P2P DNS and Signature Authority

Benshoof, Brendan
bbenshoof@cs.gsu.edu
Rosen, Andrew
rosen@cs.gsu.edu

A. *What?*

We propose a method of distributing Domain Name Services across many or all computers on the Internet. To facilitate the authentication of the records in this new DNS system and to protect against man in the middle attacks, we propose a means of creating a distributed signing authority for SSL certificates.

B. *Why?*

Recent events have yielded new understanding that the mutually trusted third party used for most online key exchanges, specifically corporate signing authorities based in the United States or countries with similar active surveillance programs, have been compromised by the adversary and are being used to facilitate man in the middle attacks. In order to prevent these attacks, we need a method of authenticating domain name records and signatures those domains use to secure communications that are difficult to be systematically subverted by any government or corporation.

C. *How?*

- Use a Distributed Hash Table (DHT) to organize a P2P network (Chord)
- Use a variant on NameCoin to secure a list of servers and public keys and to record DNS registration and transfers.
- Use the DHT to load balance and distribute responsibility for hosting DNS records and certification keys.

D. *Distributed Hash Table (Chord)*

- Means of organizing communication and responsibility in a P2P network
- Each peer is responsible for a verifiable span of hash values
- Facilitates one-to-one communication and one-to-many communication

E. *Namecoin Variant*

- Allows for a shared, immutable and secure public records
- Based on the block chain verification of Bitcoin
- One block can include the validation of a new server's public key
- One block can include a DNS record or change
- Blocks require a proof of work to authenticate, causing records to be produced at a semi-fixed rate
- Unlike Bitcoin there is one transaction per block. Thus mining only happens when a new record is required

F. *Man in the Middle Prevention*

- Given: an existing network where nodes have exchanged keys securely
- Given: a new peer who wishes to join the network and share their public key
    - At least 2 members of the network interrogate the new peer for its public key
    - Those peers that interrogated the new peer compare their results
    - If those results match
        - The new peer mines a block with an authentication record
        - The peers who authenticated the new peer sign that block
        - The new block is distributed across the network
    - If the results do not match
        - An attack is detected and reported to the new peer by all authenticating servers
        - A member of the network may mine a block with a ban of the compromised peer
        - Otherwise the joining process may be repeated in hopes of success

G. *Distribution of DNS*

- Responsibility for serving DNS records is distributed across the network
- Each node of the network acts as a DNS server reverse compatible with the DNS RFC
- Any end user who wishes to use this DNS network sets any node as their DNS server (and ideally this node is nearby to the client)
- Each node keeps a local hosts file that caches the results of recent and frequent results
- If a node does not have the DNS record for a request locally or stored in the cache, it may either internally seek the value or return its best peer for that record, depending on the recursive bit of the DNS request.
- Optionally, if a DNS request is for a domain the P2P DNS is not configured to manage, the request is forwarded to a conventional DNS server