An Abstract View on the De-anonymization Process

Alexandros Bampoulidis, Mihai Lupu
Research Studios Austria - Studio Data Science
Vienna, Austria
{name.surname@researchstudio.at}

Abstract—Over the recent years, the availability of datasets containing personal, but anonymized information has been continuously increasing. Extensive research has revealed that such datasets are vulnerable to privacy breaches: being able to reveal sensitive information about individuals through de-anonymization methods. Here, we provide a taxonomy of the research in de-anonymization.

Index Terms—de-anonymization, privacy, re-identification

I. INTRODUCTION

De-anonymization is not as hard a task as one might think. A common misconception is that removing all explicit identifiers such as name, address and phone number from a dataset, makes the data anonymous. Several approaches described in the de-anonymization literature have proven this belief wrong. The continuously increasing availability of datasets, either private or public, that can be used as auxiliary data in de-anonymization techniques and the fact that there is a privacy breach when even a single individual is identified from a dataset, make anonymization of data a difficult challenge to address, while making de-anonymization easier.

This short paper provides an abstract view of data de-anonymization and raises the awareness of data providers on this topic. Our survey differs from the three other existing surveys on de-anonymization [1]–[4] in providing a more abstract view on this topic and being targeted at data providers. In the next section, we present our view on the de-anonymization along with references to scientific publications. Note that due to the space limitation, we only cite the most important and representative publications of their kind.

II. DE-ANONYMIZATION PROCESS

We identify three elements in the de-anonymization process: purpose, data (target and auxiliary), and approach.

A. Purpose

Purpose refers to why one would perform a de-anonymization attack on a dataset. We identify the three following purposes:

1) Proof of Concept: An attack of such purpose aims in revealing whether a dataset is de-anonymizable or that it cannot be de-anonymized with reasonable effort. This is an important action for data providers to take before releasing their dataset(s), keeping in mind that the re-identification of just one individual is considered a privacy breach and is subject to legal action and fines imposed by governments.

2) Research: De-anonymization attacks having such purpose intend to explore the weaknesses of published datasets and anonymization methods, advance the field of data privacy and encourage others to do so. All publications cited in this work have such a purpose and most of them do not report a de-anonymization attack has been performed, but merely prove the de-anonimizability of the dataset(s) they study and report the extent to which it is de-anonymizable. Those who report a de-anonymization attack has been performed, do not reveal the identities of the individuals they managed to re-identify and their findings are not confirmed by the dataset owners.

3) Malicious: An attacker with malicious intents would perform a de-anonymization attack in order to publicly reveal private, sensitive information of individuals who would, otherwise, not want to have this information published.

B. Target and Auxiliary Data

The target dataset is defined as the anonymized dataset, potentially containing sensitive information of users that an attacker tries to de-anonymize. The target dataset’s availability might be public or private, with the public ones being the most used in research. Some examples from the literature are: health records [5], movie ratings [6] and telecommunication mobility trace data [7].

The auxiliary data/information is defined as the non-anonymized information that aids the attacker in the de-anonymization of the target dataset. The auxiliary information’s availability might be public or private, with the public ones being the most used in research. Some examples from the literature are: voter registration list [5], IMDB’s user reviews [6] and social networks [8]. We categorize the auxiliary information into internal and external.

Internal refers to the auxiliary information that comes from the same source as the target dataset. This is the case of many research publications where the studied dataset is split into training and test set, corresponding to internal auxiliary...
information and target dataset, respectively. Another case is when an attacker obtains part of the target dataset non-anonymized.

External refers to the auxiliary information that does not come from the same source as the target data, and usually does not have the same structure as the target dataset.

C. Approach

The intuition behind all approaches in data de-anonymization is that all users have uniquely defining characteristics. There exist varying approaches exploiting this uniqueness, whose complexity depends on the complexity of the data they apply to. Therefore, in the following we will group the approaches by the type of data they apply to.

Low dimensional data require the least complex approaches to de-anonymize. Sweeney [5] demonstrates that the combination of {ZIP code, gender, date of birth} is enough to uniquely identify 87% of the U.S. population using the Generalized Dirichlet drawer principle (also known as the Pigeonhole principle). Frankowski et al. [9], in one of their experiments, showed that even a simple set intersection is enough to identify a part of the users in a movie ratings dataset just by the movie mentions they made in another dataset.

High dimensional data refers to transaction-like data which contain multiple interactions per user, such as ratings and web browsing history. In order to de-anonymize such data, a model of the user must be built and the de-anonymization method usually depends on similarity between the users in the target dataset and the auxiliary information. The intuition behind such methods is that each user’s behavior is unique. Narayanan and Shmatikov [6] successfully matched up to 99% of the users in the Netflix Prize dataset (movie ratings) to their publicly available IMDB profiles, by applying a scoring function. This de-anonymization could reveal political, religious and societal views of the users that they do not publicly express, but are inferred through their private ratings of movies. Frankowski et al. [9] applied a similar approach for movie ratings and Su et al. [10] for web browsing histories.

Graph data are any kind of data that can be modelled with nodes connected with each other through edges. The most notable cases are the social networks where users correspond to nodes and edges to the relationships between them (uni- or bi-directional). The intuition here is that each user has a distinctive social network and, therefore, social graph. Several approaches have been introduced exploiting the unique structure of the graphs, by trying to match the anonymized graphs to the non-anonymized ones [11].

Some data can be categorized to either high dimensional or graph data depending on the way they are interpreted. Trace data are such an example: Gambs et al. [12] interpret mobility traces as a set of states and transitions and they define several metrics calculating the similarity between the anonymized and non-anonymized traces, while Srivatsa and Hicks [3] interpret mobility traces as a graph consisting of meetings between users and match it to a non-anonymized social network graph.

III. Discussion

The intuitions of the de-anonymization approaches in the literature rely on the uniqueness of the users’ characteristics and if an attack is to be performed on a large scale, a model needs to be built, which is, mostly, more complex than the Generalized Dirichlet drawer principle used by Sweeney to show that 87% of the U.S. population is uniquely identifiable by the combination of {ZIP code, gender, date of birth} [5]. However, an average person with data processing skills would be interested in attacking very specific individuals and his/her attack would not require a complex model to be built and a naive approach might suffice.

Consider this example: An attacker obtains access to an anonymized mobile phone trace dataset which contains the antenna a mobile phone is connected to at certain time intervals. Would it be hard for the attacker to re-identify his/her neighbor in the dataset, if the attacker knows where the neighbor works or where he/she’s been during the weekend? Simple SQL queries to the dataset containing the location of an antenna and time of connection would most probably suffice. As de Montjoye et al. [7] claim: “four spatio-temporal points are enough to uniquely identify 95% of the individuals” in such a dataset.

IV. Conclusion

In this paper, we presented a taxonomy of the research in de-anonymization from an abstract point of view, oriented towards data providers. Specifically, we identified three elements in the de-anonymization process, referenced prior research on de-anonymization and point out that de-anonymization is not as hard as one might think, if one is given strong auxiliary information.

REFERENCES

[1] D. Al-Azzuy, D. E. Millard, I. Symeonidis, K. O’Hara, and N. Shadbolt, “A literature survey and classifications on data deanonymisation,” in CRISS, 2015.
[2] X. Ding, L. Zhang, Z. Wan, and M. Gu, “A brief survey on de-anonymization attacks in online social networks,” in CASeN, 2010.
[3] K. El Emam, E. Jonker, L. Arbuckle, and B. Malin, “A systematic review of re-identification attacks on health data,” PLOS ONE, vol. 6, no. 12, 2011.
[4] S. Ji, P. Mittal, and R. Beyah, “Graph data anonymization, de-anonymization attacks, and de-anonymizability quantification: A survey,” IEEE Communications Surveys Tutorials, vol. 19, no. 2, 2017.
[5] L. Sweeney, “Simple demographics often identify people uniquely,” 2000.
[6] A. Narayanan and V. Shmatikov, “Robust de-anonymization of large sparse datasets,” in S&P, 2008.
[7] Y.-A. de Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, “Unique in the crowd: The privacy bounds of human mobility,” in Scientific reports, 2013.
[8] M. Srivatsa and M. Hicks, “Deanonymizing mobility traces: Using social network as a side-channel,” in CCS, 2012.
[9] D. Frankowski, D. Cosley, S. Sen, L. G. Terveen, and J. Riedl, “You are what you say: privacy risks of public mentions,” in SIGIR, 2006.
[10] J. Su, A. Shokla, S. Goel, and A. Narayanan, “De-anonymizing web browsing data with social networks,” in WWW, 2017.
[11] A. Narayanan and V. Shmatikov, “De-anonymizing social networks,” in S&P, 2009.
[12] S. Gambs, M. Killijian, and M. N. d. P. Cortez, “De-anonymization attack on geolocated data,” in TrustCom, 2013.