Securing Kademlia with a low overhead PKI

Orson Peters

February 5, 2013

Abstract

This paper outlines a low overhead protocol that creates a robust public-key infrastructure (PKI) to secure Kademlia. Presented here is a centralized solution that uses a certification authority that provides identity to nodes. If correctly implemented this solution implicitly resists common attacks aimed at DHTs and can be extended in various ways to further limit malicious activity to a minimum, depending on the use case. This solution is unprecedented in low overhead (both latency and bandwidth) and supporting a recursive/iterative routing hybrid.

1 Introduction

Kademlia [1] is a high-profile Distributed Hash Table (DHT). Used in many P2P applications (LimeWire, Gnutella, Overnet, EDonkey2000, eMule, BitTorrent, etc) it is the most used DHT around. For good reason, it's nifty topology allows for fast, flexible and low-overhead routing. However, Kademlia does not concern itself with security, and is vulnerable to many attacks.

In this paper we expand on the work in [2]. Similarly, we propose a centralized certificate authority (CA) trusted by all participating nodes. However, we reduce overhead by introducing optimizations such as smaller signatures, timestamps instead of nonces and a novel way to pick randomized node ids. Through the use of secure request tokens and node ids we also enable a hybrid

between recursive and iterative routing for lower latency while maintaining security.

2 Terminology

Throughout this paper we use the following terminology:

$a||b$ - the concatenation of a and b
$H(x)$ - the SHA-1 hash of x
K^+ - the public key of the Ed25519 key pair K
K^- - the private key of the Ed25519 key pair K
$Sign(x, K)$ - the Ed25519 signature of x signed with the key pair K
$Verify(s, x, K^+)$ - verification of the Ed25519 signature s of message x with K^+

Ed25519 [3] is a novel public key signing algorithm, with the desirable property of having small signatures and public keys (respectively 64 and 32 bytes). Furthermore, it is fast, highly secure and allows randomization of a public key without knowing the private key (more on this later). Listed below are the most prominent attacks against Kademlia, later we will discuss how our protocol mitigates these.

3 Attacks

Kademlia suffers from a wide range of attacks. In this paper we only discuss and prevent attacks against the network infrastructure - not network content. We do however provide a provable identity for every node, allowing various solutions like blacklists and reputation systems to secure content.

Man In The Middle. All unsecured internet protocols suffer from this attack. Because the transport layer is not secure any intermediate hop can change or drop any packet, and any party might be able to forge packets.

Replay attack. This is a more subtle version of the Man In The Middle (MITM) attack. An adversary eavesdrops some secured communication and stores it. Now if the communication does not contain any temporary resource such as a timestamp or nonce (number used once), the communication gets accepted when sent by the adversary - breaking the security. Worse, if the communication does not address a receiver for the content the adversary may *replay* the communication to any party. Replay attacks are attacks in it's own right, but may be used to set up other attacks. For example, if a secured request for content is sent out, but does not contain the intended receiver for the request an adversary might send this request to many content providers, effectively creating a cheap and anonymous DDOS attack on the requester.

Routing attack. Each Kademlia node keeps track of a number of nodes to communicate with - the routing table. A routing attack is aimed at this table, filling it with either invalid, offline or even malicious nodes, hampering or even stopping the connectivity of the attacked node.

Eclipse attack. The Eclipse attack [4] is a routing attack where malicious nodes exploit the topology of the network to "surround" a victim node. If successful all or a majority of the routing of the victim node goes through the malicious nodes, allowing them to manipulate or block the communication.

References

[1] P. Maymounkov and D. Mazieres, "Kademlia: A peer-to-peer information system based on the xor metric," *Peer-to-Peer Systems*, pp. 53–65, 2002.

[2] L. Aiello, M. Milanesio, G. Ruffo, and R. Schifanella, "Tempering kademlia with a robust identity based system," in *Peer-to-Peer Computing, 2008. P2P'08. Eighth International Conference on*, pp. 30–39, IEEE, 2008.

[3] D. Bernstein, N. Duif, T. Lange, P. Schwabe, and B. Yang, "High-speed high-security signatures," *Cryptographic Hardware and Embedded Systems–CHES 2011*, pp. 124–142, 2011.

[4] A. Singh *et al.*, "Eclipse attacks on overlay networks: Threats and defenses," in *In IEEE INFOCOM*, Citeseer, 2006.