Identity-Based Cryptography in Credit Card Payments

Kimmo Halunen and Mirko Sailio

VTT Technical Research Centre of Finland,
Oulu, Finland
{kimmo.halunen,mirko.sailio}@vtt.fi

Abstract. In this paper we describe how to apply identity based cryptography to credit card payments. This would help with reducing the possibility of credit card fraud that is prevalent on the Internet. Our method is founded on the identity-based cryptography and it secures the credit card transactions in such a way that many types of credit card fraud become either impossible or much more difficult for the attacker to perform simply by stealing the credit card number and some related information. Our method would require some changes to the functionality of the credit cards and thus it is not an immediate remedy. However, the decreasing costs of more advanced hardware and the fairly fast cycle of reissuing new credit cards make it possible to include identity-based cryptography methods to credit cards in the near future.

1 Introduction

Modern networked society has made it possible to conduct credit card transactions over the Internet and this has had a huge impact on the trade of goods and services across the world. It is now fairly easy to purchase almost anything from anywhere in the world with your laptop or even mobile phone. The payments are usually made using credit cards, although in recent years different online systems such as PayPal and even digital currencies (e.g. Bitcoin [14]) have emerged.

Credit card fraud is a global problem that costs billions of dollars to different actors annually. As the credit cards had emerged already before the explosive growth of online commerce, there were few security measures against novel attacks on payments. New security methods and procedures, e.g., security codes on the back of the card, chip and PIN authentication and the opt-in use of online transactions on the cards provided by some banks, have been deployed as new forms of attacks and fraud have been discovered. Still, the amount of credit card fraud worldwide was over 5 billion dollars in 2012.[1]

The new countermeasures have not been able to stop the growth of credit card fraud especially in the e-commerce. One of the key problems is that the credit card number itself is used partially as a secret that then enables transactions on that card's account. However, this credit card number is stored by many

[1] See http://www.statisticbrain.com/credit-card-fraud-statistics/

Z. Kotulski et al. (Eds.): CSS 2014, CCIS 448, pp. 49–58, 2014.

vendors in order to make the purchasing of goods and services online as easy as possible and can not be considered a secret known only to the credit card holder. This has led to a situation, where attackers can get into their hands sometimes enormously large databases containing credit card numbers. Even though there are standards such as PCI DSS [17] and EMV [6] for processing payments and handling this data and these have helped against fraud, these attacks continue to be successful. In 2013 there were 84 reported hacking attacks with lost credit card numbers with over 250 million credentials lost. The majority of incidents (57) had unknown amount of credentials lost and thus the total tally may be even greater.[2] Also there are some results that show that even the EMV protocols contain weaknesses that can be exploited [2]. Thus, there is a need to enhance the security of credit card payments.

Modern cryptography has provided our society with a wide variety of tools for conducting secure actions over the Internet. Public key cryptography (PKC) in general has made it possible for example to exchange keys between two previously unacquainted entities [4]. More recent developments have provided systems for electronic voting [18], digital signatures [8] etc. One particular special case of public key cryptography is identity-based cryptography (IBC), which was first introduced in [19]. Later on practical constructions realising both identity-based encryption (IBE) [3] and signatures (IBS) [9] have been proposed. With the help of these techniques, new countermeasures against credit card fraud can be devised.

1.1 Our Contributions

In this paper, we introduce a method for applying IBC in credit card payments. In our method, the credit card number, together with some other identifying information, acts as the identity of the person conducting the payments and thus is also the public key in the underlying IBC system. The secret key related to that public key is stored on the card and then used to sign the transactions. This means that the credit card number itself cannot be utilised by an attacker to make fraudulent transactions. The attacker needs to obtain the secret key by some manner and the security proofs of the IBC systems show that this is infeasible by merely knowing the credit card number, i.e., the public key. Our method for credit card payments requires some changes to the payment infrastructure, but provides better security against the theft of the credit card number. We also present an idea of a partial solution that could be used with existing systems, but does not offer all the benefits of our IBC based system and has also some other weaknesses.

This paper is organised as follows. The next section presents the most relevant previous work on IBC systems and some basic information on e-commerce, online payments and credit card fraud. The third section describes the basic theoretical foundations of the IBC systems that can be utilised in our methods. The fourth section contains our proposal for payment system with the help of IBC. Finally, we discuss our findings and their implications and give some conclusions of our work.

[2] `http://datalossdb.org/`

2 Previous Work

As mentioned above, the identity-based cryptography was already proposed in [19]. The first proposal lacked a concrete system over which the IBC could be realised. Fortunately, later on there have been several proposals that provide both IBE and IBS. For example, the scheme in [3] provides identity-based encryption in a fairly efficient manner. An example of an identity-based signature system can be found in [9].

E-commerce is nowadays an integral part of the global economy. When global transactions are concerned, credit cards are one of the most used methods of payment and thus also a very attractive target for criminals. For example, in [16] the trends show that there is a growing amount of malicious software that attacks banking and credit card information. Furthermore, the Internet provides a lot of opportunities to monetise the stolen credit card numbers. The price of a credit card number can vary greatly from a few dollars to hundred dollars or more depending on the known qualities of the card [16].

Today, a lot of research on securing the transactions of the networked world is directed at so-called *cryptocurrencies*. The most famous form of such a digital currency is Bitcoin [14], which has gathered a fairly large (and somewhat underground) economy around it.[3] These new ideas have not yet been adopted as widely as the credit card system and are thus not so vital to the functioning of our e-commerce. There are also many new security issues raised by the new cryptocurrencies.

As the research on cryptocurrencies is getting more and more traction, there have not been very many proposals to improve the security of the credit card payment system. Especially, there has not been research on radical improvements in the system and some of the implemented improvements towards security, such as the '3-D Secure' protocol, have been critiqued [13]. On the other hand, the security of the credit card system has been proven vulnerable by the amount of fraud and the large scale database leaks of large vendors. Furthermore, there has been some critique on the forensic capabilities of the modern credit card payment system, although many other alternatives such as Bitcoin fall short of the required forensic properties [12].

3 Identity-Based Cryptography

IBC systems are usually based on *pairings*. In cryptography, a pairing is defined as a mapping $e : G_1 \times G_2 \to G_3$, where G_1, G_2 and G_3 are the groups of prime order p with the generators g_1, g_2 and g_3 respectively. Furthermore, the pairing needs to satisfy two conditions: For all $a, b \in \{0, 1, \ldots, p-1\}, e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$ and $e(g_1, g_2) \neq 1 \in G_3$. Also these pairings need to be efficiently computable in order to be useful. The Weil pairing and the Tate pairing over elliptic curves have been popular choices to build IBC systems on. An interested

[3] See for example `https://coinmarketcap.com/` for recent trading volumes.

reader can find more on the basic properties of pairings and a survey of IBC systems in [5].

Pairings have also been used in the attribute-based cryptography, which offers a more granular approach to user identities (see for example [11,15] for concrete proposals). In the attribute-based cryptography, there is no single identity, but a set of attributes that are verified by some attribute authorities. Then different predicates over these attributes can be formed and for example signatures attesting to having a certain set of attributes can be computed. Thus, in contrast to IBC, the "complete" identity of a user does not need to be revealed.

One important thing to note about IBC is that the identities in this respect do not need to be identities as we usually understand them. The identity information can be some string of information related to identity, e.g., an email address, name or even social security number. The methods of IBC map this information to a public key of a cryptosystem and also generate the corresponding secret key to form a public/private key pair. Usually, this is done with the help of cryptographic hash functions, which can map arbitrary strings of information into values of a fixed length. Furthermore, hash functions ensure that the likelihood of a collision, i.e., two-identities mapping to same hash value, is negligible.

4 Applying IBC to Credit Cards

In this section we present our method for applying IBC to credit cards. We also discuss the effect of our system to the overall credit card payment ecosystem.

4.1 Our Method

The standard four-party payment card scheme is described in Figure 1. Our proposal would be a new specification on the Payment card scheme that is utilised in the transactions between the different parties and is presented in the center of Fig. 1. The Cardholder is making an (online) purchase from the merchant that wants to receive payment from the Cardholder. The Issuer has granted the Cardholder a credit card and generates a public/private key pair for that card. The private key is stored on the credit card and is awarded to be used by the Cardholder. In addition, the card could also have separate functionality to identify or authenticate the Cardholder. The purpose of the card is to conduct signature operations on the chip in order to facilitate payment.

The public key, i.e. the identity, would be the credit card number of the Cardholder's card together with the expiry date. This would be signed with the credit card Issuer's private key. Also other identifying information such as the Cardholder's name may be included to the public key. However, adding too much identity information on the public key makes the system more cumbersome and may lead to situations, where the card needs to be replaced too often. The credit card number and expiry date at least are usually required by the vendors and thus should be considered public information in any case. Name, address and other identifying information are also many times required for purchases,

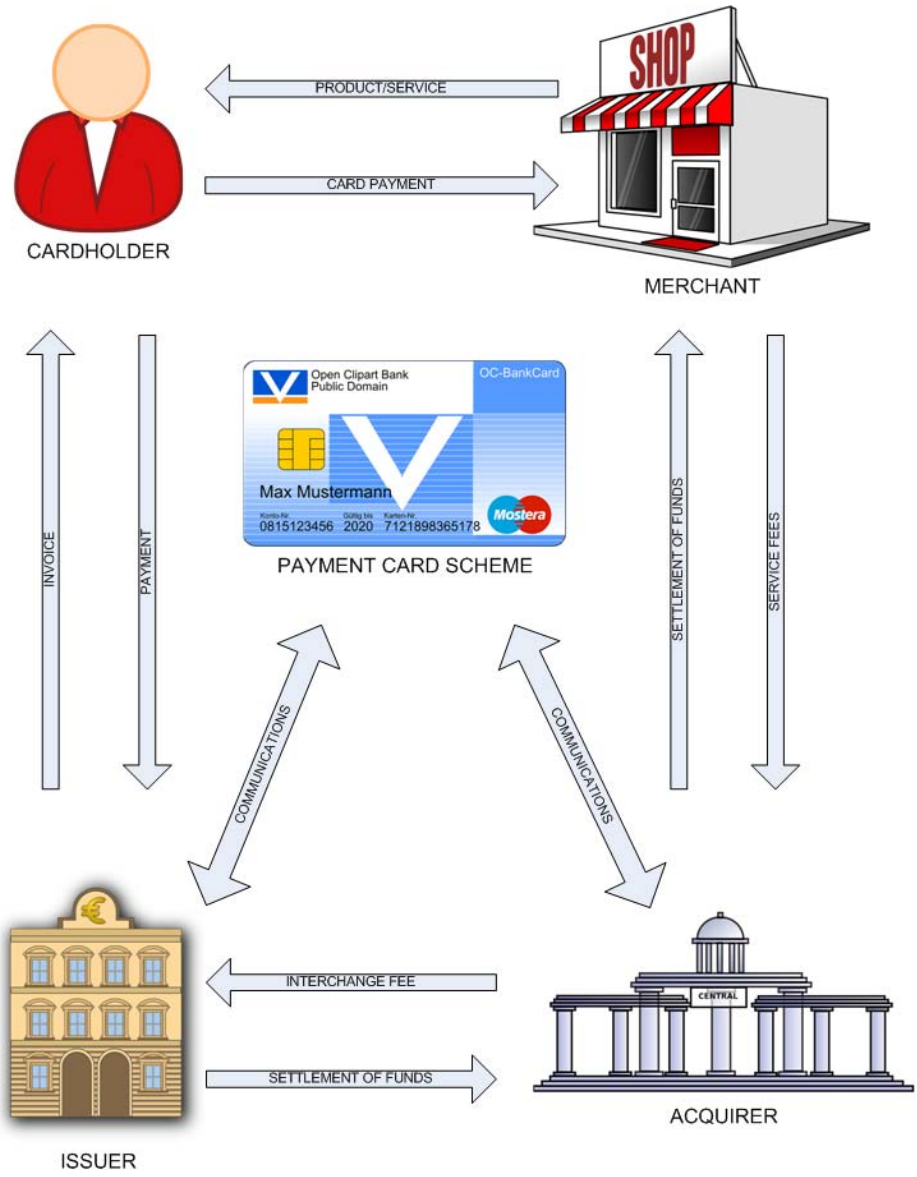

Fig. 1. Standard Four-Party Payment Card Scheme

but may be a subject to changes during the validity period of the card and thus be limiting factors in the use of the credit card.

If the card provided to the Cardholder does not contain methods for identifying or authenticating the Cardholder and communicating the results of the signature computation to the payment framework, it can only be used with point

of sale systems or with other card reader mechanisms. Then the system interacts with the card and conducts the signing after the reader has received authentication from the Cardholder, e.g., the Cardholder enters her PIN to the terminal. If the card has the functionality to both authenticate the Cardholder and to communicate with other parts of the framework, there is no need for external readers. This could be a simple numerical pad and a small display for showing the results of the computations to the Cardholder or some wireless communication method for directly communicating the results to the requesting party.

After the signing of the transaction, an authorisation request would go through its designated route in the credit card payment ecosystem to the card issuer as described in Figure 1. After the Issuer receives the request, it can check the validity of the signature (as can any other party with access to the Cardholder's public key), check available funds and decide whether to approve or deny the request. Also the Merchant could check the signature for validity after confirming the certificate on the Cardholder's public key. It is assumed that the public keys of card issuers are available for all merchants that accept credit cards from these issuers.

4.2 Credit Card Payment Ecosystem

The presentation of Figure 1 is somewhat a simplified view of the credit card ecosystem and in reality there are a few more different stakeholders in the credit card payment ecosystem and it is important to know how our proposed changes would affect their view of the system. The most evident players are of course the customer and the merchant. In addition to them, there are several other entities involved.[4] In the following, we briefly mention some of the other stakeholders and the possible effect of our method on their position.

First of all, there is the bank or credit card issuer of the customer. In our system this party would be responsible for issuing the credit card and providing the IBC functionality on the credit card. Thus, one of the biggest burdens of changing the system would be carried by the issuers. The merchants would also need to update their systems to accept these new types of credit cards. These updates might require new readers that can be prohibitively expensive. On the other hand, the updates might be possible at software level and not be that expensive to deploy.

Usually, the online payment is processed via a payment gateway, that finds the correct processors for payments. Furthermore, the payment processor authorises payments for different businesses and communicates with the credit card interchange that either acts on behalf of the credit card issuer (in the case of many large credit card companies) or furthers the request to the issuing bank. The merchant's bank handles the transaction from the merchant's side, i.e., accepts the money from the credit card interchange or the card issuing bank. These parties would not necessarily need to make much adoptions as most of these

[4] See for example `http://www.practicalecommerce.com/articles/168-Credit-Card-Processing-How-It-All-Works`

could adopt the new IBC infrastructure and make their respective checks on the signatures with the IBC. Also, the system as a whole would not need to be overhauled and it would be possible to forward the requests based only on the certificate on the public key of the customer's credit card. There is no need to new trust relationships as the card issuers can be the facilitators of the new IBC infrastructure.

4.3 Partial Solution Without IBC

As the merchant databases have been a popular source of credit card information for the attackers, there is an incentive to try to keep the merchant from storing the sensitive credit card number in its database. The above IBC based method solves this problem, but with the introduction of new public key infrastructure. Below we detail another possible solution to this problem that has the benefit of being usable without any new public key cryptography infrastructure for the credit card issuer and the merchant.

Our solution would be to treat the credit card number and expiry date (and possibly other identity information) as a (single) password that is used to authenticate the transaction. With this method, the expiry date could be public and available in the clear for the merchant. The credit card number, expiry date and other data would be hashed with a secure password hashing method and this value would be stored by the merchant. Thus the merchant would not have the real credit card number stored. The authorisation of the transaction could be conducted by a well-established password based authentication protocol, e.g. [1] and should also include unique transaction numbers to prevent replay attacks. By using tag-based methods (see [7,10] for more details), the transaction number and other relevant information can be linked to the password-based authentication.

One downside of the above method is that the guessing of a credit card number from such a hash value could be fairly easy. There is fairly little entropy in the credit card numbers as they convey a fairly large amount of information about the issuing bank etc. and thus are not even close to random strings of digits. Any attacker obtaining the hashes could use this information to speed up their guessing activities and even if the numbers were completely random, 16 decimal digits is not enough to withstand brute force attacks. Thus, it is our opinion that the IBC based method presented earlier is far superior to this partial solution, even though it requires completely new infrastructure to operate and is not applicable online without new capabilities on the credit cards.

5 Discussion

Our proposal presents a novel way to apply IBC systems to a practical and global problem. However, some of the benefits that can be gained with our methods require changes in the credit card payment infrastructure. As the industry is both global and somewhat slow to adopt changes, it is possible that new systems implementing our method cannot be delivered to all customers in a timely

manner. In any case, it is important to provide new options to increase security in credit card payments.

The most evident limitation of our proposed method is that it cannot be used without utilising the secret within the credit card. Thus, for backwards compatibility with legacy systems, the old way of payments may be needed in parallel to the new one. This could be overcome in a fairly short amount of time as the processing power and capabilities of the credit cards could increase and provide a way to interact with the payment ecosystem without a special reader. This could be done for example with integrated numerical pads or other means of input as well as some small displays on the credit cards. Then a standard challenge-response protocol could be utilised even in online transactions made from computers, handheld devices and other personal devices. However, credit cards are replaced in a fairly fast cycle of a few years and thus this new technology could reach customers in a few years.

The other part of the problem is in the point of sale terminals which are not replaced that often. Furthermore, there is a disparity between different regions in the world and many old systems are still in use in the developing countries and other parts of the world that have not yet been able to adopt for example the chip and PIN systems. This could be a more complicated problem, especially if there is no possibilty to update the terminals with only a software update. When parallel systems for payments exist, the attackers will choose the weakest one for their purposes.

Also at the moment it seems that the most advanced proposals of IBC systems are not yet optimised for the efficient use in resource constrained devices such as credit cards. Thus, the credit card itself could only be used as a storage device for the secret key at first. However, as already mentioned above, the capabilities of the credit cards and the chips used on them become more powerful and will soon enable the full-fledged use of IBC in consumer settings.

In any case, our proposal would make it more secure for the merchant to store the credit card numbers of their customers or not to store them at all. The very idea of public key systems is that the public key information cannot be used to conduct actions that require the knowledge of the secret key, nor can any information about the secret key be inferred from the public key. Thus, an attacker does not stand to gain anything from the knowledge of the credit card number or any other property used as the public identity.

As with almost all public key infrastructures, there is the question of reliability of the public identities. This should be addressed by the card issuers and it is their responsibility to make checks on the customer as it is also their incentive not to give credit to unreliable customers. The issued credit card should also include a digital certificate for the public key of that card. This certificate should be provided to the merchant that the card holder makes purchases from. The certificate would be signed by the card issuer and the merchant would have the card issuers public key for checking the certificate for validity.

6 Conclusion

In this paper we described one possible application of identity based cryptography in protecting credit card transactions. Our method would require new public key infrastructure to be established on the credit card ecosystem, but it would effectively make stealing the credit card numbers en masse from different e-commerce vendors ineffective for the attackers. The attackers would need to steal the private keys from the individual credit cards in order to do similar damage as with mere credit card numbers in the current system. This should be much harder as there would not necessarily be any large databases, where the lucrative information is stored.

Our proposed system would also require the credit card to sign the transactions (as the card contains the necessary secret keys) and thus it could be difficult to apply it to online purchases at first, if for example special readers are required. As the capabilities of the credit cards increase in the future, the system could be used also online with a challenge-response type of protocol, where the responses are computed on the credit card with the help of user input. If these results can be easily communicated to the computer or other device on which the service is provided, this system could offer usability comparable with the current system. In any case, we think that there should be new security measures developed to tackle the credit card fraud problem. In a very extreme scenario, if no new measures can be found and adopted, credit cards may become outdated by the rapidly developing cryptocurrencies and other alternative online payment systems, even though these are not immune to fraud either.

References

1. Bellare, M., Pointcheval, D., Rogaway, P.: Authenticated key exchange secure against dictionary attacks. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 139–155. Springer, Heidelberg (2000)
2. Bond, M., Choudary, O., Murdoch, S.J., Skorobogatov, S., Anderson, R.: Chip and skim: cloning emv cards with the pre-play attack. IEEE Symposium on Security and Privacy (2014), http://www.cl.cam.ac.uk/~sjm217/papers/oakland14chipandskim.pdf
3. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. SIAM Journal on Computing 32(3), 586–615 (2003)
4. Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Transactions on Information Theory 22(6), 644–654 (1976)
5. Dutta, R., Barua, R., Sarkar, P.: Pairing-based cryptographic protocols: A survey. Cryptology ePrint Archive, Report 2004/064 (2004), http://eprint.iacr.org/
6. EMV co.: The EMV 4.3 standard specifications (November 2011), http://www.emvco.com/specifications.aspx?id=223
7. Fleischhacker, N., Manulis, M., Sadr-Azodi, A.: Modular design and analysis framework for multi-factor authentication and key exchange. Cryptology ePrint Archive, Report 2012/181 (2012), http://eprint.iacr.org/
8. Goldwasser, S., Micali, S., Rivest, R.L.: A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal on Computing 17(2), 281–308 (1988)

9. Hess, F.: Efficient identity based signature schemes based on pairings. In: Nyberg, K., Heys, H.M. (eds.) SAC 2002. LNCS, vol. 2595, pp. 310–324. Springer, Heidelberg (2003)
10. Jager, T., Kohlar, F., Schäge, S., Schwenk, J.: Generic compilers for authenticated key exchange. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 232–249. Springer, Heidelberg (2010)
11. Maji, H.K., Prabhakaran, M., Rosulek, M.: Attribute-based signatures. In: Kiayias, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 376–392. Springer, Heidelberg (2011)
12. Murdoch, S.J., Anderson, R.: Security protocols and evidence: Where many payment systems fail (2014), http://www.ifca.ai/fc14/papers/fc14_submission_124.pdf
13. Murdoch, S.J., Anderson, R.: Verified by visa and mastercard securecode: Or, how not to design authentication. In: Sion, R. (ed.) FC 2010. LNCS, vol. 6052, pp. 336–342. Springer, Heidelberg (2010), http://dx.doi.org/10.1007/978-3-642-14577-3_27
14. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008), https://bitcointalk.org/bitcoin.pdf
15. Okamoto, T., Takashima, K.: Decentralized attribute-based signatures. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013. LNCS, vol. 7778, pp. 125–142. Springer, Heidelberg (2013)
16. Panda Security: The cyber crime black market (2011), http://press.pandasecurity.com/wp-content/uploads/2011/01/The-Cyber-Crime-Black-Market.pdf
17. PCI Security Standards Council: Payment card industry data security standard v3.0 (2013), https://www.pcisecuritystandards.org/security_standards/documents.php
18. Schoenmakers, B.: A simple publicly verifiable secret sharing scheme and its application to electronic voting. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 148–164. Springer, Heidelberg (1999)
19. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakley, G., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985), http://dx.doi.org/10.1007/3-540-39568-7_5