Secure naming structure and P2P application interaction

draft-dannewitz-ppsp-secure-naming-02

IETF – DECADE WG

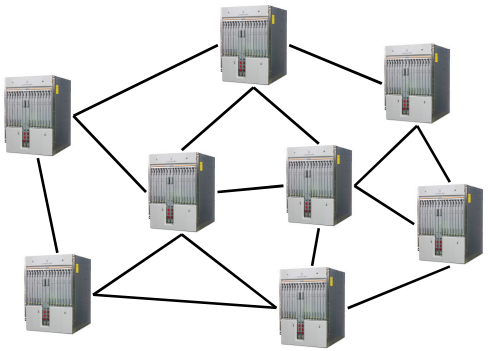
March 2011

Börje Ohlman, Ove Strandberg, Teemu Rautio and Christian Dannewitz

General motivation

Today's Internet

Focus on
nodes

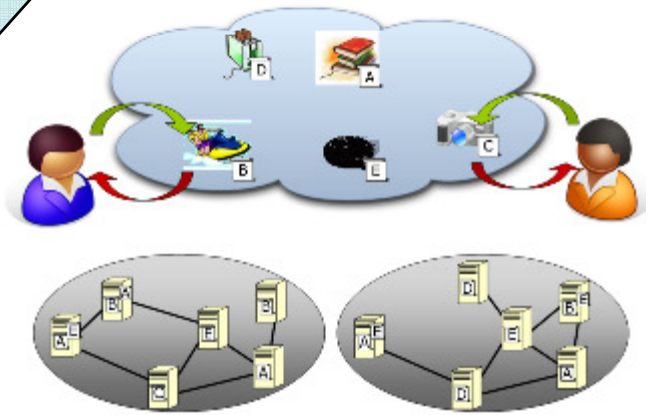


Evolution

Web CDN P2P

Future
Information Centric Network

Focus on
information objects and real world objects



In today's Internet, accessing information is the dominating use case!

Main message of this draft

"A common, application independent, naming scheme for information objects is needed for the Internet"

Requirements for naming scheme

- Location independent names
- Name persistence
- Application independent names
- Secure names - no need to trust the hosts
- Owner authentication
- Owner identification

(Not all mandatory for all applications/use cases, but the naming structure should support them as it is difficult to change once introduced – remember ipv4/ipv6)

Secure naming for P2P

- Different applications uses different naming schemes
- Currently has no guarantee that downloaded content is the same as expected
- Secure naming scheme requires simple extensions to P2P (BitTorrent as an example):
  - Extended torrent file with additional security metadata
  - Torrent name generated according to special rules
    - > client can check torrent file integrity that relates to torrent's name

Secure naming in DECADE

- Basic requirements for naming:
  - The naming of the data objects must be collision free
  - The name should point to the correct data
    - > naming based on the hash of the content is one alternative
- Additional requirements:
  - Verification of the content owner
  - Persistent names for dynamic content
  - Potential identification of the content owner (may require third party certifier)

Secure naming for CDNs

- Challenge in naming between:
  - End-users – CDN
  - Different CDNs

- By using common naming all available cached copies (in different caches and CDNs) can be used efficiently

Draft changes -01 -> -02

New in -02 draft:

- Main message: “A common, application independent, naming scheme for information objects needed for the Internet”
- Abstract updated
- Section 4. Now: Examples of application use of secure naming scheme
  - In addition to Bit-Torrent example for PPSP it now also includes examples for DECADE and CDNI