PRACTICAL ANONYMOUS AUTHENTICATION
Designing Anonymous Authentication for Everyday Use

Jan Hajny, Lukas Malina and Vaclav Zeman

Department of Telecommunications, Brno University of Technology, Purkynova 118, Brno, Czech Republic

Keywords: Anonymity, Privacy, Authentication, Efficiency, Responsibility, Smart-cards.

Abstract: We use authentication services many times a day. Without user authentication, it would be impossible to use e-mail accounts, discussion boards, e-banking or even electronic communication. On the other hand, we release a lot of personal information during every authentication process. Our login can be linked to used services and assets by service providers. The frequency of usage and therefore the map of our behaviour on the Internet can be created to make more focused advertisement, to track us or even to steal our electronic identity. The goal of this paper is to state the requirements and provide the initial design for an anonymous authentication scheme which prevents the leakage of private information. The new scheme, to be widely acceptable, must be beneficial for both users and service providers, who implement the authentication systems. Therefore we claim that the new authentication system must provide a feature for revealing dishonest users. These users can be eventually deanonymized and charged for damages. We provide such a responsibility-protecting feature in our scheme. We also compare our scheme design with current anonymous authentication schemes and provide initial performance results from our smart-card implementation.

1 INTRODUCTION

By providing a scheme introduced in this paper, we would like to encourage Internet service providers to implement anonymous authentication protocols because it is no more inconvenient for them. By using our scheme, they do not loose their ability to identify attackers and dishonest users. On the other side, their honest users can be now anonymously verified as members of the group of valid clients (e.g., clients who paid for the service). This can be done efficiently and with the use of hardware available today. To prove this, we provide results from the implementation on off-the-shelve .NET smart-cards, which are widely available for purchase. We would like to stress that we used the smart-cards and the framework without any modification, thus without need for any changes in standards.

1.1 Related Work

We find anonymous authentication systems, e.g., the scheme by Schaffer and Schartner (Schaffer and Schartner, 2006), to be the most related systems. These schemes allow anonymous authentication but often rely on trusted third parties. The mentioned scheme is based on a device which must be trusted not to reveal private information. We would like to avoid such design. The second common problem is repeated authentication. Using existing schemes, the user cannot be authenticated infinitely many times without re-initialization. Our scheme provides unlimited number of authentication sessions without the need to repeatedly connect the smart-card to user's PC.

The credential systems, represented by (Lysyanskaya, 2001; Camenisch and Lysyanskaya, 2003; Camenisch and Van Herreweghen, 2002; Bichsel et al., 2009), are also usable for anonymous authentication. Although these systems can be used in many scenarios for privacy protection, only some of them provide real identity revelation of dishonest users. Such feature is provided in theory (Camenisch and Lysyanskaya, 2003) but the implementation would be very inefficient or even impossible on current smart-cards.

1.2 Our Contribution

Our goal is to provide a universal system which will be convenient for both users and service providers. As existing work is focused on either users or service providers, their schemes are often hard to implement

Hajny J., Malina L. and Zeman V..
PRACTICAL ANONYMOUS AUTHENTICATION - Designing Anonymous Authentication for Everyday Use.
DOI: 10.5220/0003576404050408
In *Proceedings of the International Conference on Security and Cryptography* (SECRYPT-2011), pages 405-408
ISBN: 978-989-8425-71-3

since they are not acceptable by both groups. In contrast to these existing schemes, we provide a scheme where honest users can anonymously access restricted services of service providers while providers can still de-anonymize dishonest users and make them responsible for their acts. This solution comes at no extra performance cost in comparison to existing schemes. In fact, our scheme is more efficient than most common anonymous authentication solutions and is practical even on slow devices like smart-cards.

We also focus on the security of the scheme. The building blocks are based on provable cryptography, so the scheme can be analysed from the security point of view and the proofs of security can be given.

In this paper, we propose the initial design of the scheme and give our preliminary performance results with the comparison to related work. We also provide a proof of concept by creating an implementation on a .NET smart-card. The results of first tests are included. In this position paper, we do not provide full cryptographical analysis of the scheme and all proofs, since these details can be found in the full paper.

2 SCHEME DESCRIPTION

This section is divided into three parts: the statement of requirements, the description of the communication pattern and the cryptographic primitives used.

2.1 Requirements

The anonymous authentication scheme, to be acceptable and implementable in practice, must provide following features.

- Completeness: valid users must be always accepted.
- Soundness: invalid users must be always rejected.
- Anonymity: honest users cannot be identified during authentication.
- Unlinkability: verification sessions must be unlinkable.
- Responsibility: dishonest users must be identifiable.
- Efficiency: the scheme must be efficiently implementable even on weak devices like smart-cards.
- Manageability: users can be easily added or removed from the group of valid users.
- Security: the scheme must be provably secure, based on strong primitives.

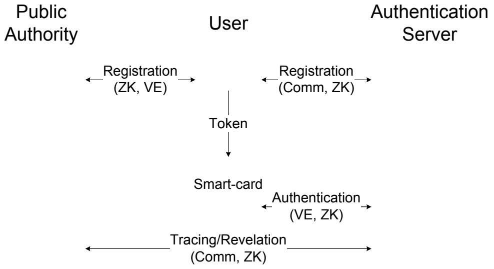

Figure 1: Communication Pattern of the Proposed Scheme.

Our system gathers all these requirements in one scheme, thus provides a universal solution for anonymous user authentication.

2.2 Communication Pattern

The scheme we propose in this paper is based on three players. They are the user, Authentication Server (AS) and Public Authority (PA). The roles of these players and their description is following:

- **User**: the user wants to be anonymously verified as a valid user of a service. The example is the anonymous access to a discussion board, where only registered users can enter, but where the content which is read by a particular user cannot be tracked. The user wants to stay anonymous and can use a smart-card for authentication.
- **AS**: the Authentication Server wants to verify users before it allows them to use its services. The role of AS is to decide, whether the user is valid (e.g., registered or paying some fees). AS should not be able to learn the concrete identity of a user, only the information whether he is allowed to use a service.
- **PA**: the Public Authority is a player who is used in the case of dispute. Without PA, the AS is unable to learn the identity of a user. PA can be distributed to more entities to lower the trust to a single point of failure.

The scheme consists of three protocols. The first protocol is user registration, the second is the authentication protocol and the last one is the revelation protocol. The purpose of the registration protocol is to establish an authentication token, which will be stored on user's smart-card and later used for authentication. The registration is done over a computer network (likely Internet) using anonymous routing protocols like TOR (Dingledine et al., 2004). All three entities are involved during this phase.

The second protocol is the authentication protocol. It runs between the user's smart-card and AS. The protocol allows user to provide a proof, that the token is valid, anonymously, without leaking information about his identity or previous uses of the token. That is why the authentication phase is anonymous and unlinkable to previous authentication phases. The provided proof is always randomized, thus the single token can be used many times without the concern about its tracing.

The last protocol is the revelation protocol. This protocol is executed between AS and PA when some disputes occur in the system. In that case, AS can contact PA and give proofs about disputes, rule breaking or e.g. some thefts in his systems. The PA then decides, whether proofs are strong enough, and if yes, it continues in user revelation. The user can be anonymously removed from the system, traced in the system (but not identified) or completely identified. The level of revelation depends on PA, therefore AS cannot break users' privacy without proofs of strong policy violation.

All described protocols are efficient, their complexity does not depend on the number of users. The authentication protocol, which will be the most used protocol, is practical for smart-card implementation. The whole communication pattern is depicted in Figure 1. The figure also includes cryptographic primitives placement, described in Section 2.3.

2.3 Used Primitives

In this section we provide information on our choice of used cryptographic primitives together with their placement in the scheme. In the registration protocol, the discrete logarithm (DL) commitments and proofs of representation (Camenisch and Stadler, 1997) are used during the communication with AS. During the communication with PA, we use proofs of representation and Bao's verifiable encryption (Bao, 2000). We also assume the existence of a secure signature scheme, like RSA.

The registration protocol starts with the user choosing a random number and creating a DL commitment to it. The knowledge of the secret number is then proven to AS by running the proof of representation on the commitment. AS can therefore link user identity with the commitment, while user's secret number remains hidden. AS stores the commitment in its database and provides the user with the signature on the commitment. The user then anonymously contacts PA and anonymously provides the commitment and AS's signature. He also has to provide the proof of knowledge of the secret number in the commitment using (Schnorr, 1991). Based on this information, PA creates the token with user's commitment inside. The token is unlinkable to user's secret number and to his commitment for anyone except PA. The user then transfers the token to his smart-card.

The authentication phase is a proof of representation (Camenisch and Stadler, 1997; Schnorr, 1991) of the token, thus a proof of knowledge of a secret number chosen by the user and a second secret number given by PA during the registration. Based on the proof of representation, AS can be efficiently convinced about the right token construction.

The revelation protocol is based on the DL verifiable encryption (Bao, 2000). The secret user number is hidden in a verifiable encryption and given to AS during the authentication protocol. AS can verify the construction of the encryption, but is unable to decrypt. The only entity able to decrypt is PA, therefore AS can resend the verifiable encryption to PA, which is able to decrypt and either remove the user from the system or release the real identity of the user to PA. The removal of the user is done by publishing the DL commitment of users secret value. Such published values create a ”blacklist” of removed users, who are no more able to be successfully authenticated.

The described primitives (the verifiable encryption (VE), commitments (comm) and proofs of representation (ZK)) are placed in the scheme as visible in Figure 1. The detailed description of primitives and all supporting mechanisms is out of the scope of this short paper and will be published in the full paper.

3 TESTING SMART-CARD IMPLEMENTATION

One of our main goals is to provide a scheme efficient enough for a smart-card implementation. The implementation of modular addition, subtraction or exponentiation is easy due to low complexity and the ability to delegate some computations to RSA crypto co-processor. Multiplication is more difficult to implement since no direct function is available in the framework. We compared more approaches to modular multiplication, from paper-and-pencil method, Comba's method, Montgomery multiplication to the trick provided in (Bichsel et al., 2009). From the results it is obvious that the most efficient method is the so called RSA tunnel method from (Bichsel et al., 2009), where multiplication is converted to exponentiation using the binomial formula and then accelerated using the RSA function. This method is introduced for Java smart-cards in (Bichsel et al., 2009).

3.1 Performance Analysis

Based on modular multiplication and exponentiation implemented by us on a .NET smart.card, we created a testing implementation of our scheme. We used the .NET smart-card V2+ platform with no additional modification. The authentication phase, with all features presented in this paper, was implemented on the smart-card. Since the scheme works with modular arithmetic, we tried several moduli sizes to analyse the effects on the performance of the system. The dependency of the verification time on the size of the modulus can be seen in Figure 2. The optimal size of the modulus is 1024 b. The performance loss above 1408 b is given by the implementation of RSA on the smart-card and the improvement of the performance for higher moduli is one of our future concerns. The most related system is the Idemix credential system (Camenisch and Lysyanskaya, 2003) implemented on a Java smart-cards (Bichsel et al., 2009).

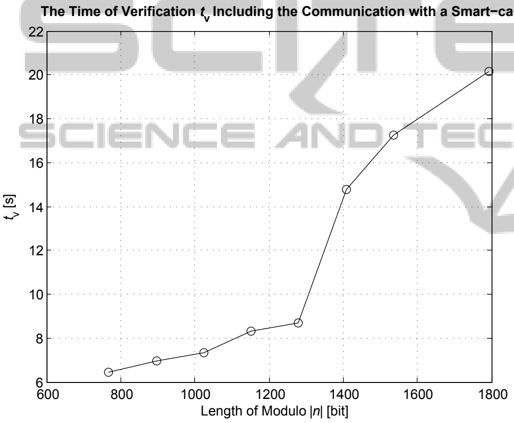

Figure 2: The Dependency of the Verification Time on the Modulus Size.

Current implementation provides reasonable verification times around 8 s, in comparison to related implementations on Java smart-card (Bichsel et al., 2009), which need around 10 s.

4 CONCLUSIONS

The paper introduced a new scheme for anonymous authentication. Unlike related work, our scheme combines features required by both users and service providers. Using our scheme, the user can be authenticated without real identity revelation and the service provider can be sure about the control over his assets. We provided the communication pattern of the scheme and identified cryptographic primitives used. The scheme is very efficient and implementable on weak devices like smart-cards. Nevertheless, the works are still in progress and we expect a significant performance improvement. Our goal is to reach 30 % performance advantage over related schemes, an increase which is achievable based on the theoretical construction of the scheme. Moreover, we are working on the support of ”attribute authentication”, where users can prove not only the group membership but any attribute ownership (e.g., driving licence, age, citizenship).

ACKNOWLEDGEMENTS

Sponsored under the National Program of Research II by the Ministry of Education, Youth and Sports of the Czech Republic in 2C08002 Project - KAAPS Research of Universal and Complex Authentication and Authorization for Permanent and Mobile Computer Networks.

REFERENCES

Bao, F. (2000). An efficient verifiable encryption scheme for encryption of discrete logarithms. In Schneier, B. and Quisquater, J.-J., editors, *Smart Card. Research and Applications*, volume 1820 of *Lecture Notes in Computer Science*, pages 213–220. Springer.

Bichsel, P., Camenisch, J., Groß, T., and Shoup, V. (2009). Anonymous credentials on a standard java card. In *Proceedings of the 16th ACM conference on Computer and communications security*, CCS ’09, pages 600–610, New York, NY, USA. ACM.

Camenisch, J. and Lysyanskaya, A. (2003). A signature scheme with efficient protocols. In *Proceedings of the 3rd international conference on Security in communication networks*, SCN’02, pages 268–289, Berlin, Heidelberg. Springer-Verlag.

Camenisch, J. and Stadler, M. (1997). Proof systems for general statements about discrete logarithms. Technical report.

Camenisch, J. and Van Herreweghen, E. (2002). Design and implementation of the idemix anonymous credential system. In *Proceedings of the 9th ACM conference on Computer and communications security*, CCS ’02, pages 21–30, New York, NY, USA. ACM.

Dingledine, R., Mathewson, N., and Syverson, P. (2004). Tor: The second-generation onion router. In *In Proceedings of the 13 th Usenix Security Symposium*.

Lysyanskaya, A. (2001). An efficient system for non-transferable anonymous credentials with optional anonymity revocation. pages 93–118. Springer.

Schaffer, M. and Schartner, P. (2006). Anonymous authentication with optional shared anonymity revocation and linkability. In *Smart Card Research and Advanced Applications*, volume 3928 of *Lecture Notes in Computer Science*, pages 206–221. Springer Berlin / Heidelberg.

Schnorr, C. P. (1991). Efficient signature generation by smart cards. *Journal of Cryptology*, 4:161–174.