OB-PWS: Obfuscation-Based Private Web Search

Ero Balsa, Carmela Troncoso and Claudia Diaz

ESAT/COSIC, IBBT - KU Leuven

Wednesday, 23 May 2012
The Privacy Problem

- sports
- art
- music

PRIVACY PROBLEM:
Individual search queries and/or profiling may reveal sensitive information.

Some solutions:
- Anonymous communications
- PIR
- OB-PWS

⇒ Prevent profiling and provide query deniability.
The Privacy Problem

Individual search queries and/or profiling may reveal sensitive information.

Some solutions:
- Anonymous communications
- PIR
- OB-PWS

⇒ Prevent profiling and provide query deniability.
The Privacy Problem

Individual search queries and/or profiling may reveal sensitive information. Some solutions:

- Anonymous communications
- PIR
- OB-PWS

⇒ Prevent profiling and provide query deniability.

E. Balsa, C. Troncoso and C. Diaz

Obfuscation-Based Private Web Search
The Privacy Problem

**PRIVACY PROBLEM:**
Individual search queries and/or profiling may reveal sensitive information.
The Privacy Problem

- PRIVACY PROBLEM:
  Individual search queries and/or profiling may reveal sensitive information.

- Some solutions:
  - Anonymous communications
  - PIR
  - OB-PWS \(\Rightarrow\) Prevent \textit{profiling} and provide query \textit{deniability}.
Our contribution

- General model.
- Evaluation framework
  \[ \Rightarrow \text{with relevant privacy properties (details in the paper).} \]
- Analysis of 6 existing systems (4 in this talk).
An abstract model for OB-PWS
An abstract model for OB-PWS
An abstract model for OB-PWS
An abstract model for OB-PWS

The user interacts with the OB-PWS system, which generates dummy queries. The adversarial semantic classification algorithm processes these queries and generates observed profiles. The real profile is used for semantic classification and generation strategy. The unclassified queries are also processed by the adversarial semantic classification algorithm.
An abstract model for OB-PWS
An Evaluation framework for DGS

A dual analysis is required:
An Evaluation framework for DGS

A dual analysis is required:

Query-Based Analysis

Exploit vulnerabilities in the DGS to distinguish real from dummy queries.
An Evaluation framework for DGS

A dual analysis is required:

**Query-Based Analysis**

- Exploit vulnerabilities in the DGS to distinguish real from dummy queries.

**Profile-Based Analysis**

- Exploit vulnerabilities in the DGS to filter observed profile and recover the real profile.
GooPIR  \( h(k) \)-Private Information Retrieval

from Privacy-Uncooperative Queryable Databases [1]

- A \( k \)-anonymity inspired approach.
- Prevents attacks based on:
  - Timing/metadata.
  - Popularity of queries.
  - Statistical disclosure.
- However does not consider the *topic* of the queries.
  \[\Rightarrow\text{No dummy indistinguishability}\]
PDS  Plausibly Deniable Search [2]
PDS  Plausibly Deniable Search [2]
PDS  Plausibly Deniable Search [2]
PDS Plausibly Deniable Search [2]
PRAW (A PRivAcy model for the Web) [3]

- Privacy = Dissimilarity.
- Dissimilarity $\propto$ amount of dummy queries.
Privacy = Dissimilarity.

Dissimilarity $\propto$ amount of dummy queries.
PRAW (A PRivAcy model for the Web) [3]

- Privacy = Dissimilarity.
- Dissimilarity \( \propto \) amount of dummy queries.

Considering prior information \( \Pr[X = X] \):

- \((1,0,0)\) observed profile
- \((0,1,0)\) distance between profiles (depends on dummy rate)
- \((0,0,1)\) high probability region for the real profile

\[ \Pr[X = X \mid Y, d] \]
PRAW (A PRivAcy model for the Web) [3]

- Privacy = Dissimilarity.
- Dissimilarity $\propto$ amount of dummy queries.

Considering prior information $\Pr[X = X]$:
PRAW (A PRivAcy model for the Web) [3]

- Privacy = Dissimilarity.
- Dissimilarity $\propto$ amount of dummy queries.

Considering prior information $\Pr[\mathcal{X} = X]$:
Privacy = Dissimilarity.

Dissimilarity $\propto$ amount of dummy queries.

Considering prior information $\Pr[X = X]$:
Privacy = similarity to population's average profile.

Exploitable features:
- Known target profile.
- Amount of dummy queries.
- Waterfilling-based DGS.
OQF-PIR  Optimized Query Forgery for Private Information Retrieval [4]

- Privacy = similarity to population's average profile.

- Exploitable features:
  - Known target profile.
  - Amount of dummy queries.
  - Waterfilling-based DGS.

- Query-based Analysis: Unpopular queries must be real.
OQF-PIR  Optimized Query Forgery for Private Information Retrieval [4]

- Privacy = similarity to population’s average profile.
- Exploitable features:
  - Known target profile.
  - Amount of dummy queries.
  - Waterfilling-based DGS.
- Query-based Analysis: Unpopular queries must be real.
- Profile-based Analysis:

![Diagram showing b < c < a relationship with dummy rate and average population profile]
OQF-PIR Optimized Query Forgery for Private Information Retrieval [4]

- Privacy = similarity to population's average profile.
- Exploitable features:
  - Known target profile.
  - Amount of dummy queries.
  - Waterfilling-based DGS.
- Query-based Analysis: Unpopular queries must be real.
- Profile-based Analysis:

b < c < a

a = b < c
OQF-PIR Optimized Query Forgery for Private Information Retrieval [4]

- Privacy = similarity to population's average profile.
- Exploitable features:
  - Known target profile.
  - Amount of dummy queries.
  - Waterfilling-based DGS.
- Query-based Analysis: Unpopular queries must be real.
- Profile-based Analysis:

![Diagram showing relationships between a, b, c, and the dummy rate.](image)

\[
b < c < a = b < c
\]

\[
a = b < c
\]

\[
b < c < a
\]

\[
a = b < c
\]

\[
Pr[\rho = \rho]
\]

\[
observed\ profile\ equal\ to\ target\ profile
\]

\[
dummy\ rate\ average\ population\ profile
\]
Two main categories of DGS:
- Query based.
- Profile based.

Different definitions of what privacy means:
- $k$-deniability.
- The (dis)similarity of profiles.

Ad-hoc analyses and evaluations.
Open problems and future work

- Plausibility of dummy queries, e.g., The dictionary issue.
- Adversarial modelling, e.g., Adversarial SCA issue.
Conclusions

- Abstract model for OB-PWS systems.
- Analysis framework
  - Definition and formalization of relevant privacy properties.
- Analysis of 6 existing OB-PWS systems (4 in this talk).

- Both profile and query based analyses are needed!
Thank you.

Main references:

$h(k)$-private information retrieval from privacy-uncooperative queryable databases. 

Plausibly Deniable Search. 

PRAW - A PRivAcy model for the Web. 

Optimized query forgery for private information retrieval. 