COMP7370 Advanced Computer and Network Security

Generalizing Data to Provide Anonymity when Disclosing Information (5)

Topics:

1. Introduction
2. Architecture

Topic 1: Introduction

- Why we should read this paper?
  - Citation rate: 2164 (4/19/2011)
  - http://freenetproject.org/
  - Different flavor compared with the k-anonymity paper
  - Build a system based a theory

- Distributed vs. Centralized Storage Systems (**discussion**)
  - Distributed
    - Pros: reliability; security; scalability
    - Cons:
  - Centralized
    - Pros: thin client; usability; maintainability;
    - Cons:
  - Which is better in terms of privacy protection?
  - Which is more energy efficient?
  - Distributed Systems vs. P2P Sys

- Design goals (**If I ask you to develop a P2P storage system, what will be your design goals?**)
  - Decentralization of all network functions (for Storage System)
  - Dynamic storage and routing of information (for Storage System)
  - Anonymity for producers and consumers of information (Privacy)
  - Deniability for storers of information (Privacy)

Topic 2: Architecture

- Big picture
  - Cooperative distributed file system
  - Each node – local datastore
  - Location independence
  - Lazy replication
  - Share unused disk space (for users)
  - Routing (adaptive): Requests -> nodes (local decision about where to send requests next)
  - Hops-to-live: prevent infinite chains

- Keys and searching
  - File IDs: binary file keys
  - 160-bit SHA-1
  - Keyword-signed key (KSK)
    - Keywords = string -> [generate key pairs] -> public/private key
    - Public key -> [hash function] -> file key
    - Private key, file -> [sign the file] (Why? integrity check)
    - Encryption: file, string -> [encryption]
  - How to share? Use the string (keywords)
  - Flat global namespace: problem? Solution? Use personal namespace