Applied Privacy Enhancing Technology for P2P Networks with p3lib

Gonçalo Pestana (goncalo@hashmatter.com)

Abstract: In this lightning talk, we discuss the importance of bridging the gap between research on Privacy Enhancing Technologies (PETs) for P2P networks and the current decentralized web industry. In addition, we discuss how to design and implement practical software that can be used by system engineers to enhance privacy of current P2P systems, while focusing on current open challenges in production systems such as IPFS and Dat.

Talk motivation and goals

As P2P networks and decentralized systems (re)gain popularity among researchers and industry alike, it is important to design and implement decentralized systems that not only preserve users' privacy but also deliver on scalability, performance and usability. Failing to deliver on those properties will render decentralized systems unusable and unattractive for mass adoption or as a viable alternative to centralized systems.

It has been demonstrated that naive implementation of decentralized systems potentially harm user privacy more than centralized systems (Troncoso et al. 2017), (Wolchok and Halderman 2010), (Jia et al. 2016). However, while the user base and number of applications built on top of large scale decentralized networks such as IPFS ("IPFS" 2018) and Dat ("Dat Project" 2018) has been increasing, there hasn't been enough research and development efforts to design and implement primitives and protocols that allow users to leverage those systems in a secure way.

p3lib In this lightning talk, we discuss the importance of bridging the gap between research on PETs for P2P networks and the current decentralized web industry. We also introduce p3lib ("P3lib" 2018), a modular toolbox for system engineers to build secure and privacy preserving P2P systems. p3lib implements a set of primitives and protocols derived from academia work such as Onion Routing on top of arbitrary overlay networks (Danezis and Goldberg 2009), (Kate and Goldberg 2010), ShadowWalker [1], Octopus DHT lookup [2], plausible deniability for DHT lookups, among and others. The goal is to provide modular software implementing those primitives that can used by system developers to enhance privacy of P2P services built on top of Dat, IPFS and, more generally, libp2p ("Libp2p" 2018) and other P2P networking stacks.

In addition, we outline the current industry needs in terms of privacy engineering, introduce the roadmap p3lib and show how the research community can actively contribute with suggestions, research and implementation work.

hashmatter At hashmatter ("Hashmatter" 2018) we believe that P2P and decentralised networks will play an important role in the future of connected services. Our goal is to research, design and implement primitives and protocols that enhance privacy in P2P networks for application developers to use out of the box. We aim at creating a research-to-industry pipeline that brings the most recent privacy and security primitives to the hands of system P2P engineers.

References

Danezis, G., and I. Goldberg. 2009. "Sphinx: A Compact and Provably Secure Mix Format." In *2009*

30th Ieee Symposium on Security and Privacy, 269–82. https://doi.org/10.1109/SP.2009.15.

"Dat Project." 2018. https://datproject.com.

"Hashmatter." 2018. https://hashmatter.com.

"IPFS." 2018. https://ipfs.io.

Jia, Yaoqi, Guangdong Bai, Prateek Saxena, and Zhenkai Liang. 2016. "Anonymity in Peer-Assisted Cdns: Inference Attacks and Mitigation." *Proceedings on Privacy Enhancing Technologies* 2016 (4): 294–314. https://content.sciendo.com/view/journals/popets/2016/4/article-p294.xml.

Kate, Aniket, and Ian Goldberg. 2010. "Using Sphinx to Improve Onion Routing Circuit Construction." In *Financial Cryptography and Data Security*, edited by Radu Sion, 359–66. Berlin, Heidelberg: Springer Berlin Heidelberg.

"Libp2p." 2018. https://libp2p.io.

"P3lib." 2018. https://github.com/hashmatter/p3lib.

Troncoso, Carmela, George Danezis, Marios Isaakidis, and Harry Halpin. 2017. "Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments." *CoRR* abs/1704.08065. http://arxiv.org/abs/1704.08065.

Wolchok, Scott, and J. Alex Halderman. 2010. "Crawling Bittorrent Dhts for Fun and Profit." In *Proceedings of the 4th Usenix Conference on Offensive Technologies*, 1–8. WOOT'10. Berkeley, CA, USA: USENIX Association. http://dl.acm.org/citation.cfm?id=1925004.1925007.