Searchable encryption
An alternative to surveillance
Ning Luo
Outline

Debate over surveillance

Searchable encryption

Searchable encryption Implementation
Debates over surveillance

Privacy Vs. Security

The leaks in 2013 by Edward J. Snowden

Many technology companies add encryption to their products and services

Tension between security and privacy

Congress approve six-year extension of surveillance law, section 702.
Debates over surveillance

Look forward, what about next 6 years?

“People, even for people from foreign country, should be assumed to be trustworthy and worthy of respects, instead of criminals,”

The possibility to abuse Section 702

Bulk collection approach can also damage security

Ignoring some of the ways these capabilities might allow the public to have the best of both worlds:
Searchable encryption

Introduction

Outsourced the storage of data to another party in a private manner

Ability to search over it

Delegated search
Searchable encryption

Properties and why it works

**The entire database is encrypted**  -->  **Privacy will be ensured**

**Data owner generates tokens for search queries**  -->  **Search will not be abused**

**Searching will only leak limited information**  -->  **Privacy will be further protected**
Implementation: Tools

Searchable encryption protocol: Oblivious cross-tag encryption (OXT).

Language: Python3.6

File processing: Natural Language Toolkit

Cryptographic tools: Cryptography

Connection between server and client: TCP socket
Implementation : Tools

Oblivious cross-tag encryption (OXT)

Advantage : First sublinear conjunctive-search solution

Approach : Apply search based on term frequency into encryption setting
Implementation : Tools

Oblivious cross-tag encryption (OXT)

\( T\_Set : \) Single keyword search (SKS)

Client : \( T\text{setGetTag} \)

Server : \( T\text{setRetrieve} \)

\( X\_Set : \) Collection of certificates for every pair \((\text{ind}, w)\)
Workflow

Set up

Client pre-processes files $\rightarrow$ Database: $\{w, D_w\}$

Client encrypted database $\rightarrow$ T_set file & X_set file

Client send T_set file & X_set file to server
Workflow

Search

client

name

got your name

server

search over t_set with stag

compute stag

compute tokens

tag

count

tokens

search over x_set with tokens

encrypted index
Reference

Charlie Savage (JAN. 18, 2018) . Congress Approves Six-Year Extension of Surveillance Law
Charlie Savage (JAN. 18, 2018) . House Extends Surveillance Law, Rejecting New Privacy Safeguards
Gopal Ratnam (SEP. 11, 2017) . Congress Braces for Tense Debate on Surveillance Law
Tony Kontzer (JAN. 29, 2018) . Congressional Votes on Controversial Surveillance Law Close Door on Privacy Debate—Or Do They?
Henry Farrell (Apr. 24, 2018) . Most lawyers don’t understand cryptography. So why do they dominate tech policy debates?