Protecting Privacy in Terrorist Tracking Applications

Philippe Golle
(Palo Alto Research Center)

Paul Aoki, Dirk Balfanz, Glenn Durfee, Teresa Lunt, Diana Smetters, Jessica Staddon, Jim Thornton, Tomas Uribe (SRI)
Problem

• Countering terrorism involves gathering information from diverse sources to discover key facts and relationships

• Many of these data sources contain personal information

Goal: Allow authorized analysts to search for terrorist-related activity while providing a realistic degree of privacy protection for ordinary citizens’ data

Approach

– Inference control to prevent unauthorized individuals from completing queries that would allow identification of ordinary citizens

– Access control to return sensitive identifying data only to authorized users

– Immutable audit trail for accountability
Privacy Appliance

- Standalone devices
  - Under private control
  - Better assurance of correct operation

- Sits between the analyst and each private data source
  - Easily added to an enterprise’s computing infrastructure
  - Like firewalls

Benefits
- Private data stays in private hands
- Privacy controls isolated from the government
Functions of the Privacy Appliance

- **Inference control** to identify queries that would allow identification of individuals
- **Access control** to return identifying data only to appropriately authorized users
- Logging to create an **immutable audit trail** for accountability
Outline

1. Privacy appliance
2. Inference control
3. Access control
4. Immutable audit trail
Inference Control Tool

- **Withhold identifying attributes**
  - E.g., name, SSN, credit card number, address, phone number

- **Discover which additional fields allow inference of identity**
  - Produce a knowledge base of undesired inferences
    - This serves as input for the access control tool

```
employer

zipcode

type of car

Individual identity
```

Block the inference by raising the authorization required for one of these data items
Statistical Inference Extensions

• **k-anonymity**
  – Information for each person cannot be distinguished from at least $k-1$ other individuals

• The Census Bureau calls a statistic sensitive if $n$ or fewer values contribute more than $k\%$ of the total

\[
\begin{align*}
\text{select } \text{sum(earnings)} & \text{ from census-data} \\
\text{where city} & = \text{“Endicott”}
\end{align*}
\]

is sensitive because IBM in Endicott earns 100x the combined earnings of all other businesses in Endicott

• The inference control tool will enforce $k$-anonymity and other statistical notions of privacy
  – An offline statistical analysis can be done periodically to precompute the basis for a large number of queries
  – Results are input to the inference analysis
Inference analysis is performed ahead of time

- Prepare the input
- Obtain the source database schemas
- Mark fields that are clearly identifying
- Specify additional information
  - Type declarations
  - Quasi-identifiers
  - Functional dependencies
- Produce the access control data for use at runtime
- Analyze the annotated schemas
- Inference control KB
- Perform the inference analysis:
  - Once initially
  - When schemas change
  - When new data sources become available
  - After a large number of updates

Access control DB
Example input to inference tool

(create_table FLIGHT (group
  (column RECORDLOCATOR :identifying t)
  (column ARRIVE :type datetime)
  (column DEPART :type datetime)
  (column TICKETING)
  (column DESTIN)
  (column ORIGIN)
  (column AIRLINE)
  (column FLIGHT :type flight)
  (column AMOUNT)
  (column FOP :type fop) ;; form of payment
  (column NAME :identifying t :type name)
  (column CARDNUMBER :identifying t :type cardnumber)
  (column PASSENGERTYPE)
  (column PHONE :identifying t :type homephone)
  (column BILLINGADDR :identifying t :type addr)
  (column BILLINGCITY)
  (column BILLINGSTATE)
  (column BILLINGCOUNTRY)
  (column BILLINGPOSTAL)
  (column DELIVERYADDR :identifying t :type addr)
  (column DELIVERYCITY)
  (column DELIVERYSTATE)
  (column DELIVERYCOUNTRY)
  (column DELIVERYPOSTAL)
  (column SEAT)
  (column MEAl)
  (column AGENCYID)
  (column AGENCYPHONE)
  (quasi-identifier BILLINGSTATE BILLINGCITY DELIVERYCITY TICKETING)
  (primary-key RECORDLOCATOR)
  (f_dependency BILLINGPOSTAL (BILLINGCITY BILLINGSTATE BILLINGCOUNTRY)))

(create_table FTR (group
  (column STUDENTID :identifying t :type name)
  (column ORIGIN :type nationality) ;; **country of origin**
  (column SCHOOLID)
  (column TYPE) ;; **type of training**
  (column NAME :identifying t :type name)
  (primary-key STUDENTID)
  (near-key NAME))

(create_table HGR ;; hotel guest record
  (group
    (column CUSTOMERID :identifying t)
    (column HOTELID)
    (column CHECKIN :type date)
    (column CHECKOUT :type date)
    (column AMOUNT)
    (column FOP) ;; form of payment
    (column COUNTRY :type nationality)
    (column NAME :identifying t :type name)
    (column CARDNUMBER :identifying t :type cardnumber)
    (column ROOM)
    (column VEHICLE :identifying t)
    (column RATE)
    (column ADDRESS)
    (column LOCALITY)
    (column REGION)
    (column POSTAL)
    (primary-key CUSTOMERID))

(create_table AIRLINE (group
  (column CODE)
  (column NAME))
  (primary-key CODE) )
Output of inference tool (Inference Channels):

C1: INS.BIRTHDATE
   FLIGHT.FLIGHT
   FTR.ORIGIN
   INS.GENDER

C2: INS.BIRTHDATE
   FLIGHT.FLIGHT
   HGR.COUNTRY
   INS.GENDER

C3: FLIGHT.BILLINGPOSTAL
   FLIGHT.DELIVERYCITY
   FLIGHT.TICKETING

C4: INS.BIRTHDATE
   FLIGHT.FLIGHT
   INS.NATIONALITY
   INS.GENDER

C5: INS.BIRTHDATE
   INS.FLIGHT
   FTR.ORIGIN
   INS.GENDER

C6: INS.BIRTHDATE
   INS.FLIGHT
   HGR.COUNTRY
   INS.GENDER

C7: INS.BIRTHDATE
   INS.FLIGHT
   INS.NATIONALITY
   INS.GENDER

C8: INS.BIRTHDATE
   INS.PORTOFENTRY
   FTR.ORIGIN
   INS.GENDER

C9: INS.BIRTHDATE
   INS.PORTOFENTRY
   HGR.COUNTRY
   INS.GENDER

C10: FLIGHT.BILLINGSTATE
    FLIGHT.BILLINGCITY
    FLIGHT.DELIVERYCITY
    FLIGHT.TICKETING

C11: INS.BIRTHDATE
    INS.PORTOFENTRY
    INS.NATIONALITY
    INS.GENDER

Singletons: FLIGHT.RECORDLOCATOR.
    FLIGHT.NAME,
    FLIGHT.CARDNUMBER,
    FLIGHT.PHONE,
    FLIGHT.BILLINGADDR,
    FLIGHT.DELIVERYADDR,
    FTR.STUDENTID, FTR.NAME,
    HGR.CUSTOMERID, HGR.NAME,
    HGR.CARDNUMBER,
    HGR.VEHICLE, INS.NAME,
    INS.PASSPORT
Outline

1. Privacy appliance
2. Inference control
3. Access control
4. Immutable audit trail
Access Control

For lowest authorization:
- Withhold identifying attributes
- Prevent completion of inference channels

Analyst query

Check authorizations

Modify query as needed to withhold data

Mark access “history”

Send modified query to data source

The privacy appliance will recognize
- Which queries touch inference channels
- Whether the user is authorized for the query

Input special authorizations

For higher authorization:
- Can retrieve specific identifying info
- Must specify scope of data authorized

Analysis can’t combine non-sensitive queries to obtain sensitive info
Access Control Rules

• **Identifying Attributes:**
  – A query is blocked if it requests an identifying attribute.

• **Inference Channels**
  – A channel with \( k \) attributes: \(<\text{Attr}_1, \text{Attr}_2, \ldots, \text{Attr}_n>\)
  – Queries may request up to \( n-1 \) attributes in channel
  – This bound applies “globally” to all queries ever asked by any user.

• **Flexible and fast:** performance depends on length of inference channel (not size of query histories)
• **Collusion resistance:** Users cannot combine non-privacy-violating queries that in sum are privacy-violating (we distribute keys)
Identifying Attributes

A query is blocked if it requests an identifying attribute.

Select **name** from flight
where flight = 503 and
arrive = '2005-09-05 08:41:23'

Query blocked!
Identifying attribute:
<flight.name>

select **cardnumber** from flight
where flight = 503 and
arrive = '2005-09-05 08:41:23'

Query blocked!
Identifying attribute:
<flight.cardnumber>
Attributes that appear in the "where" clause of a query also count.

Select amount from flight
where name like '%Nemo%'
and flight = 503 and
arrive = '2005-09-05 08:41:23'

Select amount from flight
where fop = 'MCRD'
and flight = 503
and arrive = '2005-09-05 08:41:23'

Query blocked!
Identifying attribute:
<flight.name>

amount,
-------------
649,
647,
Inference Channel

Example from table “INS”:

<flight, nationality, gender, birthdate>

None of the attributes in this channel have yet been requested.
A query is blocked if it requests all the attributes in the channel (including in the “where” clause)

User One:
Select flight, nationality, gender, birthdate from ins
where arrive > '2005-09-05 00:00:00'
and arrive < '2005-09-06 00:00:00'
Query blocked!

User One:
Select nationality, gender, birthdate from ins
where flight = 8864
and arrive = '2005-09-05 15:24:46'
Query blocked!
A query may request up to n-1 attributes in a channel of length n

User One:
Select flight, nationality, gender from ins
where arrive > '2005-09-05 15:30:00'
and arrive < '2005-09-05 16:00:00'

Inference channel:
<flight, nationality, gender, birthdate>
Subsequent queries for the last attribute are blocked for all users

User Two:
Select `birthdate` from `ins`
where `arrive` > '2005-09-05 15:00:00'
and `arrive` < '2005-09-05 16:00:00'

User Three:
Select `birthdate` from `ins`
where `flight` = 18

Query blocked!

Query blocked!

Note: future implementation will allow the 2nd query
But anyone may ask again for attributes already revealed for that channel.

User Two:
Select nationality from ins
where gender = 'F'
and flight = 8864
and arrive = '2005-09-05 15:24:46'

nationality,
----------------
BR,
BR,

User Four:
Select gender from ins
where flight = 998
and arrive > '2005-09-05 15:00:00'
and arrive < '2005-09-05 16:00:00'

gender,
----------------
F,
M,
Outline

1. Privacy appliance
2. Inference control
3. Access control
4. Immutable audit trail
Immutable Audit Trail

Protection against authorized but dishonest users

• Dishonest users may execute a pattern of queries from which they hope to discover identities

• Such abusive patterns may be discernable by retrospective inspection of an audit trail of analyst activity

• The audit trail will be sensitive and must be protected from inappropriate disclosure

• The audit trail must be protected from tampering by a dishonest user
Generation of Audit Record Shares

Each query is recorded immediately and permanently
– No agent can misuse private data without the strong probability of exposure

Use threshold cryptography
– Each share is meaningless unless combined with \( k \) out of \( n \) other shares
– Share alteration can be detected when shares are recombined

• Reduces the window of vulnerability for tampering
• Generation of shares is fast and can be done in real time
Inspection of the Audit Trail

• If an individual feels harmed by government use of private data, he or she can petition to have relevant records inspected by an independent third party

• Reconstruction of history from shares is fast

• We will develop methods to search encrypted shares to limit the scope of any investigation
  – It should be possible to retrieve only those audit records pertaining to a given individual without having to decrypt the entire audit trail (hard or impossible)
  – It should be possible to retrieve only those audit records pertaining to a given analyst’s actions without having to decrypt the entire audit trail (easy)
Likelihood of Detecting Abuse

- Audit record generation is distributed
  - To prevent the logging of their activity, an analyst must attack each relevant privacy appliance
  - Such behavior is highly unlikely to be successful and go undetected

- Realtime audit trail analysis can scan for attempted abuse
  - Each privacy appliance can analyze its local data. The results can be pooled for further analysis
  - This can increase the probability that authorities will discover any abuse
Summary

Allow authorized analysts to search for terrorist-related activity while providing a realistic degree of privacy protection for ordinary citizens’ data

- Inference analysis identifies sensitive data
- Dynamic access controls prevent access to such data
- Immutable audit trail means high likelihood of detection of abuse
- Integrate all these into a privacy appliance