Secure Identity Research Group
http://www.inf.fu-berlin.de/groups/ag-si/

Freie Universität Berlin

CryptID - Distributed Identity Management Infrastructure

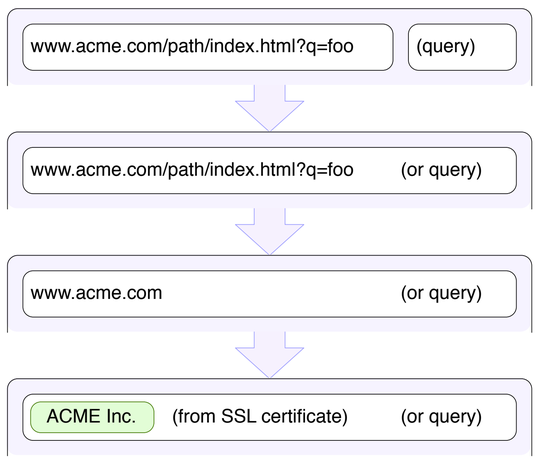
Jan-Ole Malchow and Volker Roth

<firstname>.<surname>@fu-berlin.de

Many of the services on which we depend on the Internet where designed when communications security was not a major concern. Security measures are the result of organic growth. This growth added complexity and often lead to unanticipated problems. Our research questions are: 1) how can we radically simplify the architecture, and 2) how can we do so without breaking too much.

Opportunity: Search instead of DNS Names

When search engines emerged, user behavior changed



This paradigm shift ultimately allows us to:

1. replace human-readable but insecure names with secure but random-looking identifiers, and to
2. disentangle, replace and simplify the existing stack of Internet services related to name services and security.

Keys come before names. Local names are more valuable than global names.

Searching Identities

An index provides service entries that map descriptions to IDs. Descriptions are limited in length but their structure is not mandated. In order to connect to a service, the index makes use of dictionaries. A dictionary provides routing entries that map IDs to routing addresses. Neither indexes nor dictionaries have to be trusted.

Service entries and routing entries are self-authenticating, that is, signed

Status

Implementation	
DHT (based on Kademlia)	✓
Search (based on Apache Blur)	✓
Registration	✓
DNS Proxy	✓
Public Logserver	–

Future Directions

Indexes and dictionaries do not solve the trust issue. They yield a clean architecture and highly scalable infrastructure that separates trust concerns from infrastructure operations.

CryptID allows to focus on what's relevant: where should trust come from?

System Overview

The CryptID system consists of a management component, a service registration and indexing component, and a routing address resolution component. Users interact with CryptID by means of the identity management. It allows users to:

1. Perform searches for identities,
2. Create and publish CryptIDs,
3. Manage indexers (use or blacklist),
4. Register identities at indexers, and
5. Manage pet names.

The identity registration and indexing component is illustrated here. Solid lines show the registration process. Dashed lines are part of the retrieval process.