Privacy Vulnerabilities on Distributed Hash Tables

Gonçalo Pestana (goncalo@hashmatter.com)

DRAFT: This document is work in progress. Please send your comments, suggestions and corrections to gpestana@hashmatter.com or join the conversation at https://ppdht.hashmatter.com

Abstract

Distributed Hash Tables (DHT) are overlay networks that enable distributed nodes to store and request data in a peer-to-peer (P2P) network. Data storage and data lookups are resolved collectively through a collaborative routing protocol in a deterministic way. The collaborative nature of DHTs results on resilient, scalable and decentralized networks where nodes are not required to maintain a complete view of the network while, simultaneously, not relying on central authorities. These properties make DHTs an important building block for the decentralized web and P2P systems. However, the decentralized nature of DHTs introduces privacy vulnerabilities due to the metadata leaked during the routing and lookup protocols. In naïve DHT implementations, it is trivial for any adversary to gather information about which nodes are requesting what data and which nodes are providing what data, without being detected and with relative low resources. Nowadays, the decentralized web ecosystem is relying heavily on DHTs as networks such as IPFS and Dat are steadily reaching mainstream adoption. Thus, it is important to address privacy preserving vulnerabilities of DHTs. Failing to deliver on user privacy will render decentralized systems unattractive as a viable alternative to centralized systems. In this paper we outline the privacy vulnerabilities of the most common DHT protocols and show how those vulnerabilities affect current applications that rely on distributed hash tables.

Introduction

Previous work

Threat model

Privacy vulnerabilities of DHTs

Conclusion

References