SECURE AUTHENTICATION FOR SMART-CARDS

Lukáš Malina and Jan Hajný
Doctoral Degree Programme (1), FEEC BUT
E-mail: lukas.malina@phd.feec.vutbr.cz, jan.hajny@phd.feec.vutbr.cz

Supervised by: Karel Burda
E-mail: burda@feec.vutbr.cz

Abstract: The goal of this paper is to give an introduction to the topic of user authentication and privacy protection. We provide an overview of current authentication systems and systems for providing anonymity. Based on the current state analysis we briefly describe a new proposal for an anonymous authentication protocol. The protocol provides standard features known from current systems, but adds more features for privacy protection. Using advanced cryptography, we are able to protect all private information of users during the authentication against any verifiers. The protection is provably secure and efficient, which is shown on implementation results.

Keywords: Cryptography, authentication, privacy, smart-cards

1 INTRODUCTION

Currently there are many protocols usable for user authentication in the Internet. These protocols are mostly based on the possession of secret information, mostly on passwords or private keys from a Public Key Infrastructure (PKI). Using these protocols means giving our identifier (e.g. a username) and our secret (e.g. a password) to a verifier, who is then able to verify, whether these credentials are correct. We use such an authentication procedure every time we access our emails, social network accounts, internet banking or a discussion board. With the growing number of services more and more service providers know our login information. Based on that knowledge, the service providers can track your behaviour – e.g. what types of services do we access, how often we use their services and how we use service providers' assets. Moreover these information can be shared among multiple service providers, or sold to advertising companies. The information about Internet user behaviour is becoming more and more valuable, since it has a direct relation to e-business.

This potential leak of private information has been already identified and therefore many systems for privacy protection have been developed. There are systems for anonymous authentication, where only group membership is verified, and there are also credential schemes usable for multi-purpose verification of user attributes (e.g. usable in electronic passports, IDs or access cards). Nevertheless these anonymous systems are not very convenient for service providers, since they lose control over their assets. An anonymous user is not responsible for his behaviour, therefore he can damage the system or steal valuable asset without being personally responsible for that.

The goal of the scheme very briefly introduced in this paper is to provide an anonymous authentication protocol, which will provide user accountability. Using such a protocol, the privacy of an honest user is protected, but malicious users can be identified. Therefore this solution is acceptable for both users and service providers.

1.1 RELATED WORK

We mentioned above that currently there are many solutions for user authentication. Protocols like RADIUS [1], Kerberos [2] or EAP [3] are well-known, commonly used and considered secure for a practical deployment. All of these protocols reveal the user identity to the verifier, thus the verifier is able to track user behaviour. There are also many proposals for privacy protection protocols, e.g. anonymous authentication protocols [4] or credential schemes [5]. Most of these protocols do not provide user accountability, since the real identity of a user cannot be revealed. Even if there is a protocol with the real identity revelation feature, the feature is not efficiently implementable on personal devices like smart-cards. That is the reason why we propose our scheme, which has same features as modern privacy protection protocols, but on top of that adds efficient features for real identity revelation of (only!) dishonest users. It is also important that our scheme provides around 30 % better efficiency in a smart-card implementation.

2 SMART-CARDS AND PROTOCOL OPTIMIZATION

Our implementation of the anonymous authentication protocol is based on the usage of smart-cards. Using a device similar to current credit-cards it is possible to run the whole authentication phase of the user. The smart-card holds the secret information, which is used during the verification of the user. The authentication protocol takes place between the smart-card and a terminal with a card reader. Since the protocol is based on advanced cryptographic primitives, it is necessary that the smart-card is capable of non-trivial computations. We demand efficient modular exponentiation and multiplication to be provided by the smart-card. Unfortunately, these operations are not provided by standard smart-cards (at least not for numbers as large as we need), therefore we had to create our own implementation of these operations. We used the cryptographic co-processors, which are common on modern smart-cards, for computation acceleration. Based on [6] we implemented a method for fast modular multiplication, which is considerably faster than any common method, due to the use of hardware acceleration. The performance gain is very clear for higher moduli ($>$ 700 b). The results can be seen in Figure 1. The modular exponentiation operation was implemented using the standard interface for RSA encryption function, which is basically the exponentiation, as seen in Equation 1

$$c = m^e \bmod n \tag{1}$$

where m is a plaintext for encryption (a base in our case), e is a public key (an exponent in our case) and n is a public key (a modulus in our case).

3 SECURE AUTHENTICATION PROTOCOL

Our protocol has 3 entities, namely a user, who wants to get verified, an Authentication Server (AS), who wants to verify the user, and a Public Authority (PA), who serves as a partially trusted third party, who is able to revoke/identify malicious users. The communication starts with the user requesting data needed for authentication token construction from AS and PA. Based on these data the user is able to construct a token for user authentication. The token is put on a smart-card and the authentication phase between the user and AS can take place. After the authentication protocol is finished and the user e.g. breaks some policies of AS, his identity can be revealed, but only by a joint cooperation of PA and AS. The privacy of users is secured since PA is revealing the identity of a User only if proofs of policy breaks are given by AS. The communications scheme is depicted in Figure 2.

The main idea of the scheme is to let the user choose his own secret number and let him create a commitment to it. The commitment is made public, so the user cannot change his mind and choose a different number later. Nevertheless the chosen number is still secret, since the commitment reveals no information about the value of the chosen number. Then the commitment is bound by AS and PA to a user token, without any revelation of user's secret number. The token can be used for authentication multiple times using a specific randomization process. This is due to the fact, that during the authentication phase AS is able to verify, whether the valid commitment is inside the token or not.

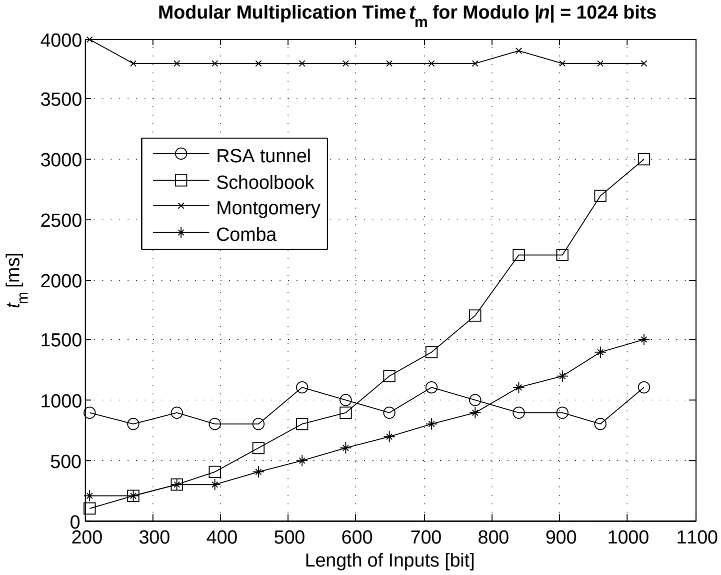

Figure 1: The comparison of various techniques for modular multiplication.

Later, if any policy breach is detected by AS, then the commitment can be revealed by the cooperation of PA and AS and from the commitment there is a unique link to user's unique identity. Thus the user can be held responsible for his acts.

The commitments are created using the commitment scheme which is secure under the discrete logarithm (DL) assumption. For construction proofs we used provably secure protocols (proofs of DL equivalence) also based on DL assumption. The authentication process is based on a verifiable encryption scheme, which is based on hardness of factorization assumption. The whole authentication process can be proven secure, since it is possible to build a theoretical protocol simulator. Using this tool common in most security proofs, we are able to provide an evidence, that no secret information is released during the protocol run. This is based on the fact, that the output of the simulator (which does not know the secret numbers) is computationally indistinguishable from the real run of the protocol.

The cryptographic background of the whole scheme is out of the scope of this paper, nevertheless we list cryptographic primitives used to construct the scheme. We used Zero-Knowledge proofs (ZK) [7], Σ-protocols [8], Verifiable Encryption (VE) schemes [9], One-Way Trapdoor Function [10] and commitments. The placement of these primitives is depicted in Figure 2 and details can be found in the full paper.

4 IMPLEMENTATION RESULTS

In the beginning of this paper we claimed that our implementation is more efficient than the modern schemes for privacy protection. We compare our scheme to the Idemix implementation [6], which requires 9 modular multiplications, 10 exponentiations and 7 additions with size of the modulus of $|n| = 1536$ per verification. Our scheme needs 6 modular multiplications and exponentiations and 4 additions in a same size of the modulus. This results in around 30 % performance gain and the decrease of verification time from over 11 s to 8 s. We would like to stress out that our implementation works as a proof-of-concept only and therefore a major performance increase is expected by more efficient programming. The performance of all modular methods (including the time needed for communication with the card) is shown in Table 1.

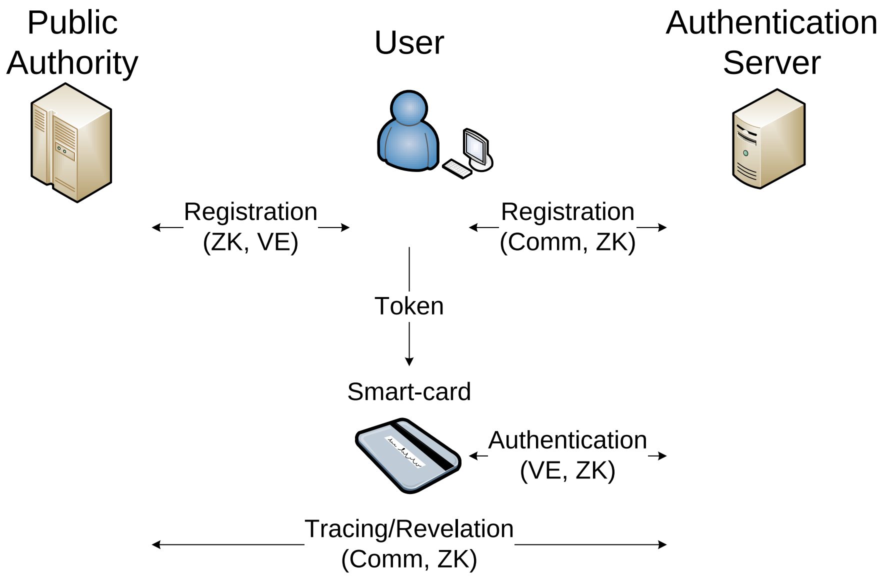

Figure 2: Communication pattern of proposed scheme

Input length	Time of computation t				
$\|a\| = \|b\|$	Addition	Subtraction	Division by 2	Exponentiation by 2	Multiplication
[bits]	[ms]				
160	303	377	290	237	830
512	342	376	288	234	823
1024	352	379	296	237	880
1280	372	384	299	280	952
1536	382	388	307	281	1167

Table 1: Time t required for computing arithmetic operations for the modulus length $|n| = 1024$ b.

5 CONCLUSION

The goal of this paper is to give a brief introduction to our anonymous authentication scheme. Although there are no complex technical details, which are too extensive for a short paper, we presented the basic idea of the developed scheme, the implementation results and the comparison with related works. The most important results – the fast modular multiplication running on smart-cards and the anonymous authentication scheme – are currently in the process of publication, therefore all details can be found in the full papers. By using the fast modular multiplication method in the newly designed authentication scheme we get a way how to authenticate a user without releasing his private information. This can be done more efficiently than in the case of comparable schemes. The improvement in efficiency is around 30 %, which was verified on a real-world implementation on .NET smart-cards.

ACKNOWLEDGEMENT

The research was supported by the project for Specific Research BD18012 "Výzkum autentizace a autorizace v moderních počítačových sítích".

REFERENCES

[1] Rigney, C.: Remote Authentication Dial In User Service (RADIUS). 1997, http://www.faqs.org/rfcs/rfc2138.html.

[2] Kohl, J.: The Kerberos Network Authentication Service (V5). 1993, http://www.faqs.org/rfcs/rfc1510.html.

[3] Aboba, B.: Extensible Authentication Protocol (EAP). 2004, http://www.ietf.org/rfc/rfc3748.txt.

[4] Schaffer, M.; Schartner, P.: Anonymous Authentication with Optional Shared Anonymity Revocation and Linkability. In *Smart Card Research and Advanced Applications*, *Lecture Notes in Computer Science*, volume 3928, Springer Berlin / Heidelberg, 2006, p. 206–221.

[5] Camenisch, J.: Specification of the Identity Mixer Cryptographic Library. Technical report, IBM Research – Zurich, 2010.

[6] Bichsel, P.; Camenisch, J.; Groß, T.; et al.: Anonymous credentials on a standard java card. In *Proceedings of the 16th ACM conference on Computer and communications security*, CCS '09, New York, NY, USA: ACM, 2009, ISBN 978-1-60558-894-0, p. 600–610.

[7] Camenisch, J.; Stadler, M.: Proof Systems for General Statements about Discrete Logarithms. Technical report, 1997.

[8] Schnorr, C. P.: Efficient signature generation by smart cards. *Journal of Cryptology*, volume 4, 1991: p. 161–174, ISSN 0933-2790.

[9] Bao, F.: An Efficient Verifiable Encryption Scheme for Encryption of Discrete Logarithms. In *Smart Card. Research and Applications*, *Lecture Notes in Computer Science*, volume 1820, editor B. Schneier; J.-J. Quisquater, Springer Berlin / Heidelberg, 2000, p. 213–220.

[10] Okamoto, T.; Uchiyama, S.: A new public-key cryptosystem as secure as factoring. In *Advances in Cryptology — EUROCRYPT'98*, *Lecture Notes in Computer Science*, volume 1403, editor K. Nyberg, Springer Berlin / Heidelberg, 1998, p. 308–318.