Chord-PKI: Embedding a Public Key Infrastructure into the Chord Overlay Network*

Agapios Avramidis, Panayiotis Kotzanikolaou, and Christos Douligeris

Department of Informatics, University of Piraeus,
Karaoli & Dimitriou 80, 185 34 Piraeus, Greece
{agapios,pkotzani,cdoulig}@unipi.gr

Abstract. Our goal in this paper is to provide authentication, encryption and non-repudiation services for nodes within Peer-to-Peer networks, in an efficient and scalable way. To accomplish this, we propose a distributed Public Key Infrastructure model, suitable for Peer-to-Peer networks and more particularly for the Chord protocol. Our solution integrates the PKI infrastructure within the Chord architecture. We use well known cryptographic techniques as building blocks, such as threshold cryptography and proactive updating.

1 Introduction

Peer to peer (P2P) networks have received considerable attention in the last few years. In particular, one class of P2P networks, namely structured overlays [1,2,3] seems a very attractive choice for building large scale systems. Almost all structured overlay networks utilize a *Distributed Hash Table* (DHT) abstraction. The DHT uses a consistent hash function (*e.g.* a cryptographic hash function such as SHA-1) in order to assign identifiers to nodes and keys[1]. Moreover, the DHT allows the lookup operations (*get* and *put*) to be performed with logarithmic cost in terms of communication messages. DHTs offer a desirable set of properties for distributed applications such as load balancing, decentralization and scalability.

Until recently, the main focus of research for DHTs was targeted to the performance of the lookup protocols, the topology of the overlay, load balancing and search issues (such as range queries, multi-attribute and aggregation queries) [4]. Recently, research for DHTs has also focused on security issues, *e.g.* [5,6,7].

Towards this direction, we propose the *Chord-PKI*, a distributed Public Key Infrastructure (PKI) embedded into the Chord [1] overlay network. Our system provides certification to the Chord nodes through a synergetic protocol that enables the collaboration of the nodes themselves, without the need for an external

* Research funded by the General Secretariat for Research and Technology (GSRT) of Greece under a PENED grant.

[1] These keys correspond to indices to objects such as files and are not keys in the cryptographic sense.

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 354–361, 2007.

PKI. Chord-PKI provides authentication, encryption and non-repudiation services for the nodes, in an efficient and scalable way. The system uses well known cryptographic techniques as building blocks, such as threshold cryptography [8] and proactive updating [9] and guaranties certain resistance to distributed attacks through redundancy. The rest of the paper is organized as follows. Section 2 presents Chord-PKI as well as its basic functions. Section 3 discusses performance and security issues, while section 4 concludes this paper.

2 The Chord-PKI

Our goal is to build a distributed PKI for the Chord structured overlay network. The use of an external PKI in a P2P environment (such as an external Certification Authority) is not an efficient solution, due to the high communication and management costs involved [10]. Moreover, the use of a traditional PKI would impose additional dependencies with external Trusted Third Parties, which in not always acceptable for decentralized and large-scale applications. Generally, a PKI solution for P2P networks, should achieve the following basic requirements:

- Scalability. Distributed Hash Tables are designed to support very large number of participants (internet scale). Moreover, a basic characteristic of P2Ps is high churn rates (frequent joins and leaves). A scalable PKI model for P2P network must not be affected by these characteristics.
- Efficiency. The certification, revocation, certificate storage and certificate retrieval must not impose heavy computation and communication burden into peer nodes. Traditional PKI models usually imply high computation and communication needs.
- Resiliency to compromised nodes. The trust infrastructure must be resilient to attacks. For example, a hierarchical PKI suffers from a single point of failure (the Root CA).

2.1 A High-Level Description of Chord-PKI

A basic solution for a Chord-based PKI is to empower some peer nodes with certification functionality. However, in this case, each of these certification nodes would be a single point of failure. An enhanced solution would be to partition the overlay network into a number of areas, so that each certification node would serve a single area. In that case, if a certification node were compromised, only one area would be affected. However, the adversary would only have to compromise one certification node in each partition.

Our model is resilient in such attacks, by employing threshold cryptography and it minimizes the burden of public key cryptography, by distributing the cryptographic functionality within the peers. Our solution also minimizes the storage and retrieval requirements for the public keys, by exploiting the distributed storage and retrieval functionality of the Chord protocol. The certificate directory is evenly distributed among the system nodes as a Chord *put* operation, thus balancing the storage cost. Moreover, the lookup of a certificate also exploits Chord functionality and it is implemented through a simple Chord *get* operation.