}\}$, $\{K_B, K_B^{-1}\}$ etc. and denoting encryption and decryption of a clear-text message M to a secret-containing cyphertext S respectively as $S = \text{Enc}(M; K_A)$ (which anybody can do, as the public key K_A is known by every actor) and $M = \text{Dec}(S; K_A^{-1})$ (which only A can perform, as only this actor has knowledge of K_A^{-1}).

Messages are usually split in several packets, and encrypted to follow a route-A wishes to covertly send B a message M, so they send SD to D:

$$S_D = \text{Enc} \left(\text{Enc} \left(\text{Enc} \left(M; K_B \right); K_E \right); K_D \right)$$

Once D receives and decrypts this message, the contents are just an undecipherable S_E . The message is relayed, and E performs the same operation, yielding S_B . B relays the message is then sent to B, but the decryption finally yields a cleartext M. Space for this article is quite limited, so it cannot dig in the wealth of existing PETs; suffice it to state that each media will have different needs, reality, and 1 thus the answers will necessarily be quite different. Even ignoring the actual data of which the communication actually consists, a simple comparison between the metadata derived from different media yields very different results. The user requirements for the PET in question is correspondingly different as well. As an example, if a user produces a certain pattern of network activity expressed in the amount and size of packets sent (even if their contents are unintelligible to an observer) and this same pattern can be seen at the destination endpoint, strong correlation can be made; mix networks delineated by Chaum can counteract surveillance by adding random delays and spurious dummy messages to message propagation (so that an external observer cannot easily correlate packets); in the case of e-mail, slowness is a feature-This means, given e-mail is not an interactive media, inducing delays up to several minutes in mail delivery does not harm its usual interaction mode. However, for interactive use (video or audio stream watching, Web browsing, or even instant messaging), delays are definitively not acceptable. Onion routing [5] adds to mix networks the concept of building persistent circuits, each of which operates in a fashion similar to mix networks, but adding the creation of circuits. There are two main reasons for setting up circuits [6].

Latency

Setting up a channel spanning several nodes, each of them encrypted using asymmetric cryptography is computationally very expensive-It both adds latency and hefty processing requirements. Symmetric cryptography is much faster but requires the knowledge

of a shared key. So, the circuit set up phase involves the agreement on a randomized session key [1].

Jitter


Each route set up takes a different time to be traversed. Even intuitively, if a connection between two hosts must cross nodes in different countries for each sent packet, the jitter (time deviation from the average) will have huge variation. While email does not, as we said, lead to a lower perception of quality, interactive uses will surely suffer from it. Networks based on onion routing allow for a much more transparent use, sometimes even with nearly imperceptible delay. It does offer, though, far less protection against correlation attacks-A state-level adversary might be able to control enough monitoring points of a network to correlate starting and ending points.

In the current day Internet, the best-known anonymity technology is Tor (<https://torproject.org/>), a onion routing-based, low latency network which is built over slightly over 6000 volunteer-provided relay servers (<https://metrics.torproject.org/networksize.html>), which jointly routes close to 130Gbps. Large-scale surveillance is a threat to individuals' privacy, and anonymity technologies (or, more generally speaking, privacy enhancement

technologies) are every day more a need. Be it for the posterchildren of privacy, such as reporters sending to a secure location their ongoing work or whistleblowers exfiltrating documents proving certain misdeeds, to individuals just wanting given 2 searches not to influence the set of ads presented to them in the browser, these technologies are finally entering the mainstream conscience. The author wishes to thank the support granted by the UNAM/DGAPA/PAPIME PE102718 project.

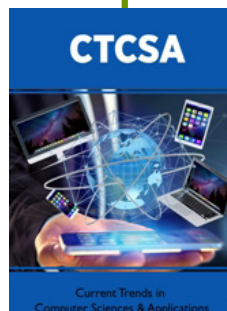
References

1. Elaine Barker (2009) Recommendation for key management-part 1: General, nist special publication. National Institute of Standards and Technology, pp. 800-857.
2. Chaum DL (1981) Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM 24(2): 84-90.
3. Diffie W and Hellman M (1976) New directions in cryptography. IEEE transactions on Information Theory 22(6): 644-654.
4. Gurevich Y, Hudis E, Wing JM (2016) Inverse privacy. Communications of the ACM 59 (7): 38-42.
5. Reed MG, Syverson PF, Goldschlag DM (1998) Anonymous connections and onion routing. IEEE Journal on Selected areas in Communications 16(4): 482-494.
6. Dingleline R, Mathewson N, Syverson P (2004) Tor: The second-generation onion router. Usenix Security.

 This work is licensed under Creative Commons Attribution 4.0 License

To Submit Your Article Click Here: [Submit Article](#)

DOI: [10.32474/CTCSA.2018.01.000103](https://doi.org/10.32474/CTCSA.2018.01.000103)



Current Trends in Computer Sciences & Applications

Assets of Publishing with us

- Global archiving of articles
- Immediate, unrestricted online access
- Rigorous Peer Review Process
- Authors Retain Copyrights
- Unique DOI for all articles