Data Protection and Privacy

University of Genoa

Lesson 4: Threats to Anonymized Data

Gaspare Ferraro <ferraro@gaspa.re>

Threat Modeling

- Threat modeling is a process by which potential threats, such as structural vulnerabilities or the absence of appropriate safeguards, can be identified and enumerated, and countermeasures prioritized.
- The purpose of threat modeling is to provide defenders with a systematic analysis of what controls or defenses need to be included, given the nature of the system, the probable attacker's profile, the most likely attack vectors, and the assets most desired by an attacker.

Threat Modeling in Data Privacy I

- Threat modeling helps in identifying possible threats to the system.
- Identifying threats is key to building an appropriate protection mechanism
- With data privacy, threat models include a broad range of de-anonymization attacks.
- 3 different threat levels to analyze:
  - Location and user complexity (adversary) → Background and external knowledge
  - Data structure complexity dimensionality, sparsity, clusters...
  - Anonymization algorithm
- Evaluate the data attack surface → which data are most critical?
- Principle: Understand the sensitivity of data and disclosure risk for a given environment and setting.

Threat Modeling in Data Privacy II

TABLE 4.1

Account Table of a Record Owner

Statistical Properties of Quasi-Identifiers			Correlation between QI and SD Fields	Clusters of Sensitive Data		Statistical Properties of SD Data Set or Individual Sensitive Attribute	
SSN	Name	DOB	ZIP	Gender	Balance	Credit Limit	Available Balance Credit
	John Snow				10,000	20,000	15,000

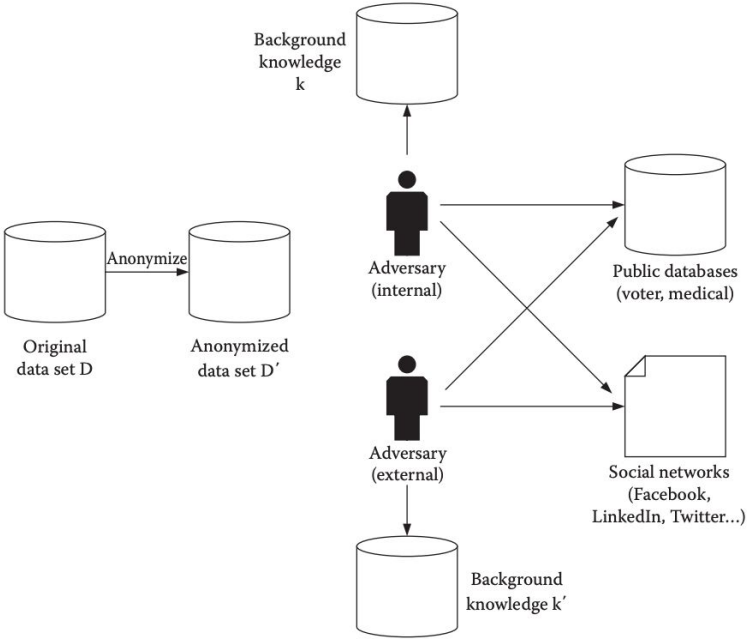
TABLE 4.2

Anonymized Version of Table 4.1

SSN	Name	DOB	ZIP	Address	Gender	Balance	Credit Limit	Available Balance Credit
	Jack Samy					10,000	20,000	15,000

Adversary's Knowledge I

- Adversary has multiple level of information → background and external knowledge



Adversary's Knowledge II

- We make a distinction between external knowledge and background knowledge
  - External knowledge is obtained from external sources (e.g. OSINT)
  - Background knowledge is the information an adversary has about an individual or individuals in the data set.
- Background information could include the distribution (statistical) of quasi-identifiers; for example, it could be the number of people of a specific country in the database or the statistical properties of sensitive data, clusters of sensitive data, and so on...

background information= dati interni, non disponibili all'esterno, fino a che qualcuqno li hackera e li rende pubblici

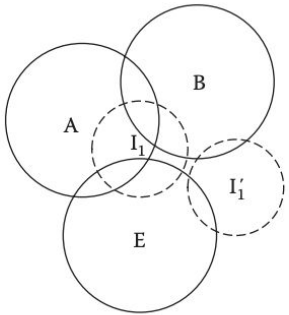
Adversary’s Knowledge III

- Is the adversary external or internal to the organization?
- The background information an internal adversary possesses will be higher than an external adversary does. (E.g. Human resource of a company)
- It is clear that an internal adversary has more background information than an external adversary
- Also, with today’s social networks QI and SD are difficult to separate and depend on the individual

gli attackers possono anche essere dall'interno. oppure aver attaccato una persona della staff e quindi aver poteri particolari e quindi aver info non pubbliche.

Adversary's Knowledge IV

1 In-house (I_1) (internal) Adversary. External Adversary (I'_1)



- Adversary (internal) has application context, background and external knowledge
- Adversary's background knowledge is difficult to model and poses significant threat

Background knowledge of the adversary could include

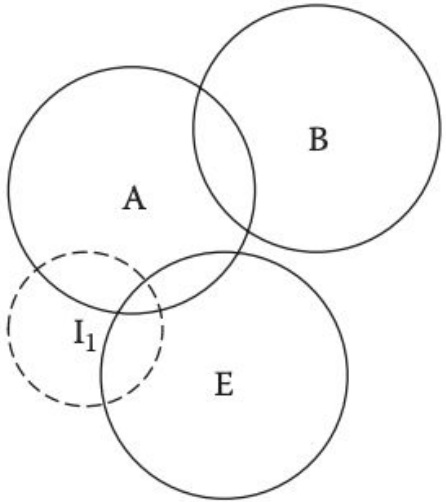
- Identity attributes
- Distribution of identity attributes
- Sensitive data (values of some sensitive data like salary or health issues of some of the users in the dataset
- Distribution of sensitive attribute values like for example, number of patients with HIV in a certain population
- Knowledge of the anonymization algorithm used for data protection
- Outliers in the data
- Associations in the data
- And many more

An external adversary will rely heavily on external knowledge; he may or may not have background knowledge

A: application and organizational context
B: background knowledge
E: external knowledge

Adversary's Knowledge V

2 Offshore (I_2) (internal)

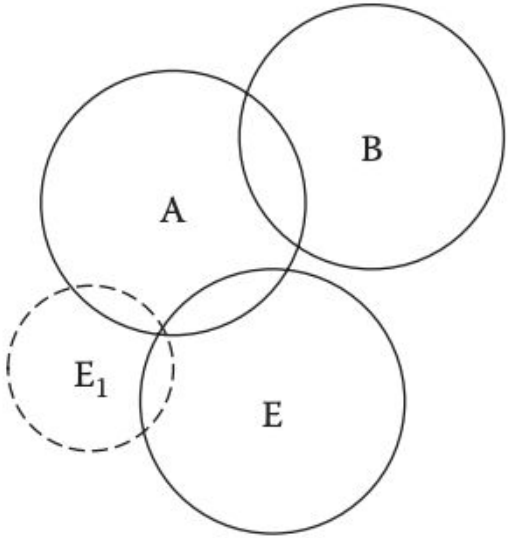


- Adversary will have some or limited application context
- Will rely on external knowledge

A: application and organizational context
B: background knowledge
E: external knowledge

Adversary's Knowledge VI

3 Outsourced (E_1)
(Same Geo)

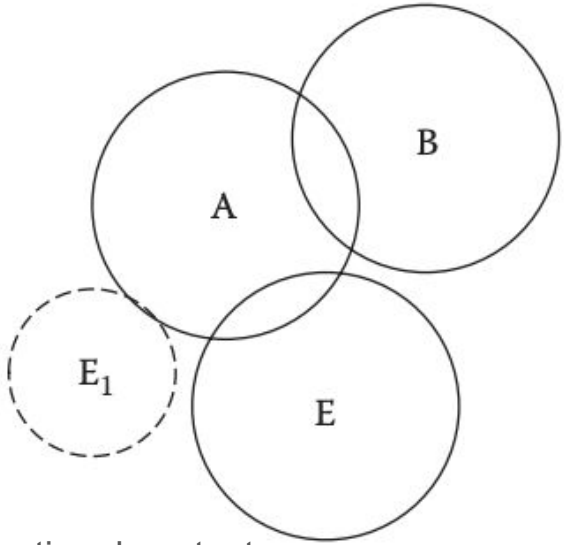


- Adversary will have some or limited application context
- Since he is from same geo, he will have geo context
- Will rely on external knowledge

A: application and organizational context
B: background knowledge
E: external knowledge

Adversary's Knowledge VII

4 Outsourced (E_2)
(Other Geos)



- Does not have application context; no geo or demographics context; no context about culture
- Least harmful when data is anonymized

A: application and organizational context
B: background knowledge
E: external knowledge

Threats to Data Structures

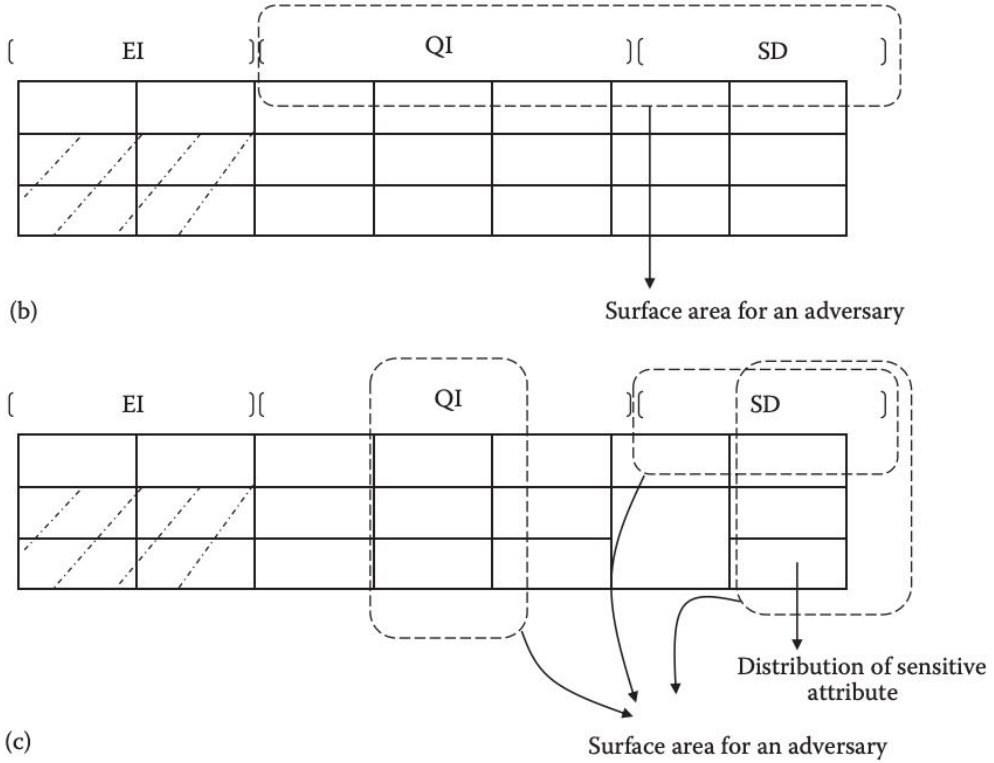
- Enterprise's data can be stored with different data structures (e.g. multidimensional, text, time series, graph data, ...)
- Privacy preservation of complex data structures is a challenge and an open problem as they provide an adversary more info for attack

per esempio le foto di instagram se le scarichi sono anonimizzata per esempio la location, info sul tuo device, ora in cui è fatta la foto . ovviamente queste info alla compagnie rimangono info

Threats to Data Structures: Multidimensional data I

- Multidimensional data can be considered as an n×m matrix, where n is the number of records and m is the number of attributes or columns
- Relational data represented as multidimensional data are the most widely used data structure
- Multidimensional data have three disjoint sets of data: explicit identifiers (EI), quasi-identifiers (QI), and sensitive data (SD)
  - EI by default are completely masked (perturbed)
  - QIs are anonymized
  - SD are left as is to enable analysis.
- Most of the attacks are directed toward QI (identity disclosure) and SD (attribute disclosure)

Threats to Data Structures: Multidimensional data II



Threats to Data Structures: Multidimensional data III

Multidimensional Data and Attack Types

Target	Attack Type
Identity (quasi-identifiers)	Linkage attacks—links to external data sources. This happens when QI attributes can be linked to an external data source.
	Background knowledge attacks.
	Inference attacks—An adversary knows that the record owner is present in the data set.
	Data distribution attack—An adversary has knowledge about the statistical distribution of QI attributes.
	Outlier identification, for example, only Asian in the population.
	Probabilistic attacks.

Threats to Data Structures: Multidimensional data IV

Multidimensional Data and Attack Types

Target	Attack Type
Attribute (sensitive data)	Homogeneity attacks—Presence of clusters in sensitive data records. Background knowledge attack—An adversary has knowledge about a record owner's QIs and knows that he or she is in the data set and some aspect of SD and hence can infer. For example, the adversary knows that Alice (record owner) smokes heavily and also some of her QIs. With this background information, the adversary can infer that Alice suffers from lung cancer by referring to the released medical records. Association attack—An adversary is able to identify shopping patterns of a record owner with the help of background information of the record owner. Data distribution attacks. Outlier identification.

Threats to Data Structures: Graph data I

- Graph is a very complex data structure
- A graph G(V,E) has many vertices V, linked through a set of edges E
  - Many dimensions in a graph that can be exploited by an adversary
- A graph has vertices, sensitive vertex labels, relationship, edge labels, edge weights, and a lot of graph properties that can be attacked by an adversary
- Graph's structural information can be used to attack the graph
- Privacy preservation of graph should ensure that the privacy of individuals, including their properties, should be protected in the anonymized graph, but the aggregate property should be available for analytics and learning

Threats to Data Structures: Graph data II

Graph of Data and Attack Types

Target	Attack Type
Identity—vertex existence	An adversary can use the vertex degree or node degree to identify the existence of a particular individual in the graph network.
Identity—sensitive vertex labels	A vertex represents an individual in a social network. An individual has associated personally identifiable information and sensitive data. The individual can be reidentified using different attack techniques: Identity disclosure—linkage attacks. Identity disclosure—background knowledge attacks. Sensitive attribute disclosure—background knowledge attacks. Background knowledge consists of both attribute knowledge and structural information—attributes of vertices, specific link relationships between some target individuals, vertex degrees, neighborhoods of some target individuals, embedded subgraphs, and graph metrics.

Threats to Data Structures: Graph data III

Graph of Data and Attack Types

Target	Attack Type
Link relationship	Background knowledge attacks—an adversary who attacks a graph always has some background knowledge of the network and the individuals in the network and some properties of the network without which it is difficult to attack an anonymized network. Re-identifying link relationships is generally based on the knowledge of the individuals in the network.
Identity and link relationship identification	Cross-reference attacks—an adversary who wants to identify individuals and their link relationships in an anonymized network G_{main} can use an auxiliary network G_{aux}. The adversary has background knowledge that the individuals are also members of the auxiliary network. He uses this information to cross-refer with G_{main} to identify the individuals and their relationships.
Identity and link relationship identification	Neighborhoods—an adversary has background knowledge of the neighborhood of a target individual.
Identity and link relationship identification	Graph metrics—an adversary uses graph metrics such as closeness, betweenness, degree, centrality, and so on to identify individuals in the network.

Threats to Data Structures: Times Series Data I

- Time series data are characterized by:
  - high dimensionality
  - pattern
  - frequency-domain characteristics
- Anonymization techniques should ensure that all these characteristics are preserved in the anonymized data set
- Conventional anonymization techniques used in relational data will not directly apply here
- Generally, the attacks focus on identity, pattern, and time series values

Threats to Data Structures: Times Series Data II

Time Series Data and Attack Types

Target	Attack Type
Identity	Even though EIs are masked, one could re-identify them using QI attributes. Background information about an entity can be used to re-identify. For example, a patient who has undergone an ECG would not want to reveal or publish his ECG values to others as he feels it is his personal data. But if an adversary knows that the patient has undergone an ECG test, then this is itself a loss of privacy even though the adversary has no knowledge of the ECG values. This is the fundamental difference between anonymity and privacy.
Time series patterns	A time series has a pattern. For example, a car rental company will have a maximum sale during the holiday season. An adversary having this kind of background knowledge will be able to re-identify.
Time series values	Filtering attacks—time series data perturbed with white noise can be subjected to filtering attacks. Specialized filters can be used to remove the noise and reveal the time series values.
Time series values	Regression attacks—time series data perturbed with correlated noise can be subjected to regression attacks. An adversary with some specific values of the time series can build a regression model to predict the values of the time series.

Threats to Data Structures: Longitudinal Data I

- Longitudinal data are extensively used in healthcare domain, especially in clinical trials.
- Longitudinal data are a series of measurements taken over a period of time from a patient in response to medication or treatment.
- The time period is generally not long as in the case of time series data.
- The measurements form the sensitive data set.
- The measurements taken from the patient are correlated with the treatment, and the measurements themselves form a correlated cluster.
- It is very difficult to anonymize a correlated cluster as any change in the values of the reading will affect the pattern of the response, which will lead to incorrect interpretations about the treatment.
- Longitudinal data are simple in structure but have innate complexity in correlated cluster of measurements.
- The threats to longitudinal data occur on both identifying attributes and sensitive data

Threats to Data Structures: Longitudinal Data II

Longitudinal Data and Attack Types

Target	Attack Type
Identity	Record linkage attacks.
	The identity of a record owner can be reidentified using external data if QIs are not anonymized properly.
Sensitive data	Background knowledge.
	An adversary having background knowledge of a patient such as admission date, disease, and so on can re-identify the record owner.
Sensitive data	Probabilistic attack.

Threats to Data Structures: Transaction Data I

- Transaction data are characterized by high dimensionality and sparsity.
  - High dimensionality means that there are too many columns or attributes in the database
  - Sparsity means that each individual record contains values only for a small percentage of the columns.
- Sparsity:
  - increases the probability that re-identification succeeds
  - reduces the amount of background knowledge required in the re-identification process
  - makes it difficult to effectively anonymize transaction data and balance privacy against utility.
- In a transaction database, identifying the sensitiveness of the transaction is important to the adversary.

Threats to Data Structures: Transaction Data II

Transaction Data and Attack Types

Target	Attack Type
Identity	Removing identification information is not sufficient for anonymity. An adversary having background knowledge of a target individual and her shopping preferences could still be able to re-identify.
Sensitive transaction	Background knowledge attacks—an adversary having some background knowledge of a target individual will be able to find the sensitive transaction.