Investigating Anonymity in Group Based Anonymous Authentication

Daniel Slamanig[1,2] and Christian Stingl[1]

[1] Carinthia University of Applied Sciences, Medical Information Technology ·
Healthcare IT & Information Security Group, 9020 Klagenfurt, AUSTRIA
[2] University of Klagenfurt, Computer Science · System Security Group,
9020 Klagenfurt, AUSTRIA
{d.slamanig,c.stingl}@cuas.at

Abstract. In this paper we discuss anonymity in context of group based anonymous authentication ($\mathcal{GBAA}$). Methods for $\mathcal{GBAA}$ provide mechanisms such that a user is able to prove membership in a group $\mathcal{U}' \subseteq \mathcal{U}$ of authorized users $\mathcal{U}$ to a verifier, whereas the verifier does not obtain any information on the actual identity of the authenticating user. They can be used in addition to anonymous communication channels in order to enhance user's privacy if access to services is limited to authorized users, e.g. subscription-based services. We especially focus on attacks against the anonymity of authenticating users which can be mounted by an external adversary or a passive verifier when $\mathcal{GBAA}$ is treated as a black box. In particular, we investigate what an adversary can learn by solely observing anonymity sets $\mathcal{U}'$ used for $\mathcal{GBAA}$ and how users can choose their anonymity sets in case of $\mathcal{U}' \subset \mathcal{U}$. Based on the information which can be obtained by adversaries we show that the probability of user identification can be improved.

1 Introduction

The Internet is nowadays used by a permanently increasing number of people. Their actions comprise on the one hand private activities, e.g. using it as a source of information, doing online banking, communicating with other persons, reading their newspapers, participating in electronic auctions. On the other hand people use it for business related activities. Obviously, the collection of information divulged and exchanged during these activities may represent an extensive picture of a person and covers many topics related to ones privacy. For example, these information may be highly valuable for providers hosting online services when analyzing user's behavior [20,35]. In this context there are tools available for free, e.g. Google Analytics, which provide a huge set of functionalities for aforementioned purposes, even for unaware and casual users. Nevertheless, users may also benefit from these methods by means of Web personalization, i.e. the customization of delivered Web content with respect to the user's preferences. However, privacy issues are very often neglected, which questions the before discussed advantages. This can be illustrated by a user who queries a health information service to obtain information on a serious disease. Recent studies show that 80 percent of health searchers seek the information for themselves and 60 to 80 percent of Americans have already used the Internet to find health information [32]. Hence, if any other party is able to link these information to the user, then it may be possible to draw compromising conclusions.

The aforementioned threats are in our opinion highly realistic, since protocols used in Internet communication do not explicitly provide mechanisms to preserve the anonymity of users. Additionally, we are confronted with a phenomenon denoted as privacy myopia [19]. This means, that people often are not aware of dangers related to privacy and sell or give away their data without reflecting on potential negative consequences. For instance, in context of the Internet this means that users reveal IP-addresses which enable third parties to link several actions and may enable third parties to identify the physical users behind their computers. Furthermore, users often easily give away person related information to third parties which exceeds the amount of information necessary. The latter aspect is the subject of privacy enhanced identity management and has experience major research interest in recent years (cf. [5]).

In this paper we will discuss anonymity aspects related to group based anonymous authentication ($\mathcal{GBAA}$), which provides anonymity for users if access to services is limited to an authorized set of users. If a user needs to authenticate to a service provider by means of traditional authentication mechanisms, in general the identity of the user is known by the service provider. By means of $\mathcal{GBAA}$, the server solely learns the membership of the authenticating user in the set of authorized users, but does not learn the exact identity. This can be valuable for users, if the sole knowledge of service accesses, i.e. the frequency of access, may lead to compromising conclusions. The applications we have in mind for $\mathcal{GBAA}$ are any kind of Internet services that require user authentication, but users want to hide their behavior from the service provider. Thereby, the main advantage of $\mathcal{GBAA}$ schemes is that they can be build upon existing and widely deployed public key infrastructures based on X.509 certificates (PKIX) and user registration for services solely requires the user to provide a valid X.509 certificate to the service provider. This results on the one hand in higher security compared to widely used username/password authentication schemes and on the other hand in a privacy improvement for the user. For instance, consider a Internet service which provides access to an electronic health record (EHR) of a person, whereas the EHR represents a life-long documentation of the medical history of a person. In this context, even the knowledge of the frequency of access to the EHR may enable a third party to draw compromising conclusions about the state of health of the person. Additionally, the use of $\mathcal{GBAA}$ schemes, which are based on public key certificates, prevents users from identity theft by means of password guessing, dictionary attacks or other threats.

The remainder of this paper is organized as follows: In section 2 we discuss aspects of anonymity that are important for Internet based services. In the subsequent section 3 we will briefly introduce $\mathcal{GBAA}$, attack models and scenarios as well as some problems related to $\mathcal{GBAA}$. Section 4 discusses the choice of anonymity sets used for authentication and provides a detailed analysis. Finally, section 5 concludes the paper and discusses some future aspects.

2 Different Aspects of Anonymity

Anonymity aspects of users in the context of Internet services are twofold. Firstly, the anonymity of a user may be revealed by the communication channel itself. Consequently, users need to hide their identity when sending messages over the communication channel. This can be achieved by means of anonymous communication channels. Secondly, identities of users may be revealed at higher network layers, i.e. the application layer. This is especially of interest if services require user authentication at the application layer. Subsequently, we will briefly discuss the aforementioned aspects.

2.1 Communication Anonymity

Mechanisms that provide anonymity and unlinkability of messages sent over a communication channel are denoted as anonymous communication techniques and have been intensively studied in recent years, see [12] for a sound overview. There are several implementations available for low-latency services like Web browsing, e.g. Tor [15], JAP [18], as well as high-latency services like E-Mail, e.g. Mixminion [13].

These anonymous communication channels help to improve the privacy of users in context of eavesdroppers and curious communication partners. Especially, regarding the latter one anonymity can be preserved if electronic interaction does not rely on additional identifying information at higher network layers, i.e. the application layer. For example, a user who queries a public web page using an anonymous communication channel may remove all identifying information from higher network layers and thus will stay anonymous.

In our considerations we assume that we have a communication channel that guarantees perfect anonymity and unlinkability. Then a user is connected to a service provider (server) via a kind of *"magic channel"* that leaks no information on the identity of the user at the communication layer. Clearly, this is a somewhat idealized consideration, since real world anonymous communication channels do not realize perfect anonymity resp. unlinkability (cf. [30]) and there may exist additional side channels, e.g. online-behavior of users, which can be used to improve the probability of identification of communicating parties.

2.2 Anonymity at Higher Layers

However, if service providers offer their services only to authorized sets of users, e.g. subscription-based services, closed communities, they require identification of users which in general takes place at higher layers by means of entity authentication mechanisms. In entity authentication or identification protocols the holder of an identity usually claims a set of attributes including an identifier and interactively proves the possession of the claimed identity to a verifier. This identifier is usually unique within a specific context, e.g. application, but may be a pseudonym, which is not linkable to the physical identity of a person. But there usually exists a party which is aware of this link and additionally, actions conducted under the same pseudonym can be linked. Nevertheless, there exists anonymous credential systems which can be used to anonymously prove the possession of attributes of credentials while preserving unlinkability of different showings of a credential and anonymity of the holders (cf. [4,7,8,24]). These approaches are especially suitable in a multi-provider setting, where users obtain credentials for a pseudonym from one provider and are able to show these credentials under different pseudonyms to other providers. Nevertheless, there are also known attacks (cf. [21,27]) against unlinkability and anonymity of anonymous credential systems when using them in a real world context. We do not consider the aforementioned approaches, since we are interested in a single-provider and "ad hoc" setting. However, the aforementioned mechanisms can also be used to realize anonymous authentication (cf. [6]), but in general they do not provide "ad hoc" mechanisms as discussed below, i.e. they rely on a proprietary setup with every user. Therefore, we will subsequently discuss an alternative approach based on cryptographic primitives like ring signatures [31], which we call group based anonymous authentication ($\mathcal{GBAA}$), that provides mechanisms to perform anonymous authentications based on "ad hoc" groups, i.e. without relying on interaction with other group members and without any additional proprietary setup.

3 Group Based Anonymous Authentication

Group based anonymous authentication ($\mathcal{GBAA}$) aims to provide a somewhat paradoxical solution to enhance user's privacy in context of authentication. It provides mechanisms such that a user is able to prove membership in a group $\mathcal{U}' \subseteq \mathcal{U}$ of authorized users $\mathcal{U}$, whereas the verifier does not obtain information on the identity of the authenticating user. The set $\mathcal{U}'$ will also be denoted as the anonymity set [29]. Clearly, anonymous communication systems are a prerequisite for providing anonymity in the context of anonymous authentication.

A naive approach to realize $\mathcal{GBAA}$ would be to give a copy of a secret k to every user $u \in \mathcal{U}$, which could be used in conjunction with a traditional authentication scheme. Obviously, the revocation of a single user u_i would result in a reinitialization and thus in reissuing a fresh secret k' to every remaining user $u \in \mathcal{U} \setminus u_i$. Hence, this approach is far from being practical. Improved techniques for $\mathcal{GBAA}$ were explicitly treated in [3,23,28,33,37] and additionally with special properties like being anonymous as long as the number of authentication is beyond a threshold [36], the ability to detect fraudulent users [6,11] and with the ability to revoke the anonymity of users [3,22]. They can be be realized by means of group signatures [1,9, etc.], witness indistinguishable signatures [10], ring signatures [16,31, etc.] or similar concepts as (deniable) ring authentication [26].

The latter two classes of signature and authentication schemes are preferable to group signatures in the context of large and dynamic groups, as it is the case with Internet services, since they can be generated "ad hoc" without depending on an explicit setup phase or reinitialization in case of dynamic groups. Thereby "ad hoc" means that an authenticating user does not need the knowledge, consent or assistance of the remaining members of an ad hoc group to perform an authentication. Furthermore, in general they do not require a proprietary setup and do only rely on standard public key certificates, i.e. X.509 certificates, which are widely deployed and available. It must be mentioned that there are already attempts to integrate group, ring and traceable signatures, which can be used for $\mathcal{GBAA}$, into the PKIX framework [2].

There are three important properties that $\mathcal{GBAA}$ mechanisms need to provide (cf. [23,33]):

1. **Anonymity:** The verifier is not able to determine the identity of an authenticating user with probability higher than $1/|\mathcal{U}'|$.
2. **Unlinkability:** It is impossible to link k, $k > 1$, instances of the $\mathcal{GBAA}$ protocol of one (anonymous) user $u_i \in \mathcal{U}'$.
3. **Security:** Only authorized users $u \in \mathcal{U}$ should be able to pass the $\mathcal{GBAA}$.

The properties we are focusing on in this paper are anonymity and unlinkability, and in particular we investigate strategies to construct groups used for $\mathcal{GBAA}$. This is especially of interest in context of large groups, since the computational effort in $\mathcal{GBAA}$ protocols usually grows (linearly) with the size of the anonymity set, i.e. the cardinality of $\mathcal{U}'$. Thus, a large set of authorized users may force a user to prove his membership using a subset of all authorized users for efficiency purposes. It must be mentioned that we do not explicitly discuss technical details on the construction of methods for $\mathcal{GBAA}$ and will treat them as a black box in the remainder of this paper.

The question that comes up is, whether a verifier or even an observer is able to reduce the anonymity and consequently unlinkability by continuously observing anonymity sets, although the underlying $\mathcal{GBAA}$ method and communication channel provides perfect anonymity and unlinkability.

3.1 Attacker Model

As mentioned above, we are not considering anonymity provided by the $\mathcal{GBAA}$ itself and the communication channel. Consequently, we assume that the $\mathcal{GBAA}$ methods provide perfect anonymity, unlinkability and security and the communication channel provides perfect anonymity and unlinkability ("magic channel"). Clearly, these assumptions are very strong with respect to the real world and thus the results presented in this paper, i.e. the reduction of anonymity of users, may even be improved enormously by substituting the perfect $\mathcal{GBAA}$ and communication channel by actually deployed methods.

The attack model used in this paper considers the following adversaries.

- **Honest but curious (passive) verifier:** An insider who is able to monitor all actions inside the verifier's system, but does not actively manipulate messages which are exchanged during the $\mathcal{GBAA}$.
- **Eavesdropper:** Anyone who is able to monitor the inbound traffic of the verifier. As above, the eavesdropper solely behaves passive, i.e. does not manipulate exchanged messages.

Passive attacks conducted by an eavesdropper can easily be prevented by means of encrypted communication, i.e. a communication channel which provides confidentiality and integrity of transmitted messages. However, it must be mentioned that an external adversary may run a denial of service (DoS) attack against the verifier's system in order to deter authentications of users anyway. We do not consider active attackers, since there exist measures incorporated into $\mathcal{GBAA}$ protocols to detect a cheating verifier (cf. [23]), which are outside the scope of this paper. Furthermore, in practice an actively cheating verifier may leak out some day and will consequently not be trustworthy anymore.

An adversary may mount the subsequent attacks, whereas we focus on the first one in this paper and the latter one will only be stated for the sake of completeness.

- **Anonymity sets only:** An adversary is clearly able to record all information which are shown to him during any instance of a $\mathcal{GBAA}$. Thus he can count the occurrences of users in anonymity sets. The adversary will try to reduce the anonymity of single users solely by means of the aforementioned information.
- **Behavioral heuristic:** Since unlinkability is a required property, every action inside the system requires a single $\mathcal{GBAA}$ protocol. Thus, authentications of a single user are likely to occur cumulative since in general at least a few operations are conducted within the verifier's system.

3.2 Some Problems Related to $\mathcal{GBAA}$

One inherent problem in "ad hoc" $\mathcal{GBAA}$ is, that the physical person which holds a digital identity, irrespective of the representation, e.g. X.509 certificates, is not directly known to a user. Consequently, a user may not be able to distinguish "real" from "fake" identities. Especially in large groups, a verifier may be able to forge identities of "authorized users" which look valid to all other users. This is crucial, if verifiers set up their system (parameters) autonomous, i.e. issue credentials or certificates on their own, and do not involve a commonly trusted party, e.g. a trusted certification authority which issues public key certificates. It must be stressed, that this attack is an active one which can be conducted by malicious verifiers to reduce the anonymity of users. However, we assume that the verifier is honest but curious in our attack model. This fake-user insertion attack can be somewhat compared to the sybil attack [17], which has been investigated in a somewhat similar context [25]. But, in our case the verifier creates a set of forged identities on his own and integrates them into the system.

Consequently, the effective anonymity set for $\mathcal{GBAA}$ will be reduced by users unawarely including fake identities in their anonymity sets.

Another problem in this context is that the authenticating user needs to be sure, that all actually chosen users are indeed authorized users at the point of time of authentication. We want to emphasize, that the task of determining authorized users, i.e. to check if a user is authorized and the respective certificate is valid, is a time consuming and non-trivial task, but is inherent to all certificate based $\mathcal{GBAA}$ protocols. However, we will not consider this problem in detail in this paper since it does not affect our investigations.

4 Analysis

In this section we firstly analyze strategies to construct anonymity sets and secondly propose methods that can be used by an adversary to improve the probability of identification of users.

4.1 Group Construction Strategies

In the following we will discuss the strategies to construct anonymity sets for $\mathcal{GBAA}$. Thereby, we consider the two possible scenarios, i.e. on the one hand the entire group and on the other hand a subgroup of authorized users.

Entire Group: If a user chooses the entire group $\mathcal{U}$ for $\mathcal{GBAA}$, the probability of user u_i being the one who actually authenticates in any anonymity set is $p_{u_i} = 1/|\mathcal{U}|$. Hence, this approach guarantees perfect anonymity [14,34]. This strategy is immune against fake-user insertion attacks, since always all users are chosen. However, it must be emphasized that for actual available protocols for $\mathcal{GBAA}$ the computational effort grows at least linearly with the size of the anonymity set. Hence, in case of a large set of authorized users, this approach is impractical.

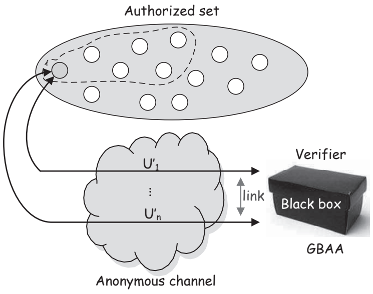


Fig. 1. Static subgroup approach from the point of view of the prover.

Subgroup: This alternative approach is characterized by choosing a subset $\mathcal{U}' \subset \mathcal{U}$ for $\mathcal{GBAA}$, whereas we assume that $|\mathcal{U}'| \ll |\mathcal{U}|$. Therefore, users need to construct subgroups following some specific strategy. The obvious method for a user u_i to construct an anonymity set of size k is, to independently choose $k-1$ users uniformly at random from $\mathcal{U}$ and to subsequently integrate himself into the anonymity set. This approach is prone to a fake-user insertion attack, since the verifier may include faked "authorized" users into the set of all authorized users. Consequently, the level of security depends on the fraction of "fake" users.

Considering the subgroup-approach we distinguish between static subgroups and dynamic subgroups.

Static Subgroup: In case of static subgroups, a user $u_i \in \mathcal{U}$ initially chooses $k-1$ users uniformly at random from $\mathcal{U}$ and forms his static anonymity set by adding himself to this set. Subsequently, he uses his initial chosen anonymity set for every $\mathcal{GBAA}$. If $\mathcal{U}$ is large, e.g. $|\mathcal{U}| = 200$, and the size of the anonymity set is smaller than the size of $\mathcal{U}$ ($\mathcal{U}' \approx 100$), it is very unlikely that two distinct users choose exactly the same anonymity set, i.e. $\approx 1/\binom{|\mathcal{U}|}{|\mathcal{U}'|}$. Hence, if a user applies this strategy all $\mathcal{GBAA}$s are in general linkable. Additional, with side channel information, e.g. user's behavior, it may be easier to identify a single user. As a consequence we want to point out that this approach is in our opinion not appropriate.

Dynamic Subgroup: In case of dynamic subgroups a user $u_i \in \mathcal{U}$ constructs his anonymity set $\mathcal{U}'$ independently for every single authentication. Thus unlinkability is guaranteed and with respect to the above strategies in our opinion it is the preferred strategy in context of large sets of authorized users. Nevertheless, we will subsequently examine potential weaknesses of this dynamic subgroup approach which can be used by an adversary to improve the probability of identifying authenticating users.

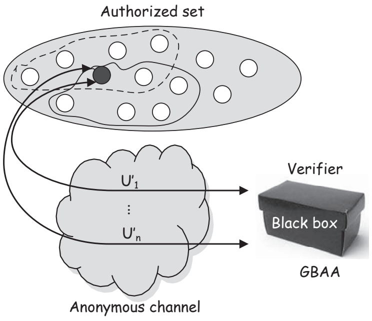


Fig. 2. Dynamic subgroup approach from the point of view of the prover.

4.2 Anonymity Sets Only Attack

As mentioned above, we are now focusing on anonymity sets independent of the protocol used for $\mathcal{GBAA}$. Furthermore, we assume that these information can be monitored by an adversary, e.g. the verifier or an eavesdropper. In particular, we introduce methods to analyze the anonymity sets and derive measures to improve attacks against anonymity. In order to compute these measures a $|\mathcal{U}| \times N$ history matrix $\mathcal{H}$ will be used, where $\mathcal{U}'_j$, $1 \leq j \leq N$, is the j-th anonymity set and N is the overall number of $\mathcal{GBAA}$ protocol runs.

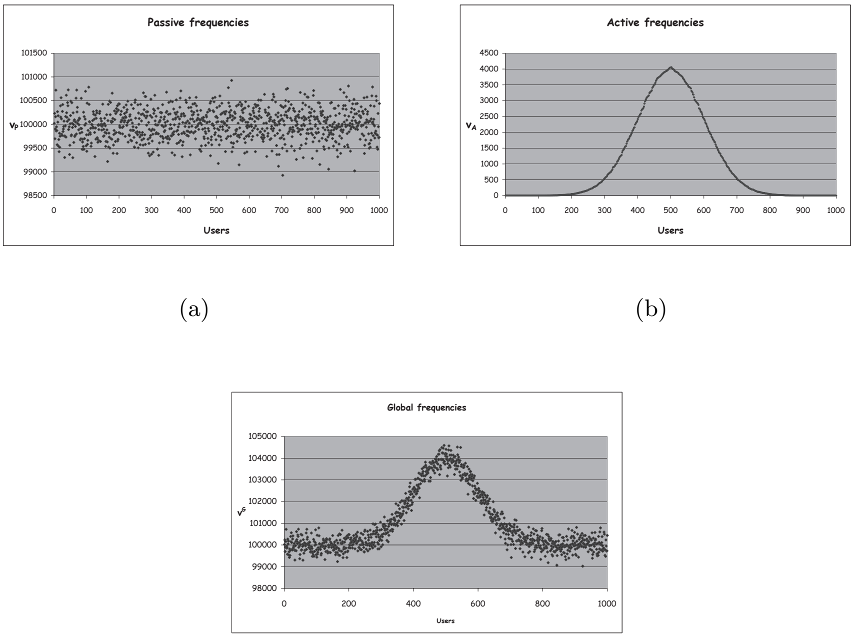
$$\mathcal{H}(i,j) = \begin{cases} 1, & \text{if } u_i \in \mathcal{U}'_j, \\ 0, & \text{else.} \end{cases}$$

Put differently, the matrix represents the collection of all anonymity sets which were used in $\mathcal{GBAA}$s and the element $\mathcal{H}(i,j)$ contains the value 1 if and only if user u_i occurred in the respective anonymity set $\mathcal{U}'_j$. Based on this matrix, we are defining the global frequency $\nu^G_{u_i}$ of user u_i which is the sum of the i-th row. The global frequency of a user u_i itself consists of an active part $\nu^G_{u_i,\mathcal{A}}$, i.e. the number of actual authentications of the user, and a passive part $\nu^G_{u_i,\mathcal{P}}$, i.e. other users choose u_i in their anonymity sets. Obviously, an adversary can solely determine the sum $\nu^G_{u_i} = \nu^G_{u_i,\mathcal{A}} + \nu^G_{u_i,\mathcal{P}}$ of the users frequency from the history matrix. The two subsequent facts can easily be obtained.

$$\sum_{i=1}^{|\mathcal{U}|} \nu^G_{u_i,\mathcal{A}} = N \tag{1}$$

$$\sum_{i=1}^{|\mathcal{U}|} \nu^G_{u_i,\mathcal{P}} = \sum_{i=1}^{N} (|\mathcal{U}'_i| - 1) \tag{2}$$

Considering the above mentioned method to create subgroups one can conclude that the passive frequencies are uniformly distributed and the average of all passive frequencies is $\bar{\nu}_{\mathcal{P}} = \sum_{i=1}^{N}(|\mathcal{U}'_i| - 1)/N$. In contrast, the distribution of the active frequencies is in general unknown, but it is very unlikely that the distribution is uniform in real world scenarios. At this point the following question arises: What kind of information can be obtained about the global frequency? A first observation is, that the sum of the passive frequencies is much greater then the sum of the active frequencies. For instance, if the size of the anonymity set is constant then $\sum \nu_{\cdot,\mathcal{P}} / \sum \nu_{\cdot,\mathcal{A}} = |\mathcal{U}'| - 1$. Secondly, we know that the passive frequencies are uniformly distributed and thus we are able to derive a confidence interval α for the expected value. Hence, all passive frequencies will lie in the confidence interval with probability p (see table 1). Based on the global frequency of a single user u_i it is possible to derive an interval for the active frequency of this user (see figure 4). The parameter (α) determines the lower and upper bound of the confidence interval. By subtracting these bounds from the global frequency one obtains an interval for the active frequency which holds



(a)

(b)

(c)

Fig. 3. The setting for this example is: $|\mathcal{U}| = 1000$, $N = 10^8$. Subfigure (a) illustrates the uniform distribution of the passive frequencies. In this example it was assumed that the active frequencies are Gaussian distributed (b). Subfigure (c) shows that the distribution of the active frequencies is still reflected in the global frequency. Furthermore, it can be conjectured that the value of the global frequency is directly “connected” to the value of the active frequency and vice versa.

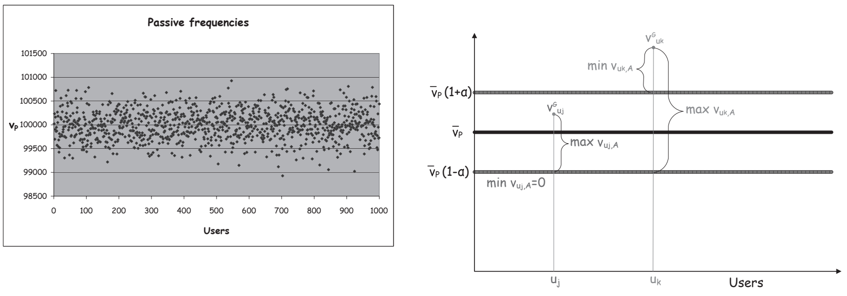
Authorized users $\lvert\mathcal{U}\rvert$	Anonymity set $\lvert\mathcal{U}'\rvert$	Number of auth. N	α	p	Outliers
1000	100	1000.000	0.005	≈ 0.8863	≈ 113
1000	100	1000.000	0.01	≈ 0.9984	≈ 2
1000	100	1000.000	0.02	≈ 1	≈ 0

Table 1. Confidence interval α, probability p and number of outliers.

with probability p.

$$max(\nu^G_{u_i} - \bar{\nu}_{\mathcal{P}}(1+\alpha), 0) \leq \nu^G_{u_i,\mathcal{A}} \leq max(\nu^G_{u_i} - \bar{\nu}_{\mathcal{P}}(1-\alpha), 0) \qquad (3)$$

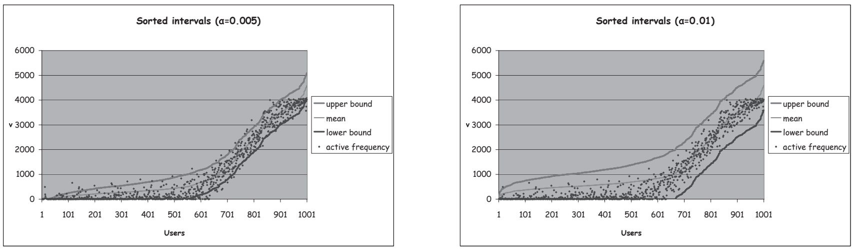
Note that the lower α the more precise are the lower and the upper bound for the active frequency. But, the number of passive frequencies which are not inside the confidence interval will grow and consequently the number of active frequencies which do not satisfy equation (3). From equation (3) it is possible to derive the



(a) (b)

Fig. 4. In subfigure (a) an exemple confidence interval is shown. Based on this confidence interval ranges for the active frequency of two users are derived (b).

maximum size of the interval $\delta_{\mathcal{A}}$, whereas $\delta_{\mathcal{A}} \leq 2\alpha\nu_{\mathcal{P}}$. This is also reflected in figure 5 where $\nu_{\mathcal{P}} = 100.000$ and $\alpha = 0.005$ ($\alpha = 0.01$). Consequently, $\delta_{\mathcal{A}} = 1000$ (2000) which can also be seen in figures 5. Considering two users u_i and u_j where



(a) (b)

Fig. 5. Upper and lower bounds for active frequencies for two choices of the parameter α; (a): $\alpha = 0.005$; (b): $\alpha = 0.01$.

the upper bound of user u_i is significantly smaller then the lower bound of the user u_j, then $\nu^G_{u_i,\mathcal{A}}$ is also significantly smaller than $\nu^G_{u_j,\mathcal{A}}$. These information can prospectively be used to improve the probability of identification of u_j in comparison to u_i.

It must be mentioned, that this estimation is independent of the distribution of the active frequencies. Furthermore, we have evaluated a number of random number generators (RNG) provided by standard libraries of different programming languages and most of them behave as the probability theory predicts and clearly was the basis for our investigations. However, we have also encountered a few RNGs that provide "better" results than expected and consequently more precise bounds could be obtained. Put differently, RNGs that behave "better" than the theory predicts, i.e. the passive frequency $\nu^G_{u_i,\mathcal{P}}$ of every user u_i will be very close to the mean passive frequency $\bar{\nu}_{\mathcal{P}}$, the active frequency of every user $\nu^G_{u_i,\mathcal{A}}$ can be determined precisely.

5 Conclusion

In this paper we have briefly discussed group based anonymous authentication ($\mathcal{GBAA}$) and strategies to construct anonymity sets. Furthermore, we have discussed attacks which can mainly be conducted by passive adversaries and finally we have pointed out how to estimate the number of authentications per user. This result can be used to reduce the anonymity of authenticating users. Additional side-channel information, e.g. user's behavior, can be used to further improve the efficiency of the proposed approach. We conclude, that $\mathcal{GBAA}$, even considered as a black box, leaks information on authenticating users over a period of time. One important fact is, that the approximated active frequencies of users are more precise the greater the number of protocol runs. In order to counter this kind of attack we recommend to significantly reduce the number of $\mathcal{GBAA}$s. This can be achieved by a combination of $\mathcal{GBAA}$ and token based anonymous transactions, which is topic to current and future research.

Acknowledgements

The authors would like to thank the anonymous referees for their valuable comments and Michael Reiner for providing the simulation results to us.

References

1. Giuseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik. A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. In *Advances in Cryptology – CRYPTO '00*, volume 1880 of *LNCS*, pages 255–270. Springer, 2000.
2. Vicente Benjumea, Seung Geol Choi, Javier Lopez, and Moti Yung. Anonymity 2.0 - X.509 Extensions Supporting Privacy-Friendly Authentication. In *Cryptology and Network Security*, volume 4856 of *LNCS*, pages 265–281. Springer, 2007.
3. Dan Boneh and Matt Franklin. Anonymous Authentication with Subset Queries. In *Proc. of the 6th ACM conference on Computer and communications security*, pages 113–119, 1999.
4. Stefan Brands. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy.* MIT Press, 2000.
5. J. Camenisch, A. Shelat, D. Sommer, S. Fischer-Hübner, M. Hansen, H. Krasemann, G. Lacoste, R. Leenes, and J. Tseng. Privacy and Identity Management for Everyone. In *DIM '05: Proceedings of the 2005 workshop on Digital identity management*, pages 20–27, New York, NY, USA, 2005. ACM.

6. Jan Camenisch, Susan Hohenberger, Markulf Kohlweiss, Anna Lysyanskaya, and Mira Meyerovich. How to Win the Clone Wars: Efficient Periodic n-Times Anonymous Authentication. In *Proceedings of the 13th ACM conference on Computer and communications security, CCS'06*, pages 201–210, New York, NY, USA, 2006. ACM.
7. Jan Camenisch and Anna Lysyanskaya. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In *Advances in Cryptology – EUROCRYPT '01*, volume 2045 of *LNCS*, pages 93–118, London, UK, 2001. Springer.
8. David Chaum. Security without identification: transaction systems to make big brother obsolete. *Commun. ACM*, 28(10):1030–1044, 1985.
9. David Chaum and Eugene van Heyst. Group Signatures. In *Advances in Cryptology – EUROCRYPT '91*, volume 547 of *LNCS*, pages 257–265. Springer, 1991.
10. Ronald Cramer, Ivan Damgård, and Berry Schoenmakers. Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. In *Advances in Cryptology - CRYPTO '94*, volume 839 of *LNCS*, pages 174–187, London, UK, 1994. Springer.
11. Ivan Damgård, Kasper Dupont, and Michael Østergaard Pedersen. Unclonable Group Identification. In *Advances in Cryptology - EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 555–572. Springer, 2006.
12. George Danezis and Claudia Diaz. A Survey of Anonymous Communication Channels. Technical Report MSR-TR-2008-35, Microsoft Research, January 2008.
13. George Danezis, Roger Dingledine, and Nick Mathewson. Mixminion: Design of a Type III Anonymous Remailer Protocol. In *SP '03: Proceedings of the 2003 IEEE Symposium on Security and Privacy*, pages 2–15, Washington, DC, USA, 2003. IEEE Computer Society.
14. Claudia Diaz, Stefaan Seys, Joris Claessens, and Bart Preneel. Towards Measuring Anonymity. In *Proceedings of Designing Privacy Enhancing Technologies,*, volume 2482 of *LNCS*, pages 184–188. Springer, 2002.
15. Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The Second-Generation Onion Router. In *Proceedings of the 13th USENIX Security Symposium*, pages 21–21, 2004.
16. Yevgeniy Dodis, Aggelos Kiayias, Antonio Nicolosi, and Victor Shoup. Anonymous Identification in Ad Hoc Groups. In *Advances in Cryptology - EUROCRYPT'04*, volume 3027 of *LNCS*, pages 609–626. Springer, 2004.
17. John R. Douceur. The Sybil Attack. In *Revised Papers from the First International Workshop on Peer-to-Peer Systems, IPTPS '01*, volume 2429 of *LNCS*, pages 251–260. Springer, 2002.
18. Hannes Federrath. Privacy Enhanced Technologies: Methods, Markets, Misuse. In *Proceedings of the 2nd International Conference on Trust, Privacy, and Security in Digital Business, TrustBus '05*, volume 3592 of *LNCS*, pages 1–9. Springer, 2005.
19. Michael Froomkin. The Death of Privacy? *Stanford Law Review*, 52(5):1461–1543, 2000.
20. A. Joshi, K. Joshi, and R. Krishnapuram. On Mining Web Access Logs. In *Proceedings of the 2000 ACM SIGMOD Workshop on Research Issues in Data Mining and Knowledge Discovery*, pages 63–69. ACM, 2000.
21. Dogan Kesdogan, Vinh Pham, and Lexi Pimenidis. Information Disclosure in Identity Management. In *Proceedings of 12th Nordic Workshop on Secure IT-Systems, Reykjavik, Iceland, 11-12 October 2007*, 2007.
22. Joe Kilian and Erez Petrank. Identity Escrow. In *Advances in Cryptology - CRYPTO '98*, volume 1462 of *LNCS*, pages 169–185. Springer, 1998.

23. Yehuda Lindell. Anonymous Authenticaion. *Whitepaper Aladdin Knowledge Systems, 2007, `http://www.aladdin.com/blog/pdf/AnonymousAuthentication.pdf`.*
24. Anna Lysyanskaya, Ronald L. Rivest, Amit Sahai, and Stefan Wolf. Pseudonym Systems. In *Proc. of the 6th Annual International Workshop on Selected Areas in Cryptography*, volume 1758 of *LNCS*, pages 184–199. Springer, 2000.
25. Leonardo A. Martucci, Markulf Kohlweiss, Christer Andersson, and Andriy Panchenko. Self-Certified Sybil-Free Pseudonyms. In *Proceedings of the first ACM conference on Wireless network security, WiSec '08*, pages 154–159, New York, NY, USA, 2008. ACM.
26. Moni Naor. Deniable Ring Authentication. In *Advances in Cryptology - CRYPTO '02*, volume 2442 of *LNCS*, pages 481–498. Springer, 2002.
27. Andreas Pashalidis and Bernd Meyer. Linking Anonymous Transactions: The Consistent View Attack. In *Privacy Enhancing Technologies, 6th International Workshop, PET 2006, Cambridge, UK, June 28-30, 2006, Revised Selected Papers*, volume 4258 of *LNCS*, pages 384–392. Springer, 2006.
28. Pino Persiano and Ivan Visconti. A Secure and Private System for Subscription-Based Remote Services. *ACM Trans. Inf. Syst. Secur.*, 6(4):472–500, 2003.
29. Andreas Pfitzmann and Marit Köhntopp. Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology. In *International Workshop on Design Issues in Anonymity and Unobservability*, volume 2009 of *LNCS*, pages 1–9. Springer, 2000.
30. Jean-François Raymond. Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems. In *International Workshop on Design Issues in Anonymity and Unobservability*, volume 2009 of *LNCS*, pages 10–29. Springer, 2001.
31. Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to Leak a Secret. In *Advances in Cryptology – ASIACRYPT '01*, volume 2248 of *LNCS*, pages 552–565. Springer, 2001.
32. Jane Sarasohn-Kahn. The Wisdom of Patients: Health Care Meets Online Social Media. http://www.chcf.org, April 2008.
33. Stuart Schechter, Todd Parnell, and Alexander Hartemink. Anonymous Authentication of Membership in Dynamic Groups. In *Proc. of the 3rd International Conference on Financial Cryptography*, volume 1648 of *LNCS*, pages 184–195. Springer, 1999.
34. Andrei Serjantov and George Danezis. Towards an Information Theoretic Metric for Anonymity. In *Proceedings of Designing Privacy Enhancing Technologies*, volume 2482 of *LNCS*, pages 41–53. Springer, 2002.
35. Jaideep Srivastava, Robert Cooley, Mukund Deshpande, and Pang-Ning Tan. Web Usage Mining: Discovery and Applications of Usage Patterns from Web Data. *SIGKDD Explor. Newsl.*, 1(2):12–23, 2000.
36. Isamu Teranishi, Jun Kurukawa, and Kazue Sako. k-Times Anonymous Authentication. In *Advances in Cryptology – ASIACRYPT '04*, volume 3329 of *LNCS*, pages 308–322. Springer, 2004.
37. Wen-Guey Tzeng. A Secure System for Data Access Based on Anonymous Authentication and Time-Dependent Hierarchical Keys. In *Proc. of the ACM Symp. on Information, computer and communications security*, pages 223–230. ACM, 2006.