Budapest University of Technology and Economics
Faculty of Electrical Engineering and Informatics

Department of Networked Systems and Services
Mobile Communications and Quantum Technologies Laboratory (MCL), and
Laboratory of Cryptography and System Security (CrySyS)

Protecting Privacy Against Structural De-anonymization Attacks in Social Networks

Thesis booklet
by

Gábor György Gulyás

Research Supervisor:

Sándor Imre, DSc.

2015

1 Introduction

Social media services are used every day by hundreds of millions, or even more. However, beside the values these services give to humanity, social media also serves as an optimal platform for all kinds of surveillance activities, as members can snoop upon each other, commercial parties can access vast amounts of private data, and as recent events confirm [1], government surveillance is also present as well. Social networks are definitely one of the key ingredients in shaping our societies today, accelerating the shift from information societies to surveillance societies [2].

Due to the variety of privacy problems emerging in social networks [3, 4], there is also myriad of related privacy-enhancing technologies (PETs). One of the most challenging tasks is to make identification with structural properties of nodes cumbersome, or even impossible. There are solutions aiming to solve this by proposing replacement of centralized social networks with distributed platforms or modify the functionality social networks in fundamental ways, eventually requiring the migration of users to novel services to maintain their privacy (e.g., to distributed social networks such as Diaspora [5]). Another line of research constructs techniques that could be put into use by social network providers to release meaningful but still private data (e.g., by using differential privacy [6]).

However, we need solutions that can be adopted gradually, thus allow contacting others who have not yet taken steps to strengthen their privacy, but yet enhance the users' privacy. Most large social network providers can be forced to handle user data out to governments, and cannot be accounted for how they share user data with third parties. Therefore, the control of anonimization need to lie in the hand of the users – even if we could assume that centralized data sanitization would be possible with an acceptable trade-off between utility and privacy.

In addition, there are several systems, where connections between entities are not considered as an explicit feature, while this kind of meta-data yet provides means of identification. Such attacks have been demonstrated for location privacy, where it has been shown that co-location information in spatio-temporal dataset can be used to reconstruct the underlying social network, and finally structural information crawled from social networks can be used to identify users [7–10]. These and similar cases yield for solutions described above, where the privacy control lies in the hands of users.

2 Motivation

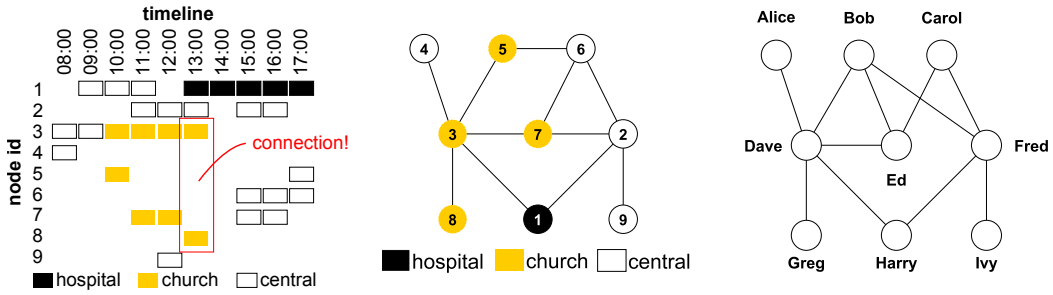
Datasets are usually protected by naive anonimization when shared with business or research partners: explicit identifiers are removed (such as names, user ids or email addresses), and the graph structure is slightly perturbed (e.g., a small fraction of edges are removed or added). Unfortunately, naive data anonymization techniques cannot provide an acceptable level of protection, as several works have proven that nodes in sanitizated datasets can be re-identified with high accuracy [8, 10–19]. Most of these methods are capable of achieving large-scale re-identification of social datasets consisting even of hundred thousand records (or more).

In particular, in my work I consider a strong class of attacks, where de-anonymization is executed by using structural information only [8, 10–15]. The following example demonstrates the core principles of these attacks, when identities that were not present in the original datset are recovered [10, 12]. It also gives an insight of the privacy threat when co-location information in spatio-temporal datasets (like mobility traces or check-ins) are converted into a social network graphs [20] to be re-identified as a social network.

Let us consider an attacker who obtains spatio-temporal data as given in Fig. 1a. For example, the attacker could buy this data from a Wifi service provider of a small city, who intentionally collects device identifiers that pass by their access points placed at different locations (e.g., smartphones with Wifi turned on). After buying the dataset, the attacker can create an anonymous social graph as Fig. 1b based on the co-occurences of each identifier at the same place and time slot. From a business point of view, the resulting dataset would be even more valuable for the adversary if it could label each node with a publicly known identity.

After crawling social relations from another source, for instance from a publicly available online social networking site (including only users who claim to live in that small city), the re-identification process can be done by the attacker in two steps. The background knowledge, or auxiliary dataset is shown in Fig. 1c. First, the attacker can search for nodes with outstanding properties, like using node degree as in this case. By searching for unique, high degree nodes the attacker can create a re-identification match between the nodes $v_{Dave} \leftrightarrow v_3$ and $v_{Fred} \leftrightarrow v_2$. As no more of such mappings can be found, next nodes related to existing mapped ones can be re-identified. For example, v_{Harry} has two connections (which is not unique globally), and he is connected to both v_{Dave}, v_{Fred}; this boils down choices to the re-identification mapping of $v_{Harry} \leftrightarrow v_1$.

After deriving conclusions from the results of the attack, the attacker can now maliciously use the fact that Harry visited the hospital for several hours, such as blackmailing



(a) Anonymized spatio-temporal data

(b) Underlying social network reconstructed from (a)

(c) Crawled public network (as auxiliary data)

Figure 1: For example, an attacker can buy anonymized spatio-temporal data for business analysis (a), from which co-occurences can be used to reconstruct a possible underlying social network (b). Next, structural information crawled from a public social networking site (c) can be used to re-identify nodes in the sanitized dataset.

Harry with publishing this information among his friends or employer, or can be used for sending unsolicited advertisements with personally-tailored content.

In order to remedy the present situation, the analysis of a user centered technique is in the focus of my dissertation, called identity separation. This technique could be applied to existing services without modification of the service itself, even without getting the consent of the service provider, and can be deployed gradually. Identity separation is based on the concept how we use our real identities in everyday life: we share different information in different situations and with different acquaintances [21]. This can also be applied to social networks to segregate information with different groups of contacts.

Returning to the previous example, identity separation could be applied by using different identifiers in different contexts, e.g., changing the MAC, or using different user names for check-in services. For example, Harry could change his MAC address when arriving at the hospital (or turn off wireless totally), in order to avoid this information being linked to his identity.

3 Research objectives

Structural re-identification of social networks is a rather new and actively researched area within the field of social network privacy. The first and yet state-of-the-art attack that enabled large-scale re-identification of sanitized social networks was designed by Narayanan and Shmatikov in 2009 [12], opening up several new lines of research (later it is also referred as Nar09). In my thesis I deal with the following problems, of which all are related to

structural re-identification attacks.

Problem Set 1. *Analysis of re-identification algorithms.* Several areas need further research related to these attacks, and I focused on two issues related to my work: on measuring anonymity and initialization of attacks. In the first case my goal was to reveal how anonymity could be measured respecting these attacks, as setting up and measuring anonymity sets in this case cannot be done by trivial means. In the second case, my goal was to determine how seeding affects the overall performance of the attack. Works in the literature used several methods for initialization, but there was no conclusive analysis that could help in differentiating between them.

Problem Set 2. *Evaluation of identity separation as a tool for defeating de-anonymization attacks.* Identity separation seems to be a suitable privacy-enhancing technique within the current context. However, it is essential to provide a validation to see if it is suitable against re-identification. Here, my goal was to answer two key questions. Primarily, under what conditions and with which strategy it is possible to defeat the attack on the network level? Then what is the privacy loss of the participating users?

Problem Set 3. *Evaluation of individual strategies for the minimization of information disclosure.* Even if turns out that stopping the attack is feasible in a given context, a user could decide that he would rather aim for individual privacy protection. Several issues emerge in this problem set. Are there feasible strategies providing data minimization if only a few users adopt it? If yes, can an adversary somehow reverse the identity separation process, and link partial identities to a public identity? Beside answering these questions, I also aim to find strategies that provide theoretical guarantees.

4 Methodology

I used simulation experiments in my dissertation, as this approach is the typical tool used in the field of the analysis of privacy issues in social networks. Besides, I also applied analytic solutions to some problems as well. As there are no datasets providing enough details for modeling identity separation (and obtaining one is beyond the scope of the current work), I designed a behavior model that could be used in both analytic and experimental cases. I also provided the necessary details for maintaining the repeatability of my simulation experiments, which were carefully selected to exclude possible biases, e.g., due to network structure or the number of experiments. I used simulation experiments in all three *Problem Sets*. In *Problem Set 2*, I used statistics and numerical analysis for analyzing failure probability of the attacker. In *Problem Set 3*, I developed an anonymity scheme based on the concept of the k-anonymity model [22]. I also used statistics and

game theory for researching suitable privacy-enhancing strategies.

5 New results

In simulation experiments I used two measures for assessing the extent of what the attacker could learn from an attack. The *recall rate* reflects the extent of re-identification, describing success from an attacker point of view (i.e., breaching network privacy). This itself can be used due to small error rates. As identity separation is an individual information hiding tool, the quantity of information the attacker gained access to should also be concerned, which is quantified by the *disclosure rate*. This describes an overall protection efficiency from a user point of view.

5.1 Analysis of Structural Re-identification Algorithms

I studied important properties of structural re-identification attacks that bear greater importance for my research. I proposed a class of anonymity measures that can be used within the current context, and then evaluate instances of this anonymity class for the Nar09 attack. These measures show which nodes are important in the network: these are the ones that are likely to be re-identified by an attacker. I argued the importance of seeding, which I characterized for multiple cases for the Nar09 algorithm how initialization effects the overall performance of the algorithm.

Thesis Group 1. *I analyzed structural re-identification attacks. I proposed a family of anonymity measures called Local Topological Anonymity (LTA), and showed that both a given LTA variant and node degree can effectively show which nodes are more likely to be re-identified by the state-of-the-art attack. With the same attack, I characterized the importance of seeding and showed how different methods significantly bias overall results.*

Thesis 1.1. *I proposed a family of measures called Local Topological Anonymity (LTA), that enable the relative assessment of the risk of re-identification for a single node. I showed that there is a particular variant called LTA_A which provided values that had strong rank correlation with node re-identification rates for the state-of-the-art and Grasshopper attacks.*
Related publications: [C3, J2, J3]

Large-scale structural re-identification attacks compare nodes against their 2-neighborhoods in their local re-identification phase, therefore, the more similar a node

is to its neighborhood, the lower chance it has for being re-identified. This property need to be captured by anonymity measures, which I introduced as Local Topological Anonymity (LTA).

Definition 1. *A Local Topological Anonymity measure is a function, denoted as LTA$(\cdot)$, which represents the hiding ability of a node in a social network graph against attacks considering solely the structural properties of the node limited to its d-neighborhood*[1].

Nodes are compared to their neighbors by using structural similarity functions, which can be measured in many ways. Nar09 compares the sets of neighbors of nodes (of G_{src}) to the neighbors of their friends-of-friends (in G_{tar}). While in other attacks this could be done otherwise, the concept of LTA need to be easily adoptable for these cases. Thus an LTA variant adopted to a given attack can be defined as follows:

Definition 2. *A Local Topological Anonymity measure variant α is a function, denoted as LTA$_\alpha(\cdot)$, which is an LTA measure that is based on the node fingerprint function $f_\alpha(\cdot)$ representing the structural fingerprint of a node in a social network graph.*

I proposed three variants based on $CosSim(\cdot)$ (which is used for similarity measurement in Nar09, and can be replaced for other algorithms). LTA$_A$ specifies the average similarity of a node compared to others in its 2-neighborhood (i.e., friends-of-friends):

$$\mathrm{LTA}_A(v_i) = \sum_{\forall v_k \in V_i^2} \frac{CosSim(v_i, v_k)}{|V_i^2|}, \tag{1}$$

LTA$_B$ uses a different normalization scheme than LTA$_A$, i.e., the degree of the node, but at least two. LTA$_C$ further divides LTA$_A$ with the standard deviation of the difference in degree values between v_i and members of V_i^2, which is the set of the neighbors within two hops. Formulas of these measures are provided in the dissertation.

I compared the re-identification results of the state-of-the-art on perturbed datasets originated from multiple networks, where I applied the Spearman's rank correlation (denoted as ρ_S) [23] of node re-identification rates and their LTA values. An acceptable LTA measure should have a correlation value that has an absolute value close to one. Finally, from the three proposed variant LTA$_A$ turned out to have best correlation results. Results are shown in Fig. 2.

[1] In my work I used $d = 2$ as using larger distances are not feasible due to small network diameter.

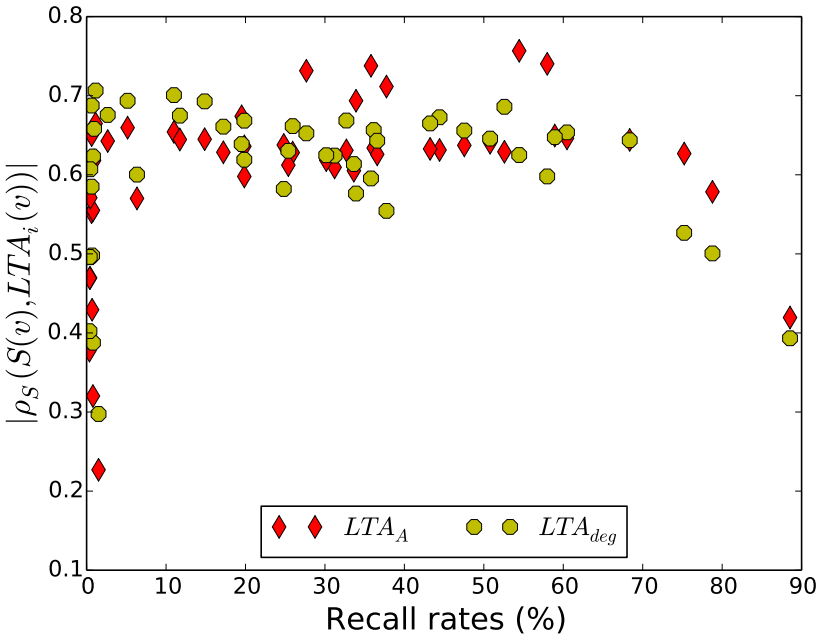


Figure 2: Comparison of LTA variants with different perturbation settings, and their relation to recall. Measures LTA_A and LTA_{deg} both have the most competitive correlation values.

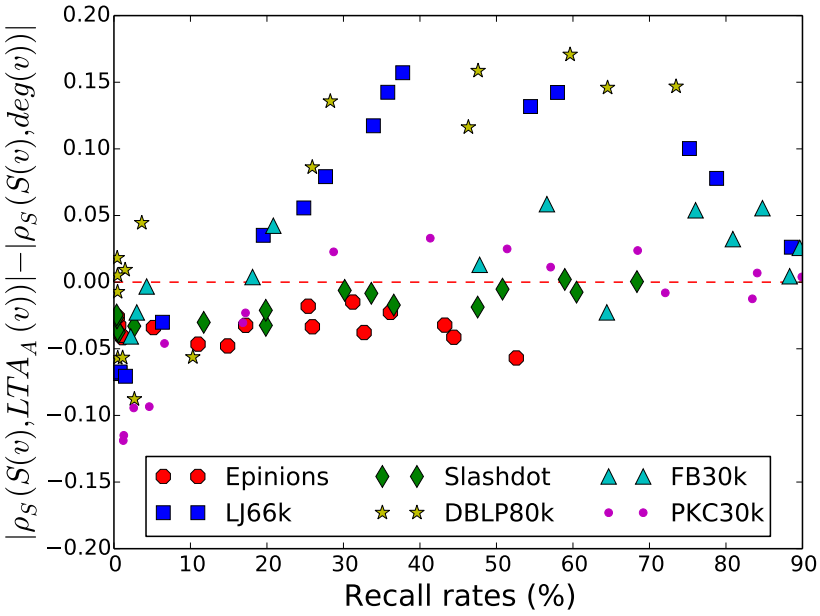


Figure 3: There is a notable difference between LTA_A and LTA_{deg}, depending on the network structure. In Epinions, Slashdot LTA_{deg} proved to be better, while in others LTA_A.

Thesis 1.2. *I showed that node degree (LTA_{deg}) is an efficient, easy to calculate alternative for LTA_A. I additionally showed how degree distribution of networks determines which metric should be used for the state-of-the-art attack: LTA_{deg} in networks where the proportion of low degree nodes are relatively high, and LTA_A in others.*
Related publications: [J2, J3]

Node degree is an important property regarding re-identification rates, and according to my measurements, Nar09 is biased to re-identify nodes with higher degree. For example, in a measurement less than 20% of nodes with $\deg(v) \leq 3$ were correctly re-identified, while this was around 80% for high degree nodes. Therefore, in my dissertation, I additionally proposed to evaluate node degree as an anonymity measure. This is denoted as LTA_{deg}. Results in Fig. 2 show that node degree also provides promising correlation values.

Correlation values of LTA_{deg} were higher in some networks than LTA_A; however, differences turned out to be consistent depending on the degree distribution of the network for the state-of-the-art attack. In my dissertation, I showed that there is a significant overlap (ca. 80%) between the nodes highlighted by top degree and bottom LTA_A. Furthermore, I showed that biases occur respecting the network structure: LTA_A provided higher correlation in networks where degree distribution is shifted towards having more high degree nodes. Further details are provided in my dissertation.

Thesis 1.3. *For the state-of-the-art algorithm, I characterized the importance of initialization. I showed how the maximum number of re-identified nodes can depend on the seeding method and its parameters. I have characterized how the minimum number of seed nodes depends on network properties and the seeding method. I also characterized seed stability and showed that even an extremely low number of seed nodes can also lead to large-scale propagation.*
Related publications: [C1]

Related to the effect of seeding on propagation, Narayanan and Shmatikov highlight in [12] that seeding has a phase transition property regarding the number of seeds [24]: at some point while increasing the number of seeds, there is only a little difference when the output of propagation rises significantly, reaching the maximum. They also note (without details) that transition boundaries depend from networks structure and seeding method. Seeding stability is also mentioned in their paper as the probability of large-scale propagation with respect to the number of seeds. However, beside these suggestions (lack significant details) most related works do not justify the seeding method they use.

The phase transition property and several other properties of seeding are illustrated in Fig. 4. In my dissertation I showed that global properties of the seed nodes (e.g.,

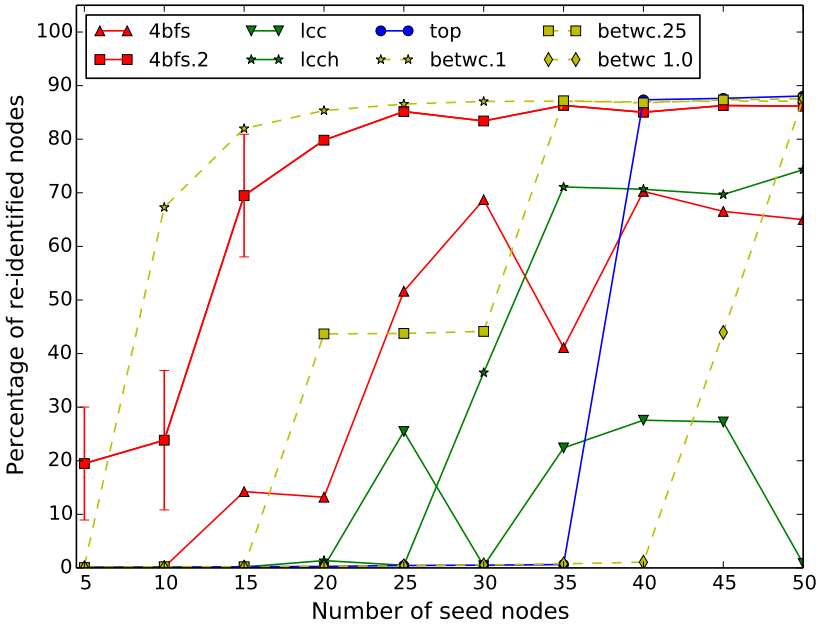


Figure 4: Differing characteristics of seeding strategies depending on seed size (here the network consists of ca. 10k nodes).

having high degree or high betweenness value), the relation between seed nodes (e.g., clique structure or neighbors only) determine the number of minimum required seed set size for large-scale re-identification. In addition, large-scale propagation is not always possible with reasonable seed sizes for some methods, e.g., Fig. 4 also shows this for `lcc`. More details are provided in my dissertation.

5.2 Evaluation of Identity Separation

The concept of how identity separation could be used in social network based services is introduced in [C7, C8], and in my work I used a statistical model capturing possible user behaviors in four sub-models that was originally published in [J4]. These modeling issues are described in details in the dissertation; however, from a bird's-eye view, it works as follows. A user v_n creates $Y = y$ new (externally unlinkable) identities and sorts the original edges (contacts) among the new identities. The proposed identity separation models differ in that if duplicating (adding an edge to multiple identities) and deleting (edge anonymization) edges are allowed or not.

This leads to four possible sub-models. I have named the model with no edge deletion, and no duplication the basic model, since this allows the least functionality for the user. Conversely, the realistic model is the opposite: it implies the fewest limitations on user

actions. Users of a social network would likely use the functionality of this model (e.g., duplication of some edges and the deletion of others); hence the notation realistic. Besides, a worst and a best model also exist, which are also named from the user-centered point of view. The best model allows a user to only decrease the number of his contacts, and therefore causing more information loss to the attacker, therefore preserving more privacy. The worst model only allows creating multiple connections between identities and acquaintances, therefore making "backups" of structural information, and helping identification.

In this thesis group I dealt with the question how identity separation could be used to defeat re-identification at the network level. First, I analyzed resistance against seeding, then against propagation phase. In the analysis of propagation phase, I dealt with a non-cooperative setting, where users are considered to adopt identity separation independently of each other. I also analyzed some cooperative settings, where cooperation is organized locally and globally in the network and the privacy-enhancing technique is adopted according to collectively pursued strategies.

Thesis Group 2. *I analyzed the possibility of defeating re-identification by using identity separation as a privacy-enhancing tool. Based on the models I proposed, I characterized and analyzed attacker failure probability when identity separation is adopted against seeding. With simulation experiments I analyzed multiple non-cooperative and cooperative identity separation strategies to determine which approaches can significantly decrease attacker recall rates, or keep disclosure rates of private information at low levels.*

Thesis 2.1. *I provided the general formula of failure probability of global identification (seeding) when identity separation is used. Using this formula, I elaborated the lower estimate of failure probability for clique-based seeding, and for a seeding method identifying top degree nodes. I showed with numerical analysis that there are efficient strategies for users to protect themselves with identity separation against these seeding methods.*
Related publications: [J4]

The probability of failure of seeding for a node v_n (based on the assertions of the model) can be described by using the law of total probability as

$$P(\text{"failure"}) = P(Y = 0) + \sum_{y=1}^{\deg(v_n)} P(\text{"failure"}|Y = y) \cdot P(Y = y). \tag{2}$$

This formula can be expanded based on the given user behavior model currently analyzed. The state-of-the-art attack compared 4-cliques in the seed matching phase. There-

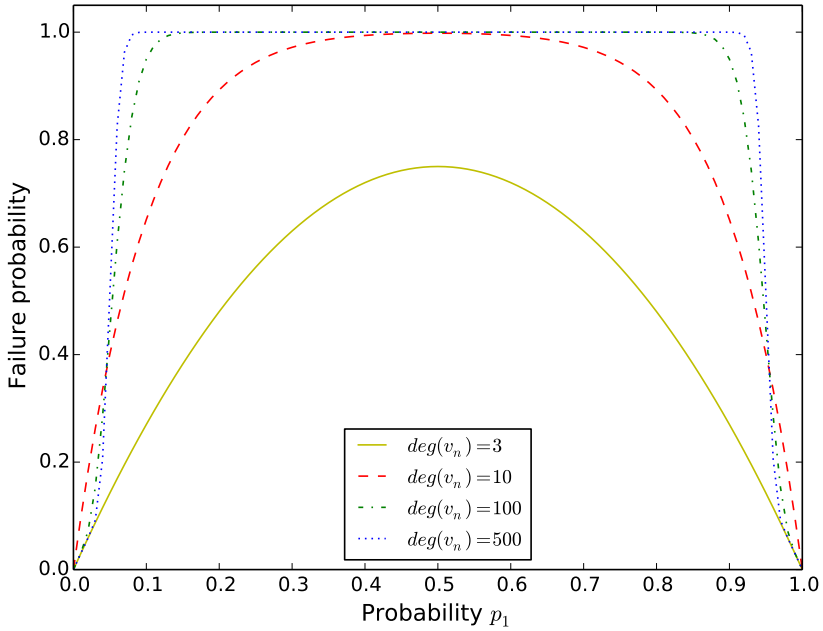


Figure 5: Basic model parameter analysis of $\deg(v_n)$: $P^B_{clique}(\text{"failure"}|Y=2)$ as a function of p_1, with fixed $k=4$ and $\epsilon=0.05$ with different values for degree.

fore in the dissertation I provided the analysis of clique based seeding methods (keeping the clique size as a parameter k) on two models: on the simpler basic model and with the realistic model. I have shown that for both models there is a great variety of strategies that lead to high failure probability (i.e., practically 1.0) even if only two partial identities are used (later denoted as $Y=2$). Fig. 5 shows an example on related parameter analysis, where the underlying formula derived from (2) is the following:

$$P^B_{clique}(\text{"failure"}|Y=y) = 1+\sum_{\forall i\in[0,\dots,y]} p_i^{k-1}\cdot\left(\sum_{x''_1+\dots+x''_y=n-k+1}\left(\frac{(n-k+1)!}{x''_1!\cdot\ldots\cdot x''_y!}\cdot p_1^{x''_1}\cdot\ldots\cdot p_y^{x''_y}\cdot e(k-1,x''_i)\right)-1\right) \tag{3}$$

where p_i probabilities (i.e., the probability of an edge is sorted to partial identity indexed by i) provide the basis of a multinomial distribution ($\sum p_i=1$).

I also provided the analysis of a seeding method (where formulas are derived from (2)), where the attacker maps the top degree nodes of two networks as the initialization of the de-anonymization attack. For a particular case, I showed that for the majority of nodes

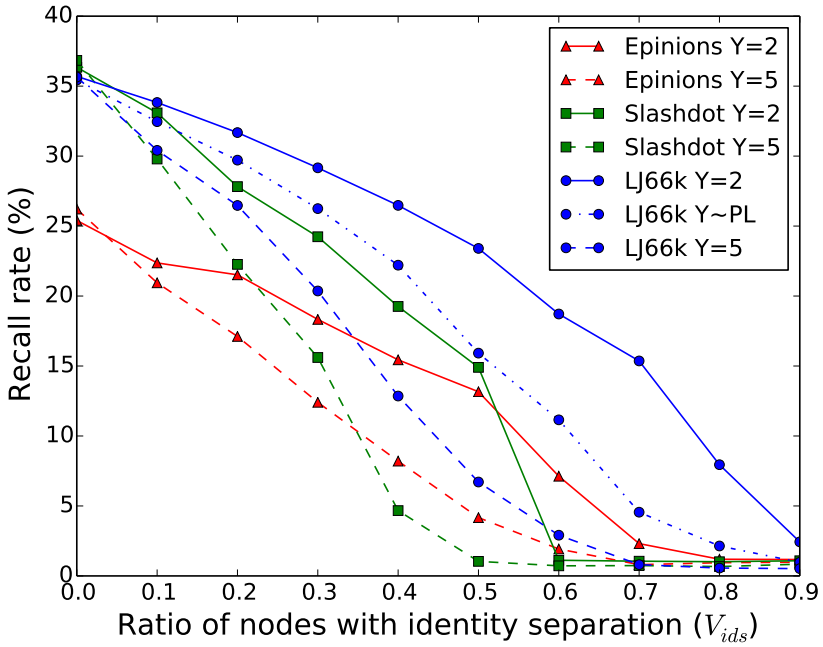


Figure 6: Experimental results using the basic identity separation model displaying effect of node splitting against re-identification.

(80.4%) of the top 1000 nodes can have high failure probability even when using only two partial identities. Using the approach and identity separation models I provided (in the dissertation), similar failure probability analysis can be done on further cases of global node identification (or seeding) methods.

Thesis 2.2. *I measured the sensitivity of the propagation phase of the state-of-the-art attack against features of identity separation, and showed the attack is quite robust: a high number of non-cooperating users need to participate to decrease the number of correctly re-identified nodes significantly.*
Related publications: [C2, J1, J3]

In order to be able to discover the strongest privacy-enhancing identity separation mechanisms, I investigated the efficiency of features in different models against the Nar09 algorithm. First, I tested the sensitivity of node splitting by simulation of the basic model (see Fig. 6 for results). Against initial expectations, the basic model turned out to be ineffective in stopping the attack: in all cases the majority of users (i.e., 50% and above) needed to adopt the technique for stopping the attack.

I executed simulations with different models allowing deleting edges (with $Y = 2$), and found that recall rates strongly resemble results of the basic model while being a slightly

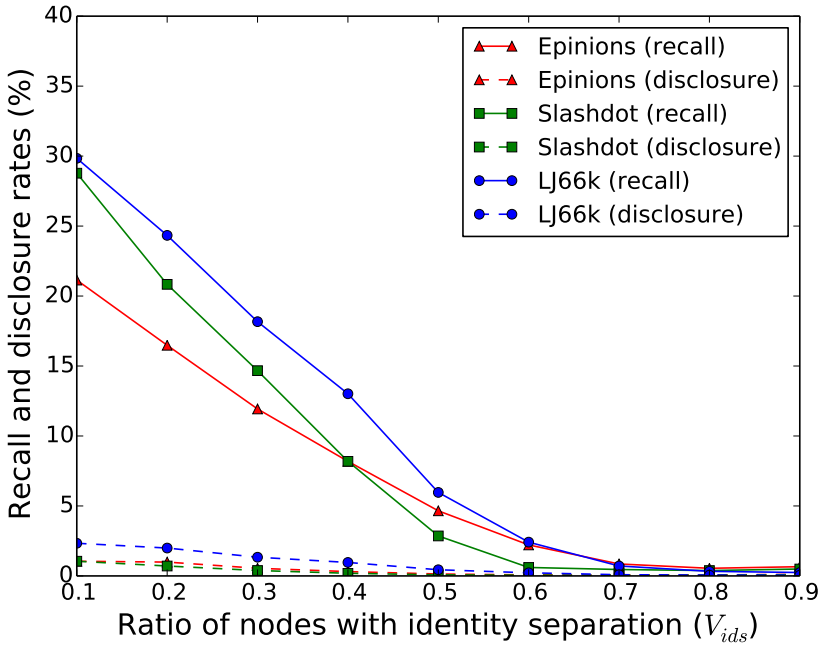


Figure 7: Allowing edge deletion with $Y = 5$: network privacy can be still breached until large-scale adoption. Results for protecting individual privacy are promising.

better; thus, these models are also incapable of repelling the attack on the network level. These results showed that another strategies need to be researched for stopping the attack on the network level. Besides, disclosure rates showed promising results which I also further investigated.

Thesis 2.3. *I characterized several properties of non-cooperative identity separation. In particular, I showed that even if the attacker changes the seeding method or seed size, he cannot significantly affect his results against identity separation used in the network.*
Related publications: [C2, J2, J3]

Based on previous results, I analyzed further strategies of identity separation. One of the most interesting findings is that using the basic model with $Y = 2$ is counterproductive: such users have higher recall rates than the network average (detailed elaboration of this issue is provided in the dissertation). In addition, I shown that even the best model with $Y = 5$ (see Fig. 7) can preserve network privacy only when majority of users participate. However, using strategies according to this model showed to provide an acceptable level of data minimization: the attacker could only reveal less then 3% of information of the users adopting the technique.

In coherence with the discussion related to Thesis 1.3, I analyzed multiple seeding

methods as part of the attacker model. In these experiments, only minor differences were observable when using different seeding methods. However, due to their robustness advanced methods turned out to be a better choice in two cases: when a higher ratio of users apply identity separation or if only a low number of seeds can be identified. Corollary of these findings is a malicious party can search for a seed set consisting of a low number of nodes on a trial-and-error basis until large-scale propagation appears. In the dissertation I provide details how stability of small seed sets vary w.r.t. the level of perturbation added by identity separation. I also dealt with the opposite case, an attacker having a larger seed set; it turned out that increasing the number of seed nodes cannot effectively increase recall rates.

Beside these findings, I have analyzed several other aspects of identity separation for which the details can be found in my dissertation.

Thesis 2.4. *I showed that even for a simple local cooperation scheme, a lower number of participants are enough to defeat re-identification compared to the non-cooperative setting.*
Related publications: [J1]

In previous measurements I showed that non-cooperative identity separation cannot defeat the attack on the network level. Therefore, I investigated multiple cooperative models, focusing on the analysis of local cooperation first. I modeled a simple local cooperation scheme including a sizing parameter n: a node is randomly selected, and then $n-1$ nodes are sampled from its neighborhood. One could expect that this scheme would provide similar results as non-cooperative identity separation, as the scale of the effect of such cooperation is small and limited regarding from a global point of view.

However, experiments proved the opposite. I evaluated this scheme for $n \in \{5, 10, 25\}$ with the basic model with $Y = 2$ and the best model with $Y = 5$. Results for $n = 10$ are shown in Fig. 8. In experiments with higher values of n, I showed that the minimum number of required participants can be decreased.

Thesis 2.5. *I showed that by using LTA_A and LTA_{deg} as a global node-selection heuristic for cooperative identity separation, the required number of participants is a small fraction compared to the non-cooperative case. In addition, I showed that changing seeding method or increasing seed set size cannot significantly enhance the attacker's results.*
Related publications: [J1–J3]

With simulations I experimentally analyzed global cooperation. I used measures of node importance to select nodes for cooperation, for which I used two predictive measures on re-identification, LTA_A and LTA_{deg} measures. In the measurements, nodes were selected

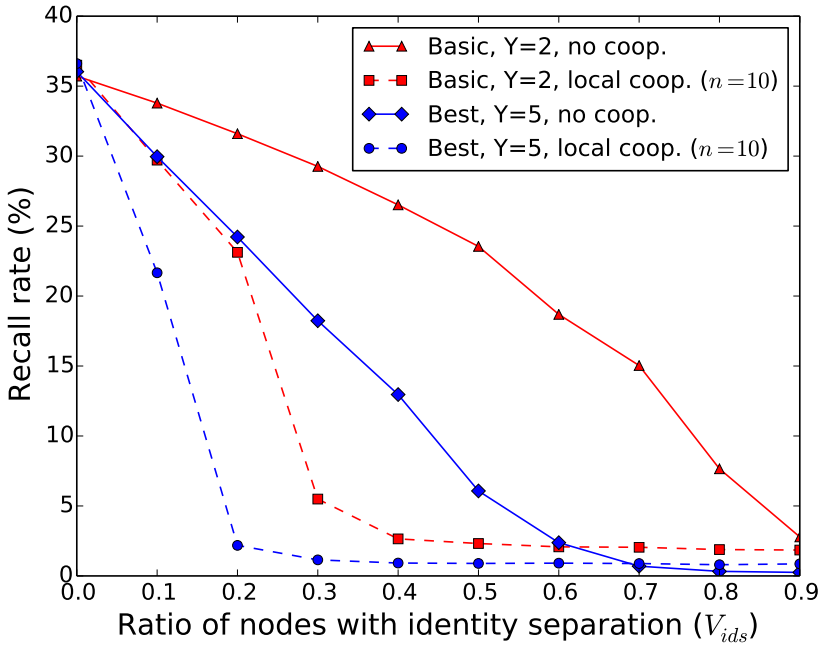


Figure 8: The effect of local cooperation compared to the non-cooperative settings in the LJ66k dataset.

to adopt identity separation that had lowest LTA_A or highest LTA_{deg} values. In both cases the minimum number of participants for stopping the attack significantly decreased compared to the non- and locally cooperative cases as Fig. 9. Efficiency depending on heuristics varied for networks, differences were not consistent with the correlation values observed for the importance measures. As a conclusion, I concluded that using global cooperation is advised for tackling the attack on the network level.

Further details on the evaluation are provided in the dissertation.

Thesis 2.6. *I showed that both for non-cooperative and globally cooperative identity separation the participation of top degree nodes is crucial. Without their support, the performance of protection of network privacy degrades rapidly.*
Related publications: [C2, J1, J3]

Previous cases are based on the assumption that all users would adopt the technique to stop the attack. However, in a real life scenario it is likely that only a subset of the selected users would participate. Furthermore, the high degree nodes are the ones that are more likely to skip cooperation, e.g., because such users do not want to divide their audience. On the contrary, we could expect that these users to use less visible solutions, such as decoys to hide their more privacy-sensitive activities.

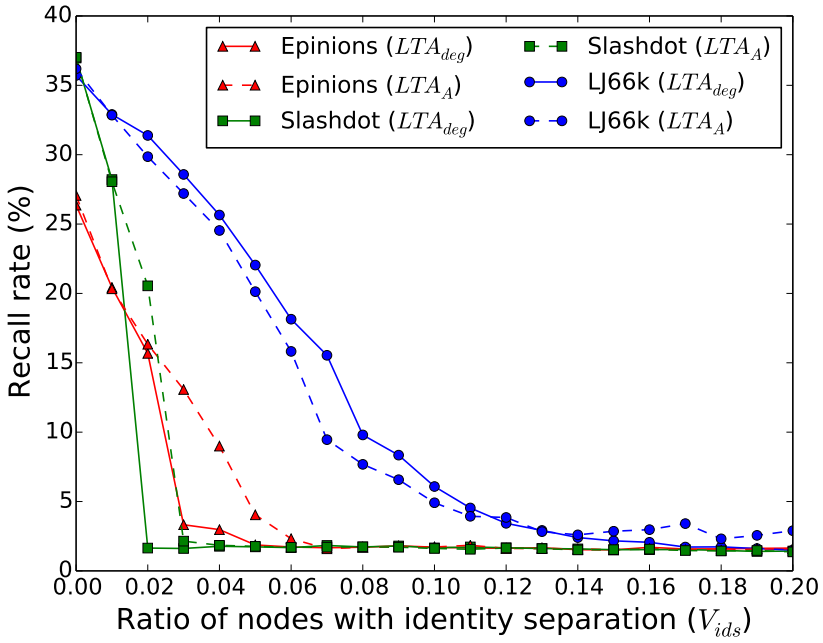


Figure 9: Comparison of results between cooperation organized by LTA_A and LTA_{deg} in the best model, $Y = 5$. Dashed lines represent results for LTA_A, and solid ones are for LTA_{deg}.

I showed how it affects the overall results if a given percent of the top degree nodes do not cooperate with others. I showed that even if only 1% of top degree users refuses cooperation a significantly larger ratio of users need to be involved for successfully tackling the attack in all cooperation cases. For example, some results for the non-cooperative setting are shown in Fig. 10, detailing both recall and disclosure rates in the Slashdot network (best model, $Y = 5$). To the contrary, the best model provided acceptable results for individual privacy. This leads to the conclusion that even if despite the best intention of participating users, network privacy could not be protected, their privacy will be still preserved with high probability. I provide further details on the comparison in the dissertation.

5.3 Evaluation of Individual Strategies

In Thesis Group 2 I showed that the state-of-the-art attack is robust against several strategies of identity separation. While I also showed that there are cooperation models allowing to stop the attack, these strategies are fragile: they need the participation of top nodes. Therefore, in the last part of my dissertation I dealt with the analysis of individual strategies that could improve previous results on individual privacy.

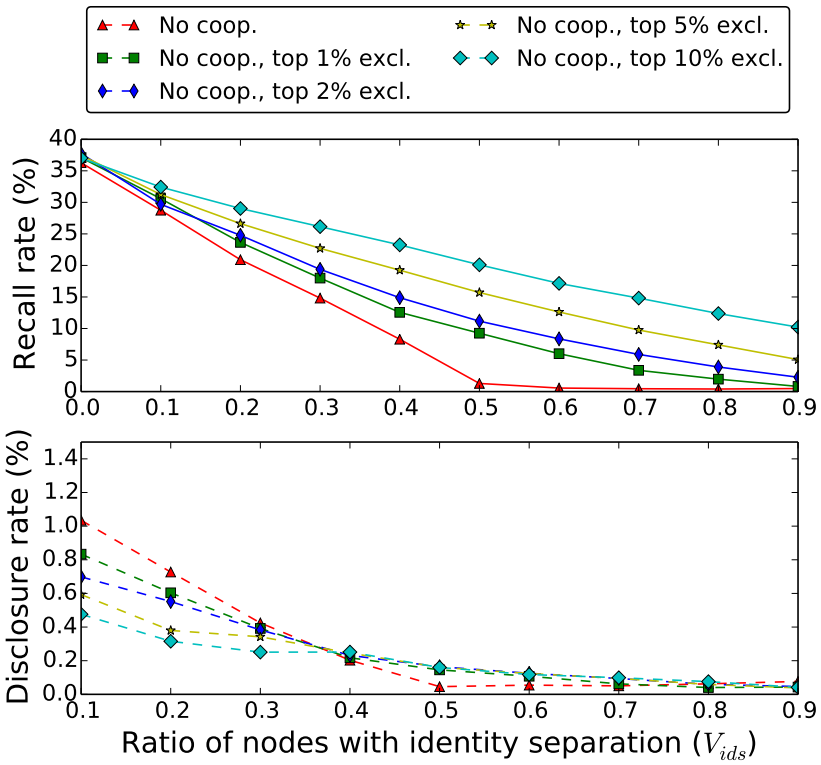


Figure 10: Recall and disclosure rates in the Slashdot network with the non-cooperative setting, (best model, $Y = 5$, random deletion). When top degree nodes do not participate, results significantly decline; however, using $Y = 5$ pays off even in those cases, as the disclosure rates are very low, around $0.4 - 1.0\%$.

Thesis Group 3. *I showed that it is worth adopting identity separation even if only a handful of users participates, and I provided a method for calculating the lower bound of the probability of the discovery of partial identities. I proposed a variant of the k-anonymity model for information hiding with identity separation, and showed its inapplicability. I proposed another model for information hiding, called the y-identity model. I devised and showed suitable strategies for different types of attackers under this model.*

Thesis 3.1. *I showed that even if a handful of users adopt identity separation, their re-identification results stay proportional to measurements observed in networks where strategies are adopted homogeneously. I proposed and successfully evaluated a method of targeted information hiding, that uses decoy identities to compel the state-of-the-art attack algorithm finding non-relevant information.*
Related publications: [C2, J3]

When looking for individual privacy-enhancing strategies for identity management, I needed to know if a small set of non-cooperating users (even well below $V_{ids} = 0.1$ which was the typical smallest adoption rate in previous measurements) or a single user can use identity separation to preserve privacy: it should be tested that if a node applies identity separation then disclosure rates should stay low. I also examined disclosure rates for cases when participation rates were low such as 1‰, meaning only a few tens or around a hundred of users using identity separation. Experiments resulted in approximately constant disclosure rates for all models with proportional values observed in previous experiments. Further details and results can be found in my dissertation.

Strategies discussed previously worked on statistical basis, and lacked user control: the user could not decide what he wished to hide from the attacker. Thus, I proposed a simple model by utilizing decoy identities. In order to apply the decoy strategy, first we need to create a decoy node v_i^P (public profile) representing non-sensitive connections with the goal of capturing the attention of attacker algorithm, assigned 90% of the acquaintances v_i has. Next, a hidden node v_i^H is created having the rest 10% of neighbors for modeling sensitive relationships, and an additional 10% that overlaps with the neighbors of v_i^P.

From the user perspective, privacy-protecting nodes achieved of revealing little sensitive information as shown in Fig. 11, which is even lower than using the best model with $Y = 5$ (e.g., compared to results in Fig. 7). Recall rates were typically small for hidden nodes, less than 0.25% within all test networks. However, this simple model can be defeated when the attacker optimizes for this specific user strategy. This fact motivated the research of

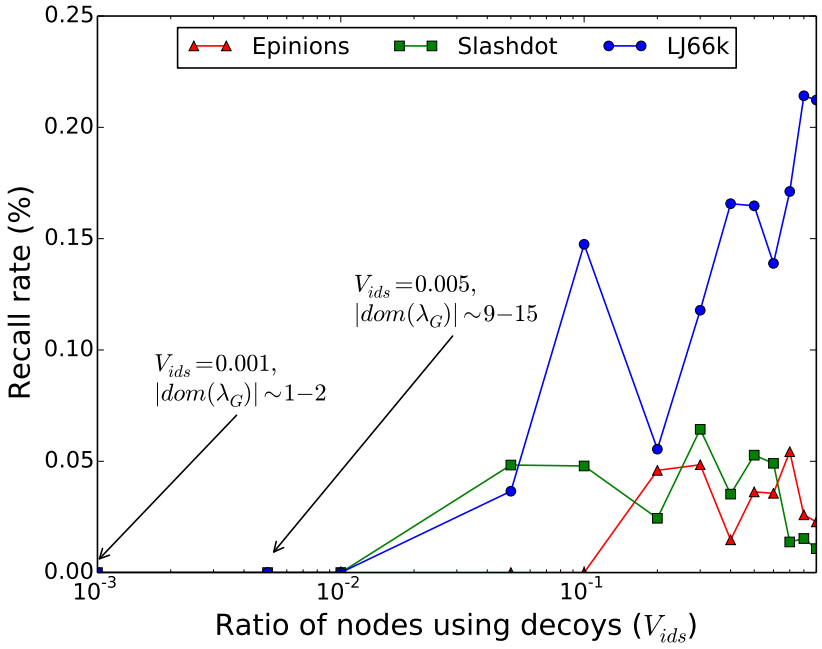


Figure 11: Searching for the most effective privacy-enhancing strategies when applied by a few: results of the decoy model.

new strategies that could be capable of achieving greater levels of uncertainty, such as k-anonymity could do that.

Thesis 3.2. *I designed a method for calculating the lower bound for the probability of the discovery of partial identities with a simple modification of the state-of-the-art attack. I showed that even with this modification only a fragment of partial identities can be found and merged.*
Related publications: [J1]

Two properties of the Nar09 algorithm prevented using the Nar09 algorithm to measure the lower estimates of the probabilities of finding an identity. First, the this de-anonymization attack could only produce one-to-one mappings, and according to my measurements, the algorithm is quite deterministic in this. Which results in having information on only the finding probability of one of the partial identities. In order to circumvent this problem, in the measurements of a particular user, I removed all partial identities but one. This resulted in an accurate lower estimation how each identity can be found; obviously, this can be topped by future algorithms or attackers using a wider range of auxiliary information than topology. This modification could also be applied in a real attack: the attacker first re-identifies a node, then removes the mapping and runs the attack again.

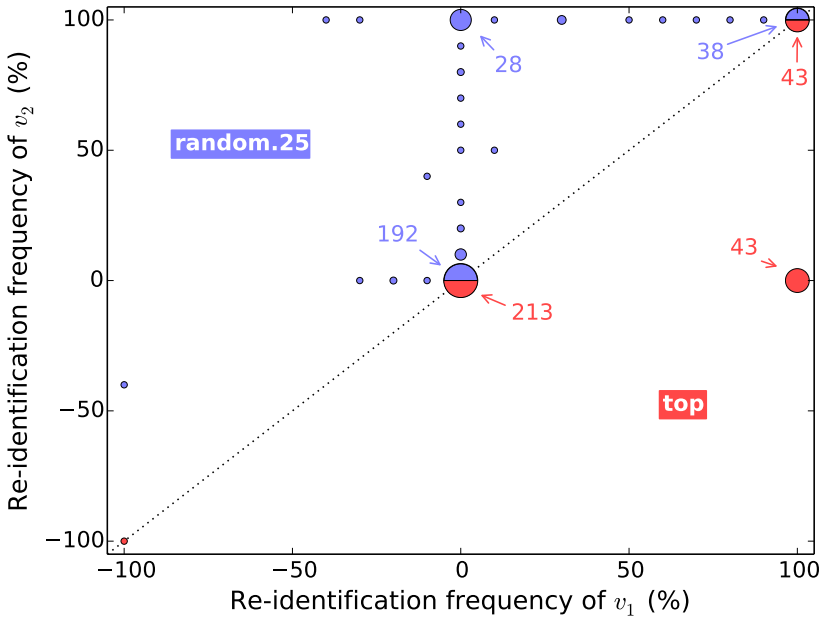


Figure 12: For the case of using two identities ($Y = 2$), re-identification frequency was measured by initializing with the `random.25` and the `top` methods. The figure shows that results depend on the seed method used by the attacker, as in the case of the `top` method re-identification rates were higher and results were more consistent. As it is shown, identity separation could be reversed certainly only in less than 15% of all cases.

In the experiments, for the basic model with $Y = 2$ identity separation could be reversed approx. 15% of all cases which is high enough to worth considering. Results were more promising for the best model setting, where the probability that a partial identity was found at least once was 2.83%, and only 1.72% of identities was always found. I provided some results in Fig. 12. Further details are in the dissertation.

Thesis 3.3. *I proposed $(k, 2)$-anonymity, a variant of k-anonymity to be adopted individually for tackling re-identification attacks. By evaluating `K-AnonymizeNode`, an algorithm that sets a $(k, 2)$-anonymous setting for a given node, I showed that the concept of k-anonymity cannot be applied efficiently within the current context.*
Related publications: [J1]

The definition of k-anonymity is based on the concept of quasi-identifiers, which are constructed from attributes of a data entity (e.g., user as a database row or a web browsing agent). Attributes of a quasi-identifier are not reckoned as explicit identifiers, but being used together can enable identification.

Definition 3. *k-anonymity. A dataset is k-anonymous if for all entries there are at least*

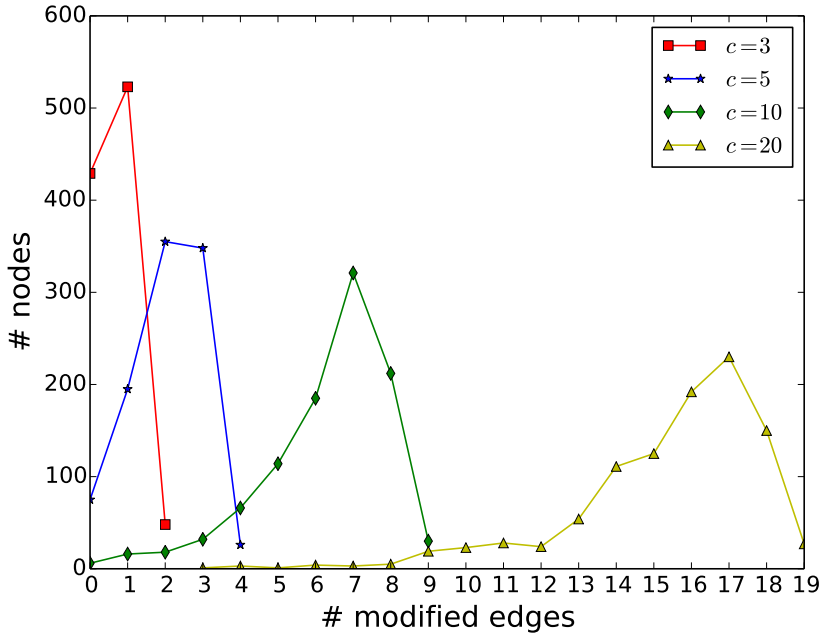


Figure 13: Results from Epinions dataset with $k = 2$. While in almost half of the cases it was possible to achieve anonymity for new identities with a very small neighborhood ($c = 3$) without modification, this was rather not possible for larger values of c. As the desired size of the neighborhood grew, the number of edges to add also increased.

k-1 *other entries with the same quasi-identifiers [22].*

As I found using overall network anonymization methods based on k-anonymity to be unrealistic (e.g., these require consent of service provider), I analyzed a method for applying k-anonymity on an individual basis regarding structural re-identification attacks.

Definition 4. $(k, 2)$*-anonymity. A user* $v_n \in G$ *is* $(k, 2)$*-anonymous if there are at least* *k*-1 *other (non-adjacent) users having exactly the same neighborhood, i.e.,*

$$\exists A_k = \{v_i : \forall v_i \in V_n^2, V_i = V_n\} \rightarrow |A| = k,$$

where V_i *denotes the neighbor set of* v_i*, and* V_i^2 *denotes the neighbors-of-neighbors of* v_i*.*

I have constructed an algorithm called `K-AnonymizeNode`, for finding $(k, 2)$-anonymous settings for users planning to apply identity separation. Beside parameter k the algorithm also takes an input of c that gives the desired neighborhood size of the new k-anonymous identity. If there are no users to propose, the algorithm tries to create new edges to meet the criteria.

With `K-AnonymizeNode`, I measured the possibility of $(k, 2)$-anonymity on $1,000$ nodes randomly sampled in multiple networks. Some of my results are shown in Fig. 13, justify that k-anonymity in this form cannot be applied to social networks. While in almost half of the cases with $c = 2$ it was possible to achieve anonymity without adding edges, this was rather not possible for larger and realistic values of c. Similar results can be observed in other networks, and also when analyzing whether this property differ as the network size change or if greater values of k is applied.

Thesis 3.4. *I designed the y-identity model as an alternative solution to k-anonymity. I proved that differing strategies are the best against weak and strong attackers. I also proved that the game theoretic equilibrium strategy proposed for strong attackers should be used if the attacker is unknown (i.e., can be either weak or strong), as it has a feasible higher bound on the expected privacy loss.*
Related publications: [J1]

In the y-identity model the user creates y new identities and randomly assigns the privacy sensitive information to one of the identities. Parameter y bounds the privacy the user can have. It is assumed the user is rational and optimizes for the best applying privacy-preserving settings. An important constraint for the attribute to be hidden is that alternatives need to be credible to maintain plausibility, otherwise the attacker can easily rule out false data and learn the sensitive one.

Definition 5. *y-identity. A users is considered to be acting according to the y-identity model if he creates y separated identities (either in one or in multiple datasets), and assigns randomly a privacy-sensitive attribute to only one of the identities, determined by a given distribution.*

We can model the attack process as follows. The attacker is rational, and aims for revealing quality private information at large in two sequential steps. First, the attacker uses a structural re-identification algorithm for discovering the mappings between the public identities of users and their separated identities in sanitized datasets. Then, after finding these mappings for a given user, the attacker makes a decision and either selects none, or picks one of the partial identities to be valid (i.e., learn the sensitive information).

Focusing on a given user and the attacker, we can formally describe this process similarly as a game. The player set $\mathcal{P}$ contains the user and the attacker. Initially, the user creates a total of y new identities denoted as $v_{n\setminus i}$, and the one having the sensitive attribute denoted $v^{\star}_{n\setminus i}$. The whole strategy set $\mathcal{S}$ can be defined as selecting one of the identities the user has, either for storing the sensitive attribute (user) or for selecting it

to be valid (attacker). In some cases the attacker only has access to $\mathcal{S}' \subset \mathcal{S}$. The user decisions are modeled with $P(R = i) = r_i$ ($\sum_{\forall i} r_i = 1$), attacker decisions are modeled with $P(Q = i) = q_i$ ($\sum_{\forall i} q_i \leq 1$). Finally, utility values (or payoffs) are denoted as $\mathcal{U}$.

We can define two types of attackers:

1. *Strong attackers*, who are able to discover all y identities of a given user v_n. The attacker knows he has access to all identities of v_n. As both the attacker and the user knows all possible choices each other could make (both players know $\mathcal{S}$), this problem can be conveniently tackled with a game-theoretic approach to find the best strategies.

2. *Weak attackers*, who are able to reveal some of the identities (even all of them), but are uncertain if there are any additional identities. More formally, while the user knows $\mathcal{S}$, the attacker only has access to $\mathcal{S}' \subseteq \mathcal{S}$, and does not know if $\mathcal{S}' = \mathcal{S}$. While this case could also be analyzed as a game (with significantly higher complexity), here we can also model the attacker as making decisions according to a given distribution on the discovered identities. Best user strategy can be analyzed with an optimization approach for minimizing the expected privacy loss.

For the analysis of *strong attackers*, I modeled the problem as the *identity partitioning game*, that consists of a single-round between the attacker and the user, where none of the players know the steps the other might have taken before. The Nash equilibrium [25] of this game is a pair of strategies when none of the players can increase their payoff by modifying only their strategies alone. It can be easily concluded that no pure strategy equilibrium exists here. Fortunately, John Nash have proven that in finite games a mixed strategy should always exist [26], and with the following theorem I proved the exact probabilities of the mixed equilibrium strategy.

Theorem 1. *A mixed strategy Nash equilibrium exists in the identity partitioning game (with a user having y separated identities), where the equilibrium strategy probabilities are* $q_i = \frac{1}{y}, r_i = \frac{1}{y}$ *(*$\forall i$*).*

The detailed proof is provided in the dissertation.

For the analysis of *weak attackers*, I assumed that the user can assess P_i, the discovery probabilities respectively of $v_{n\setminus i}$, e.g., similarly to the method I proposed earlier related to Thesis 3.2. However, calculating P_i values precisely can be a hard task in some cases; in such a case, I proposed to stick to the solution proposed for unknown attackers.

Let the fact of the discovery be stored in the discovery vector $\mathbf{m}$, where $m_i \in \mathbf{m}$ represents whether the i^{th} identity was discovered or not ($m_i \in [0, 1]$, $m_i = 1$ indicating

the identity was found, and vice versa). Let refine the attacker decision distribution, and introduce distribution vector denoted $\mathbf{q_m}$, where $q_i^{\mathbf{m}} \in \mathbf{q_m}$ denotes the probability that the attacker accepts the sensitive information stored in $v_{n\setminus i}$ (n.b. $m_i = 0$ implies $q_i^{\mathbf{m}} = 0$). Using these notations, the expected privacy loss can be described as follows:

$$E_w[u_n] = \sum_{\forall \mathbf{m}} \left(\left(\prod_{\forall j} ((1 - m_j) + (-1)^{(1-m_j)} \cdot P_j) \right) \cdot \left(\sum_{\forall i} r_i \cdot q_i^{\mathbf{m}} \right) \right) \cdot u_n^- \tag{4}$$

where $i, j \in [1, y]$. Details on deriving the formula are provided in the dissertation. However, this formula leads to an interesting advise regarding the best user strategy.

Theorem 2. *Given a weak attacker with known $\boldsymbol{q_m}$ vectors (for all $\boldsymbol{m}$), a set of pure strategies $\mathcal{S}' \subseteq \mathcal{S}$ exists which should be used in order to minimize the expected privacy loss $E_w[u_n]$. Strategies in $\mathcal{S}'$ can be used either as pure strategies or as mixed strategies.*

The detailed proof is provided in the dissertation. The conclusion of Theorem 2 is that in the case of weak attackers (w.r.t. the attacker model), in general it is advised to use pure strategies instead of mixed ones. In some specific cases, when there are multiple, equally good choices, mixed strategies can be based based on those strategies.

Now, let us seek an appropriate user strategy for the y-identity model against *unknown attackers*. From this strategy, we can reasonably expect at least a similar level of expected privacy loss compared to k-anonymity. In order to have that, I propose to use the equilibrium strategy $r_i = \frac{1}{y}$; the following theorem proves that this choice leads to an estimated privacy loss bounded by the expected privacy loss in case of k-anonymity.

Theorem 3. *Given the attacker model but with no restrictions to the attacker type, using $r_i = \frac{1}{y}$ $(\forall i)$ as a mixed strategy has a threshold for the expected privacy loss as*

$$E[u_n] \leq \frac{u_n^-}{y}.$$

The detailed proof of Theorem 3 is provided in the dissertation. This theorem shows that despite generally pure strategies are proposed in case of weak attackers, it is yet worth following the equilibrium strategy proposed against strong attackers, as the expected privacy loss would still have a feasible higher bound.

6 Application of results

The results provided in Thesis Group 1 can be used in case of designing novel attacks and protection schemes. The rest of the results (Thesis Group 2 and 3) provide the analysis

of identity separation. These findings can serve as a useful guide for designing a client-side application that supports identity separation in social networks. The resume of the findings show how different strategies could be used to achieve different privacy goals. I showed strategies which can effectively help achieving network privacy, despite the fact that it is quite difficult to achieve in some cases. However, I have also provided feasible strategies that could be used for protecting information against the state-of-the-art attack, while other strategies could help in case of even stronger attackers.

Acknowledgements

I would like to thank Sándor Imre for his supervision of my research, and his support and encouragement in all times. I would like to also thank Levente Buttyán, head of the CrySyS Lab, for providing an inspiring work environment and pushing me forward in the last two years of thesis work. Partial support of my research are also gratefully acknowledged for the High-Speed Networks Laboratory, the Mobile Innovation Centre, the BME-Infokom Innovátor Nonprofit Kft.

References

[1] "What nsa's prism means for social media users." `http://www.techrepublic.com/blog/tech-decision-maker/what-nsas-prism-means-for-social-media-users/`. Accessed: 2014-05-26.

[2] I. Szekely, "Building our future glass homes–an essay about influencing the future through regulation," *Computer Law & Security Review*, vol. 29, no. 5, pp. 540–553, 2013.

[3] A. Acquisti, B. V. Alsenoy, E. Balsa, B. Berendt, D. Clarke, C. Diaz, B. Gao, S. Gürses, A. Kuczerawy, J. Pierson, F. Piessens, R. Sayaf, T. Schellens, F. Stutzman, E. Vanderhoven, and R. D. Wolf, "D2.1 state of the art," tech. rep., SPION Project.

[4] S. Gurses and C. Diaz, "Two tales of privacy in online social networks," *Security & Privacy, IEEE*, vol. 11, no. 3, pp. 29–37, 2013.

[5] "diaspora*." `https://diasporafoundation.org`. Accessed: 2014-10-31.

[6] A. Sala, X. Zhao, C. Wilson, H. Zheng, and B. Y. Zhao, "Sharing graphs using differentially private graph models," in *Proceedings of the 2011 ACM SIGCOMM Conference*

on Internet Measurement Conference, IMC '11, (New York, NY, USA), pp. 81–98, ACM, 2011.

[7] C. Y. Ma, D. K. Yau, N. K. Yip, and N. S. Rao, "Privacy vulnerability of published anonymous mobility traces," in *Proceedings of the Sixteenth Annual International Conference on Mobile Computing and Networking*, MobiCom '10, (New York, NY, USA), pp. 185–196, ACM, 2010.

[8] M. Srivatsa and M. Hicks, "Deanonymizing mobility traces: using social network as a side-channel," in *Proceedings of the 2012 ACM conference on Computer and communications security*, CCS '12, (New York, NY, USA), pp. 628–637, ACM, 2012.

[9] G. Danezis and C. Troncoso, "You cannot hide for long: De-anonymization of real-world dynamic behaviour," in *Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society*, WPES '13, (New York, NY, USA), pp. 49–60, ACM, 2013.

[10] S. Ji, W. Li, J. He, M. Srivatsa, and R. Beyah, "Poster: Optimization based data de-anonymization," 2014. Poster presented at the 35th IEEE Symposium on Security and Privacy, May 18–21, San Jose, USA.

[11] L. Backstrom, C. Dwork, and J. Kleinberg, "Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography," in *Proceedings of the 16th international conference on World Wide Web*, WWW '07, (New York, NY, USA), pp. 181–190, ACM, 2007.

[12] A. Narayanan and V. Shmatikov, "De-anonymizing social networks," in *Security and Privacy, 2009 30th IEEE Symposium on*, pp. 173–187, 2009.

[13] A. Narayanan, E. Shi, and B. I. P. Rubinstein, "Link prediction by de-anonymization: How we won the kaggle social network challenge," in *The 2011 International Joint Conference on Neural Networks*, pp. 1825–1834, 2011.

[14] W. Peng, F. Li, X. Zou, and J. Wu, "Seed and grow: An attack against anonymized social networks," in *Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2012 9th Annual IEEE Communications Society Conference on*, pp. 587–595, 2012.

[15] P. Pedarsani, D. R. Figueiredo, and M. Grossglauser, "A bayesian method for matching two similar graphs without seeds," in *Communication, Control, and Computing (Allerton), 2013 51st Annual Allerton Conference on*, pp. 1598–1607, Oct 2013.

[16] S. Bartunov, A. Korshunov, S.-T. Park, W. Ryu, and H. Lee, "Joint link-attribute user identity resolution in online social networks," in *Proceedings of the sixth Workshop on Social Network Mining and Analysis*, 2012.

[17] D. Chen, B. Hu, and S. Xie, "De-anonymizing social networks," 2012.

[18] P. Jain, P. Kumaraguru, and A. Joshi, "@i seek 'fb.me': identifying users across multiple online social networks," in *Proceedings of the 22nd international conference on World Wide Web companion*, WWW '13 Companion, (Republic and Canton of Geneva, Switzerland), pp. 1259–1268, International World Wide Web Conferences Steering Committee, 2013.

[19] O. Goga, H. Lei, S. H. K. Parthasarathi, G. Friedland, R. Sommer, and R. Teixeira, "Exploiting innocuous activity for correlating users across sites," in *Proceedings of the 22Nd International Conference on World Wide Web*, WWW '13, (Republic and Canton of Geneva, Switzerland), pp. 447–458, International World Wide Web Conferences Steering Committee, 2013.

[20] H. Pham, C. Shahabi, and Y. Liu, "Ebm: an entropy-based model to infer social strength from spatiotemporal data," in *Proceedings of the 2013 international conference on Management of data*, pp. 265–276, ACM, 2013.

[21] S. Clauß, D. Kesdogan, and T. Kölsch, "Privacy enhancing identity management: protection against re-identification and profiling," in *Proceedings of the 2005 workshop on Digital identity management*, DIM '05, (New York, NY, USA), pp. 84–93, ACM, 2005.

[22] L. Sweeney, "K-anonymity: A model for protecting privacy," *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, vol. 10, pp. 557–570, Oct. 2002.

[23] "Spearman's rank correlation." `http://en.wikipedia.org/wiki/Spearman's_rank_correlation_coefficient`. Accessed: 2014-04-22.

[24] E. W. Weisstein, "Phase transition." `http://mathworld.wolfram.com/PhaseTransition.html`. Accessed: 2014-11-03.

[25] M. J. Osborne and A. Rubinstein, *A course in game theory*. MIT press, 1994.

[26] J. Nash, "Non-cooperative games," *Annals of mathematics*, pp. 286–295, 1951.

7 List of Publications

Highlighted publications are strongly related to my dissertation.

7.1 Bookchapter

[B1] K. Boda, A. M. Földes, G. G. Gulyás, and S. Imre, *Research and Development in E-Business through Service-Oriented Solutions*, ch. Tracking and Fingerprinting in E-Business: New Storageless Technologies and Countermeasures, pp. 134–166. IGI Global, 2013.

[B2] G. G. Gulyás, R. Schulcz, and S. Imre, *Digital Identity and Access Management: Technologies and Frameworks*, ch. Separating Private and Business Identities, pp. 114–132. IGI Global, 2012.

[B3] A. Kóbor, R. Schulcz, and G. G. Gulyás, *Szabad adatok, védett adatok 2.*, ch. Current threats of email - and what we can do against it (in Hungarian), pp. 315–340. INFOTA, 2008.

[B4] G. G. Gulyás, *Szabad adatok, védett adatok 2.*, ch. Using privacy-enhancing identity management in instant messaging services. (in Hungarian), pp. 285–314. INFOTA, 2008.

[B5] G. G. Gulyás, *Studies on information and knowledge processes 13., Alma Mater Series*, ch. Next generation of anonymous web browsers: a bit closer to democracy?, pp. 91–102. INFOTA, 2008.

[B6] G. G. Gulyás, *Tanulmányok az információ- ĂŠs tudásfolyamatokról 11., Alma Mater Series*, ch. Analaysis of anonymity and privacy in instant messaging services (in Hungarian), pp. 137–158. BME GTK ITM, 2006.

[B7] G. G. Gulyás, *Alma Mater sorozat az információ- ĂŠs tudásfolyamatokról 10.*, ch. Are anonymous web browsers anonymous? Analysis of solutions and services. (in Hungarian), pp. 9–30. BME GTK ITM, 2006.

7.2 Journal Papers

[J1] G. G. Gulyás and S. Imre, "Hiding information against structural re-identification," *Telecommunication Systems*, September 2014. (under review).

[J2] B. Simon, G. G. Gulyás, and S. Imre, "Analysis of grasshopper, a novel social network de-anonymization algorithm," *Periodica Polytechnica Electrical Engineering and Computer Science*, January 2015. (accepted for publication).

[J3] G. G. Gulyás and S. Imre, "Using identity separation against de-anonymization of social networks," *Transactions on Data Privacy*, January 2015. (accepted for publication).

[J4] G. G. Gulyás and S. Imre, "Analysis of identity separation against a passive clique-based de-anonymization attack," *Infocommunications Journal*, vol. 4, pp. 11–20, December 2011.

[J5] G. G. Gulyás, R. Schulcz, and S. Imre, "New generation anonymous web browsers (in hungarian)," *Híradástechnika (National Journal)*, vol. 62, no. 8, pp. 24–27, 2007.

7.3 Conference Papers

[C1] G. G. Gulyás and S. Imre, "Measuring importance of seeding for structural de-anonymization attacks in social networks," in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2014 IEEE International Conference on*, 2014.

[C2] G. G. Gulyás and S. Imre, "Hiding information in social networks from de-anonymization attacks by using identity separation," in *Communications and Multimedia Security* (B. Decker, J. Dittmann, C. Kraetzer, and C. Vielhauer, eds.), vol. 8099 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 2013.

[C3] G. G. Gulyás and S. Imre, "Measuring local topological anonymity in social networks," in *Data Mining Workshops (ICDMW), 2012 IEEE 12th International Conference on*, pp. 563–570, 2012.

[C4] K. Boda, A. M. Földes, G. G. Gulyás, and S. Imre, "User tracking on the web via cross-browser fingerprinting," in *Information Security Technology for Applications* (P. Laud, ed.), vol. 7161 of *Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 2012.

[C5] T. Besenyei, A. M. Földes, G. G. Gulyás, and S. Imre, "Stegoweb: Towards the ideal private web content publishing tool," in *Fifth International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2011)* (M. Takesue and R. Falk, eds.), pp. 109–114, August 2011.

[C6] T. Paulik, A. M. Földes, and G. G. Gulyás, "Blogcrypt: Private content publishing on the web," in *Fourth International Conference on Emerging Security Information Systems and Technologies (SECURWARE 2010)*, pp. 123–128, July 2010.

[C7] G. G. Gulyás, R. Schulcz, and S. Imre, "Modeling role-based privacy in social networking services," in *Third International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2009*, pp. 173–178, June 2009.

[C8] G. G. Gulyás, "Design of an anonymous instant messaging service," in *Proceedings of PET Convention 2009.1* (S. Köpsell and K. Loesing, eds.), pp. 34–40, Fakultät Informatik, TU Dresden, March 2009.

[C9] G. G. Gulyás, R. Schulcz, and S. Imre, "Comprehensive analysis of web privacy and anonymous web browsers: are next generation services based on collaborative filtering?," in *Proceedings of the Joint SPACE and TIME Workshops 2008* (L. Capra, I. Wakeman, and M. S. Foukia, Noria, eds.), CEUR Workshop Proceedings, June 2008.

7.4 Technical Reports

[T1] T. Paulik, A. M. Földes, and G. G. Gulyás, "Publishing private data to the web (in hungarian)," tech. rep., Budapest University of Technology and Economics, 2010.

[T2] S. Dargó and G. G. Gulyás, "Using privacy-enhancing identity management in anonymous web browsers (in hungarian)," tech. rep., Budapest University of Technology and Economics, 2010.