

TOWARDS MEASURING THE LINKAGE RISK IN INFORMATION FLOWS

Christoph Bier¹ and Jürgen Beyerer²

¹ christoph.bier@iosb.fraunhofer.de ² juergen.beyerer@iosb.fraunhofer.de
Fraunhofer IOSB, Fraunhoferstraße 1, 76131 Karlsruhe, Germany

Abstract

Information is one of the most important assets in industry, infrastructures, government, and armed forces. Classified information can be handled according to organizational rules and well-established access control models. However, the free flow of information is a precondition for decision-making and efficient processes in many cases. Hence, lots of information is not classified by default or on such a low level that too many people and systems have access to it. Due to sophisticated analysis methods, this poses risks.

We present a set of unlinkability metrics to determine the overall linkage risk of a collection of information processes. The metrics cover the linkage of storage location, of information flows, of sensitive data, and of sensitive data with (intelligence) sources. We developed a process simulator that allows comparing different process designs a priori and at runtime.

Keywords: Unlinkability; information flow; risk measurement; data protection; classified information.

1 INTRODUCTION

Information is becoming one of the most important assets in our modern world. It must be protected in industry, infrastructures, government, and armed forces.

Classified information can be handled according to well-established access control models. For instance, the Bell-LaPadula model [1] defines two major rules: no read-up and no write-down. Hardware based approaches are available as well. Red-black networks restrict the information flow to flows from the black to the red segment.

However, the free flow of information is a precondition for decision-making and efficient processes in many cases. Hence, lots of information is not classified by default or on such a low classification level that many people and systems have access to it. Due to sophisticated analysis methods, this poses risks. Valuable information can be derived by linking low classified and unclassified information.

The propagation of higher classifications is no solution as well. If more information is highly classified, more people need the clearance for these classification levels. Sometimes people get access to lots of top secret information without any obvious need (e.g., in the Snowden case). Therefore, the aggregation of information in systems and roles must be reduced.

We present a set of unlinkability metrics to determine the overall linkage risk of a collection of information processes. The metrics cover the linkage of storage location, the linkage of information sharing and transfer, the linkage of pre-defined sensitive data, and the linkage of sensitive data with (intelligence) sources. Different process designs can be compared a priori and at runtime. The most unlinkable one can be selected. Others can be ruled out if necessary.

The metrics are based on an analysis of information flows. Therefore, we developed a simulator for exemplary process instantiations. This simulator can easily be fed with all

aspects of the unlinkability model. On top, we present a visualization tool to make the most risky information flows visible to human decision makers.

The remaining part of the paper is structured as follows: In Sec. 2, we discuss existing approaches on measuring unlinkability. In Sec. 3, we present generalized and flexible metric for unlinkability, especially for the linkage risk between systems, sensitive data and (intelligence) sources. We discuss how to determine information flow entropy in Sec. 4. Hereafter, we introduce our simulator for information flows in Sec. 5. This simulator is used for the visualization presented in Sec. 6. In the final section, we conclude with some remarks on future work.

2 RELATED WORK

A reference work on terminology for unlinkability is the continuous updated publication by Pfitzmann and Hansen [2]. Bohli and Pashalidis [3] formalised a hierarchy of unlinkability notions based on a model similar to IND-CPA. They define unlinkability on equivalence relations only.

The concept to describe anonymity based on information theory was brought up by Serjanov and Danezis [4]. Dias et al. [5] added the normalization of the anonymity metric. Steinbrecher and Köpsel [6] transferred the concept to unlinkability. Pashalidis [7] generalised the notion from equivalence relations to arbitrary binary relations.

3 A METRIC FOR UNLINKABILITY

Requirement for the definition of unlinkability is a model of the part of the reality, for which we want to measure unlinkability. In particular, the entities E , their relations R have to be defined. The attacker, from whose perspective unlinkability is determined, must be described.

The linkage of entities can be defined over any mathematical relation R . A linkage relation R is a subset of the cartesian product of $n \geq 2$ subsets $E_1, \dots, E_n \subseteq E$ of the set of all entities E . It is common to choose the entity sets of the entity classes.

Unlinkability can be defined in an absolute or relative way. Absolute unlinkability of two or more entities means that from an attacker's perspective, the attacker cannot distinguish if the entities are in a certain relation to each other or not [2]. In situations where a certain degree of linkability is unavoidable but minimization of linkability is of interest, this kind of metric does not help.

Relative unlinkability compares the uncertainty of the attacker A regarding the true linkage relation R_τ after interaction with the system Σ^A with the uncertainty before the interaction. The uncertainty before the interaction depends on the *background knowledge* (*a priori knowledge*) of the attacker. The attacker can make *observations* I during the interaction with Σ^A . The union of background knowledge and observations is the *a posteriori knowledge*.

Entropy together with Bayesian probability (probability as *degree of belief*) has been established as the state of the art to measure relative unlinkability. Be X a random variable over the set of candidate relations \mathcal{R} . The attacker assigns a probability $P(X = R)$ to every candidate relation $R \in \mathcal{R}$ before and after interaction with Σ^A . $P(X = R)$ is the assumed probability that R is the true linkage relation R_τ between E_1, \dots, E_n .

Therefore, the entropy of the a priori as well as the a posteriori knowledge of the attacker is given as:

$$H(X) = -\sum_{R \in \mathcal{R}} P(X = R) \log_2 P(X = R) \quad [\text{bit}]$$

under the assumption that $P(X = R) \log_2 P(X = R) = 0$ for $P(X = R) = 0$.

The degree of unlinkability is the ratio between the a priori and the a posteriori entropy, given the observation I :

$$\Delta(X, I) = \frac{H(X | I)}{H(X)}$$

As we want to compare different process designs, the background knowledge is set to the observations I_{Ref} an attacker can make when interacting with the reference system, resulting in $H(X|I_{Ref})$ in the denominator and $H(X|I_{Ref}, I)$ in the numerator. As the a posteriori observations might even out the assumed probability distribution, this may result in $\Delta(X, I) > 1$ which is undesirable for a well-defined unlinkability metric. Hence, we define the normalized degree of unlinkability.

The normalized degree of unlinkability considers all possible attackers. As it is always possible to come up with an attacker with no background knowledge, even given the reference system, who can also not observe anything in the considered system, the normalized degree of unlinkability is

$$|\Delta| = \min_A(\{\Delta(X_A, I_A)\}) \in [0; 1]$$

The set of relevant attackers depend on the given scenario. In most cases, it includes the systems taking part in data processing and/or the operators controlling them. Their background knowledge is often defined by the information flows through the respective system based on the reference processes as well as on common knowledge on process design.

We identified the following four relations as most relevant for measuring unlinkability in the setting of classified information:

- The identification relation $R^{ID} \subseteq D \times O$, which expresses if sensitive data $d \in D$ is linked to a particular (intelligence) source $o \in O$.
- The equivalence relation $R^{EQ} \subseteq D \times D$, which expresses if two pieces of sensitive data $d_1, d_2 \in D$ are related to the same (intelligence) source or other relevant attribute.
- The storage relation $R^{SG} \subseteq S \times D$, which characterizes for all systems $s \in S$ if they have processed and/or stored a certain sensitive data $d \in D$.
- The flow relation $R^{FW} \subseteq S \times S \times D$, which represents for two systems $s_1, s_2 \in S$ if they have shared a certain sensitive data $d \in D$.

The last relation is especially important to derive to which degree a given process design supports the separation of concerns when handling classified data.

4 DETERMINING INFORMATION FLOW ENTROPY

The calculation of all possible probabilities $P(X = R)$ is, similar to the interference in Bayesian networks, NP-hard. In worst case, the computational complexity of calculating all probabilities of a binary relation $R \subseteq S \times S$ is in $O(2^{|S| \cdot |S|})$. For the ternary flow relation, the situation is even worse.

To cope with the ternary flow relation, the assumption of independent data flows helps. We assume that any flow of data from one system to another is independent from the flow of other data. In reality, this might not always be the case. Nevertheless, as it is possible to aggregate highly correlated data in one $d \in D$ by definition, the assumption is justifiable. Entropy is additive for independent subsystems. Therefore, we can calculate the total degree of unlinkability of R^{FW} based on the degree of unlinkability per data:

$$H(X^{FW}) = \sum_{d \in D} H(X_d^{FW})$$

Still, we cannot compute $H(X_d^{FW})$ within reasonable time. Fortunately, a heuristic solution is possible, if we add one additional assumption: All data has exactly one source. This assumption is reasonable. If one would collect data from different sources, we would simply not consider it as the same data, either because of the lack of knowledge or because of the different meta-properties of the data. Given this assumption, we can compute the probabilities along the decision tree up to a certain threshold τ . The data source is the root node. The threshold defines the minimum probability taken into account.

Algorithm 1 (Fig. 1) shows how depth-first search in the decision tree works. The tree is traversed until the probability falls below the threshold (line 3). If the current node has no leaf, the remaining subtree will not be searched further (line 5). The probability looked for is directly given by the probability of the subtree. Subsequently, the relation with the highest probability is selected as the representative of the subtree (line 6).

Algorithm 1: compute $\mathbb{P}(R_d^> \mid \sigma)$

```

1 node ← DecisionTree( $\sigma$ ).getRootNode
2 while node.hasNext do
3   while node.hasChild  $\wedge$  node.getProb  $>$   $\tau$  do
4     | node ← node.pollNextNode
5     node.touchChildNodes
6     result ← result  $\cup$  {getMostProbableR (node.getState), node.getProb}
7     node ← node.pollNextNode // poll parent node
8 return result

```

Figure 1 Traversing the Decision Tree

We found out that this approach is feasible, depending on the number of systems, up to a threshold of 10^{-6} . As the heuristic systematically underestimates the real entropy, we can provide a guaranteed unlinkability. For small system sets the underestimation is well below 0,01.

5 SIMULATING INFORMATION FLOWS

We need to define and simulate prototypical processes to compare different process designs a priori and at runtime. Input data for a simulation are the sets of the model (data, systems, and (intelligence) sources) and a description of possible information flows. Our simulator reads all these inputs as csv-files (lists of comma-separated values). Afterwards, the process is simulated and the linkage risk for the respective instantiation is measured. The syntax to describe information flows is as follows:

```

Line = DataInitLine | FlowLine | ClearLine | TimeLine ;
DataInitLine = "d", Number, { ",", Number }, ">", Number ;
FlowLine = Number, { ",", Number }, ">", Number ;
ClearLine = "c", Number ;
TimeLine = "t", Number ;
Number = DigitNotNull, { Digit } ;
Digit = "0" | DigitNotNull ;
DigitNotNull = "1" | "2" | "3" | "4" | "5" | "6" | "7" | "8" | "9" .

```

A DataNitLine defines which data is collected by which system, a FlowLine describes the information flows between systems, while a ClearLine states that data must be deleted from a certain system, resulting in a posteriori gaps in the processing chain. A TimeLine changes the internal clock of the simulator by designating a UNIX time stamp. All data numbers and system numbers used in the flow definition, must also be defined in the respective set files.

The more scenarios are simulated, the better is the validity and the significance of the unlinkability determined. If the results differ from scenario to scenario, the scenarios have to be weighted according to their relevance. As the unlinkability metric is ordinal, one has to be careful not to simply add up the results of different scenarios.

6 VISUALIZING PROCESSES FOR DECISION MAKERS

For simulations, but especially at runtime, it is helpful to visualize information flows to increase the understanding of decision makers towards unlinkability metrics. We developed a web application to inspect the information flows (Fig. 2).

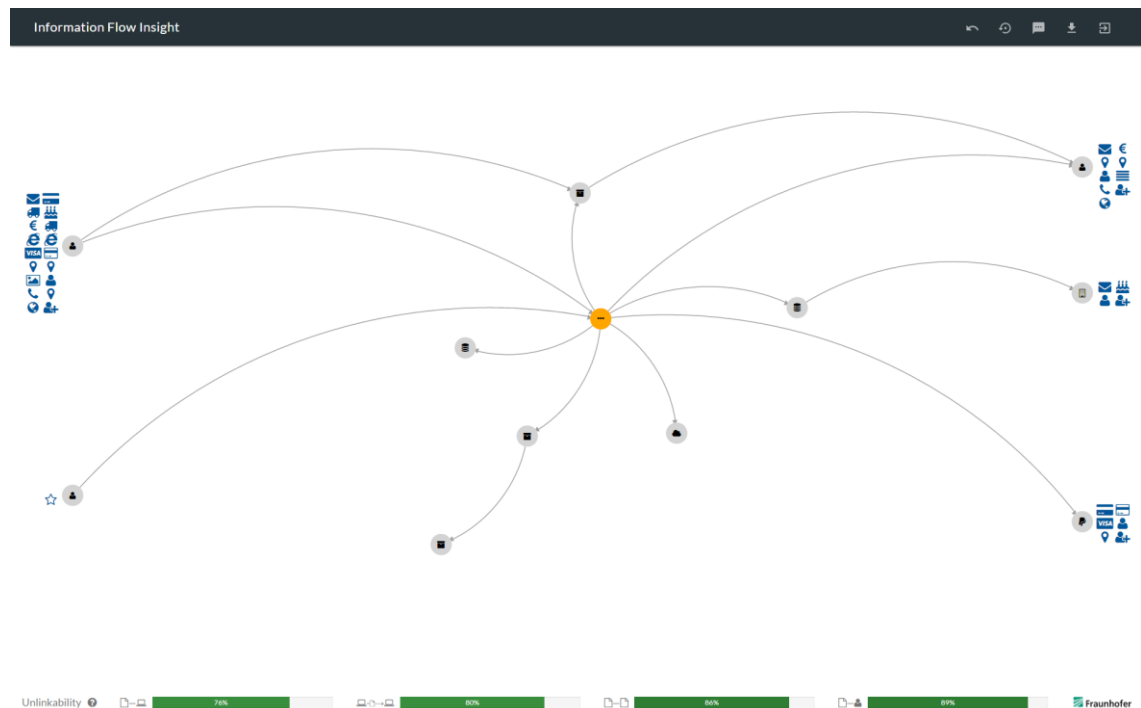


Figure 2 Information Flow Visualization

On the left hand side, one can see the (intelligence) sources. In the middle, the information flows within the organization are visualized. On the right hand side, other organizations or departments, where data has been transferred to, are listed. At the bottom, the unlinkability metrics for the current process design are presented.

7 CONCLUSION

We described an unlinkability metric for the linkage of storage locations, of information flows, of sensitive data, and of sensitive data with (intelligence) sources based on information theory. These metrics were formally introduced. An implementation for information flows, including a simulator and visualizations was presented. These metrics, especially when easily accessible via the web application, allow the improvement of handling of sensitive data in various domains.

REFERENCES

- [1] Bell, D. Elliot; La Padula, Leonard J. (1973). *Secure Computer Systems: Mathematical Foundations*. MITRE Technical Report 2547(I).
- [2] A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf, v0.34.
- [3] Bohli, Jens-Matthias; Pashalidis, Andreas (2011). *Relations among privacy notions*. ACM Transactions on Information and System Security, 14(1), p. 1–24.
- [4] Serjantov, Andrei; Danezis, George (2003). *Towards an Information Theoretic Metric for Anonymity*. In: Proceedings of the 2nd international conference on Privacy enhancing technologies. LNCS, p. 41–53.
- [5] Díaz, Claudia; Seys, Stefaan; Claessens, Joris; Preneel, Bart (2003). *Towards Measuring Anonymity*. In (Dingledine, Roger; Syverson, Paul, Hrsg.): 2nd International Workshop on Privacy Enhancing Technologies (PET 2002). Springer Berlin Heidelberg, p. 54–68.
- [6] Steinbrecher, Sandra; Köpsell, Stefan (2003). *Modelling Unlinkability*. In: 3rd International Workshop on Privacy Enhancing Technologies (PET 2003). Springer, p. 32–47.
- [7] Pashalidis, Andreas (2008). *Measuring the Effectiveness and the Fairness of Relation Hiding Systems*. In: Proceedings of the Asia-Pacific Services Computing Conference (APSCC '08). p. 1387–1394.