De-anonymizing Social Networks[1]

Arvind Narayanan - Vitaly Shmatikov (2009)

Y Saikumar - EE14B067
Rohith Bhandaru - EE13B016

10 November 2017

Abundance & Requirement of Data

- ML & AI boom - Data is required
- Research & commercial interests

Abundance & Requirement of Data

- ML & AI boom - Data is required
- Research & commercial interests
- Privacy concerns

Abundance & Requirement of Data

- ML & AI boom - Data is required
- Research & commercial interests
- Privacy concerns
- Digital trails of a person
  - Browsing
  - Social Network
  - Medical History...

Personally Identifiable Information (PII)

Figure: Can we identify a person from the digital trails left?[2]

Aspects of Privacy Protection Technologies

- Identifying and Non-identifying attributes of personal data

Aspects of Privacy Protection Technologies

- Identifying and Non-identifying attributes of personal data
- Personal Data[3] : "Any information relating to an [..] natural person who can be identified, directly or indirectly, in particular by reference [..] to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"

Aspects of Privacy Protection Technologies

- Identifying and Non-identifying attributes of personal data
- Personal Data[3] : "Any information relating to an [..] natural person who can be identified, directly or indirectly, in particular by reference [..] to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"
- De-identification and Re-identification algorithms

Social Network

A social network $\mathcal{S}$ is defined with:

- a directed graph $G = (V, E)$
- a set of attributes $\mathcal{X}$ for each node in V (eg. label and degree of node)
- a set of attributes $\mathcal{Y}$ for each edge in E (eg. type of connection)
- All attributes $Y \in \mathcal{Y}$ are defined over V^2 instead of E. If $(u, v) \notin E$, then $Y[u, v] = \perp, \forall Y \in \mathcal{Y}$

Data Sanitization & Release Process

- Select a subset of nodes $V_{san} \subset V$ and subsets of attributes to be released $\mathcal{X}_{san} \subset \mathcal{X}$, $\mathcal{Y}_{san} \subset \mathcal{Y}$

Data Sanitization & Release Process

- Select a subset of nodes $V_{san} \subset V$ and subsets of attributes to be released $\mathcal{X}_{san} \subset \mathcal{X}$, $\mathcal{Y}_{san} \subset \mathcal{Y}$
- Add noise to the network by removing some edges and adding some fake edges

Data Sanitization & Release Process

- Select a subset of nodes $V_{san} \subset V$ and subsets of attributes to be released $\mathcal{X}_{san} \subset \mathcal{X}$, $\mathcal{Y}_{san} \subset \mathcal{Y}$
- Add noise to the network by removing some edges and adding some fake edges
- Release $\Big(V_{san},\ E_{san},$ $\{X(v), \forall v \in V_{san}, X \in \mathcal{X}_{san}\},\ \{Y(e), \forall e \in E_{san}, Y \in \mathcal{Y}_{san}\}\Big)$

Data Sanitization & Release Process

- Select a subset of nodes $V_{san} \subset V$ and subsets of attributes to be released $\mathcal{X}_{san} \subset \mathcal{X}$, $\mathcal{Y}_{san} \subset \mathcal{Y}$
- Add noise to the network by removing some edges and adding some fake edges
- Release $\Big(V_{san},\ E_{san},$
  $\{X(v), \forall v \in V_{san}, X \in \mathcal{X}_{san}\},\ \{Y(e), \forall e \in E_{san}, Y \in \mathcal{Y}_{san}\}\Big)$

Can sensitive information about specific individuals be extracted from anonymized network graphs?

Attacker Model

Attacker is assumed to be in possession of an auxiliary network $\mathcal{S}_{aux}$ along with the un-labelled sanitized network $\mathcal{S}_{san}$ with a partial overlap of nodes among these networks.

Attacker Model

Attacker is assumed to be in possession of an auxiliary network $\mathcal{S}_{aux}$ along with the un-labelled sanitized network $\mathcal{S}_{san}$ with a partial overlap of nodes among these networks.

Aggregate auxilliary information with attacker is given by $\mathcal{S}_{aux}$ along with Aux_X and Aux_Y, which are probability distributions one for each attribute in V_{aux} and for each attribute of each edge in E_{aux}

- $Aux[X, v]$: Attacker's prior probability distribution of the value of the attribute X of node v
- $Aux[Y, e]$: Attacker's prior probability distribution of the value of the attribute Y of edge e

Attacker Model

It is also assumed that attacker is in possession of detailed information of a very small number of nodes in the network $\mathcal{S}$

Attacker Model

It is also assumed that attacker is in possession of detailed information of a very small number of nodes in the network $\mathcal{S}$

Types of attacker motivations:

- Global surveillance (eg. government agency)
- Abusive marketing (eg. commercial ads)
- Targeted de-anonymization (eg. private investigation)

Attacker Model

It is also assumed that attacker is in possession of detailed information of a very small number of nodes in the network $\mathcal{S}$

Types of attacker motivations:

- Global surveillance (eg. government agency)
- Abusive marketing (eg. commercial ads)
- Targeted de-anonymization (eg. private investigation)

Even though attacker can access a large $\mathcal{S}_{aux}$, de-anonymizing $\mathcal{S}$ is non trivial!

Privacy Breach

Anonymity is necessary but not sufficient for privacy. A one-one *Privacy Policy* function PP is defined as

$$PP : \mathcal{X} \cup \mathcal{Y} \times E \rightarrow \{pub, priv\} \tag{1}$$

Ground truth is defined as a mapping μ_G from the nodes of V_{aux} to V_{san}. $\mu_G(v) = \perp$ if there is no node in V_{san} corresponding to v in V_{aux}.

Node Re-identification

If, for a node $v_{aux} \in V_{aux}$, $\mu(v_{aux}) = \mu_G(v_{aux})$, v_{aux} is said to correctly identified.

Re-identification Algorithm:

A node re-identification algorithm takes $\mathcal{S}_{san}$ and $\mathcal{S}_{aux}$ as input and produces a probabilistic mapping $\tilde{\mu}$ defined as $\tilde{\mu}: \ V_{san} \times (V_{aux} \cup \{\perp\}) \rightarrow [0,1]$, where $\tilde{\mu}(v_{aux}, v_{san})$ is the probability that v_{aux} maps to v_{san}.

Node Re-identification

Mapping Adversary:

A mapping adversary corresponding to a probabilistic mapping $\tilde{\mu}$ outputs a probability distribution calculated as follows:

$$Adv[X, v_{aux}, x] = \frac{\sum_{v \in V_{san},\ X[v]=x} \tilde{\mu}(v_{aux}, v)}{\sum_{v \in V_{san},\ X[v]\neq\perp} \tilde{\mu}(v_{aux}, v)} \tag{2}$$

$$Adv[Y, u_{aux}, v_{aux}, y] = \frac{\sum_{u,v \in V_{san},\ Y[u,v]=y} \tilde{\mu}(u_{aux}, u)\tilde{\mu}(v_{aux}, v)}{\sum_{u,v \in V_{san},\ Y[u,v]\neq\perp} \tilde{\mu}(u_{aux}, u)\tilde{\mu}(v_{aux}, v)} \tag{3}$$

Node Re-identification

Privacy Breach:

For nodes $u_{aux}, v_{aux} \in V_{aux}$, let $\mu_G(u_{aux}) = u_{san}$ and $\mu_G(v_{aux}) = v_{san}$. We say that the privacy of v_{san} is *breached* with respect to the mapping adversary Adv and privacy parameter δ if,

1. for *some* attribute X such that $PP[X] = priv$, $Adv[X, v_{aux}, x] - Aux[X, v_{aux}, x] > \delta$ where $x = X[v_{aux}]$ OR
2. for *some* attribute Y such that $PP[Y] = priv$, $Adv[Y, u_{aux}, v_{aux}, y] - Aux[Y, u_{aux}, v_{aux}, y] > \delta$ where $y = Y[u_{aux}, v_{aux}]$

Measuring Success of an Attack

Success of De-anonymization:

Let $V_{mapped} = v \in V_{aux} : \mu_G(v) \neq \perp$. The *success* rate of de-anonymization algorithm giving a probabilistic mapping $\tilde{\mu}$ as output, with respect to a centrality measure ν, is the probability that μ sampled from $\tilde{\mu}$ maps a node v to $\mu_G(v)$ weighted with $\nu(v)$ as follows:

$$Success\ Rate = \frac{\sum_{v \in V_{mapped}} Pr[\mu(v) = \mu_G(v)].\nu(v)}{\sum_{v \in V_{mapped}} \nu(v)} \quad (4)$$

Measuring Success of an Attack

Success of De-anonymization:

Let $V_{mapped} = v \in V_{aux} : \mu_G(v) \neq \perp$. The *success* rate of de-anonymization algorithm giving a probabilistic mapping $\tilde{\mu}$ as output, with respect to a centrality measure ν, is the probability that μ sampled from $\tilde{\mu}$ maps a node v to $\mu_G(v)$ weighted with $\nu(v)$ as follows:

$$Success\ Rate = \frac{\sum_{v \in V_{mapped}} Pr[\mu(v) = \mu_G(v)].\nu(v)}{\sum_{v \in V_{mapped}} \nu(v)} \tag{4}$$

This is only a *lower bound!*

Re-identification Algorithm Overview

Given the above definitions and assumptions, algorithm is designed as follows:

- Identify a set of seed nodes that are present both in $\mathcal{S}_{san}$ and $\mathcal{S}_{aux}$ and map to each other.

Re-identification Algorithm Overview

Given the above definitions and assumptions, algorithm is designed as follows:

- Identify a set of seed nodes that are present both in $\mathcal{S}_{san}$ and $\mathcal{S}_{aux}$ and map to each other.
- This seed map is propagated to other nodes in the network through an iterative process based only on the topology of the network.

Seed Identification

- Assume that $\mathcal{S}_{aux}$ has k-clique and attacker knows their degrees and neighbors.

Seed Identification

- Assume that $\mathcal{S}_{aux}$ has k-clique and attacker knows their degrees and neighbors.
- Seed identification algorithm searches for a unique k-clique in $\mathcal{S}_{san}$ such that their degrees and common-neighbor counts match with those of the seeds in $\mathcal{S}_{aux}$ within a factor of $(1 \pm \epsilon)$.

Propagation

- A list of mapped nodes is maintained.
- In each iteration, an unmapped node u in $\mathcal{S}_{aux}$ is selected and scores (as defined) are calculated for every unmapped in $\mathcal{S}_{san}$.

Propagation

- A list of mapped nodes is maintained.
- In each iteration, an unmapped node u in $\mathcal{S}_{aux}$ is selected and scores (as defined) are calculated for every unmapped in $\mathcal{S}_{san}$.
- *score(u,v)* is defined as the number of neighbors of u mapped to neighbors of v.

Propagation

- A list of mapped nodes is maintained.
- In each iteration, an unmapped node u in $\mathcal{S}_{aux}$ is selected and scores (as defined) are calculated for every unmapped in $\mathcal{S}_{san}$.
- *score(u,v)* is defined as the number of neighbors of u mapped to neighbors of v.
- If the strength (heuristic) of the *score(u,v)* is above a threshold, u is mapped to v. Else, the process is continued.
- Several heuristics like strength of a score (eccentricity), edge directionality, node degree normalization and reverse mapping are defined and incorporated in the algorithm.

Propagation

- A list of mapped nodes is maintained.
- In each iteration, an unmapped node u in $\mathcal{S}_{aux}$ is selected and scores (as defined) are calculated for every unmapped in $\mathcal{S}_{san}$.
- *score(u,v)* is defined as the number of neighbors of u mapped to neighbors of v.
- If the strength (heuristic) of the *score(u,v)* is above a threshold, u is mapped to v. Else, the process is continued.
- Several heuristics like strength of a score (eccentricity), edge directionality, node degree normalization and reverse mapping are defined and incorporated in the algorithm.
- Computational complexity of the algorithm is given by $O((|E_{san}| + |E_{aux}|)d_{san}d_{aux})$, where d_{san} and d_{aux} ae the upper bounds of degrees of nodes in the respective networks.

Experiments[1]

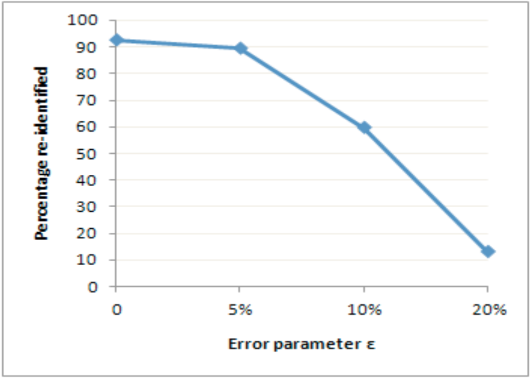

Figure: Re-identification rate decreases with noise parameter

Experiments

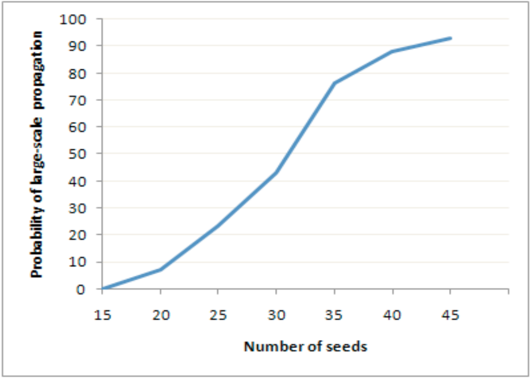

Figure: Phase transition in scale of re-identification Vs. Number of seeds

Remarks

- The more information about a person is revealed as a consequence of re-identification, the easier it is to identify the person in the future.[4]

Remarks

- The more information about a person is revealed as a consequence of re-identification, the easier it is to identify the person in the future.[4]
- A query-based release of data is generally superior to the release-and-forget approach from the privacy perspective.

Remarks

- The more information about a person is revealed as a consequence of re-identification, the easier it is to identify the person in the future.[4]
- A query-based release of data is generally superior to the release-and-forget approach from the privacy perspective.
- Ensuring anonymity is necessary but not sufficient for ensuring privacy of a person.

References:

[1] Narayanan, Arvind, and Vitaly Shmatikov. "De-anonymizing social networks." Security and Privacy, 2009 30th IEEE Symposium on. IEEE, 2009.

[2] Narayanan, Arvind, and Vitaly Shmatikov. "Myths and fallacies of personally identifiable information." Communications of the ACM 53.6 (2010): 24-26.

[3] Directive 95/46/EC of European Parliament

[4] Ohm, P. Broken promises of privacy: Responding to the surprising failure of anonymization. 57 UCLA Law Review 57, 2010