ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

Analysis of Offline E-cash Schemes

Sattar J. Aboud
University of Bedfordshire, Department of Computer science and Technology, UK

Manuscript Info

Manuscript History:

Received: 15 June 2014
Final Accepted: 28 July 2014
Published Online: August 2014

Key words:
: Over-spending, e-cash scheme, bank attack, malicious insider.

Corresponding Author

Sattar J. Aboud

Abstract

If we construct e-cash scheme, the main motivation is to stop users' malicious insiders. Players such as banks might have vital and secret information of the users; the insiders in the un-trusted banks can become threats to e-cash schemes. Many authors in this regard study the security of the e-cash schemes but many of them insufficient. In this paper, we review the security of offline anonymous e-cash schemes and study the potential useful counter measures of anti-malicious actions.

Introduction

The investigation of e-cash schemes has one of the main difficulties in cryptography. Chaum introduced the online anonymous e-cash scheme [1] using blind signature. In this scheme, a bank wants to be included in the payment transactions so as to stop over-spending of e-cash. Actually, a bank wants payment transactions between the user and the merchant to be online. This can cause a restricted access to the bank system and it stops understanding e-cash scheme. Chaum et al. introduced the offline anonymous e-cash scheme [2] where a bank is not want to be included in the payment transaction between the user and the merchant. In this scheme, the user withdraws e-cash from a bank and passes it to the merchant without needing access to the bank system. When the user spends an e-cash once, the anonymity of a user is guaranteed. But, when a user over-spends an e-cash maliciously, the bank can obtain *Id* of the user from an over-spending e-cash.

In the Chaum et al, scheme *Id* of the user is embedded in e-cash and also preserved by the banks. Such vital *Id* wants to be secure in order to no malicious bank can use dishonestly. In many current e-cash schemes, the bank is supposed to be dependable, and the insider malicious by bank is not give concentration. But, some bank may become malicious, for instance, because of corruptions and an internal private information disclosure due to the weakness in bank system. So, it is essential to assess the security of e-cash schemes in terms of an insider malicious by un-trusted authority when e-cash schemes are deployed in the real world. For instance, Ferguson [3] stated that the framing attack by the malicious bank and to avoid such malicious, suggested signing the information replaced at a withdrawal protocol. However, appears in the scheme that a user and a bank want to remain information for the long time to prevent challenges [4, 5].

In this paper, we first describe the security of Chaum et al. offline anonymous e-cash scheme. Then we describe the insider malicious. Following the remarks on offline e-cash schemes, we will also analyze some of the e-cash schemes and state the countermeasures relied on the asymmetric methods.

2. Chaum et al. Offline Anonymous E-Cash

In this section, we describe the Chaum et al. scheme. The bank B chooses the public and private keys e_B, d_B. The signature created by using d_B. This can be considered to be e-cash similar to some amount of money w. In order to promise anonymity of users, the bank B creates this signature by using the blind signature. The user U and the merchant M each have account in the bank B. However, Chaum et al. scheme have the following protocols.

Withdrawal Protocol

1. The user U determines the message m_U by using its Id_U. The user U shows to the bank B that he created m_U properly without disclosing Id_U
2. The bank B generates the signature on m_U using blind signature and withdraws cash related to w from the bank account of the user U
3. The user U calculates $s_B(m_U)$ as the bank B 's signature on m_U

Payment Protocol

1. The user U posts $(m_U, s_B(m_U))$ to a merchant M
2. The merchant M checks the signature $s_B(m_U)$ and if $s_B(m_U)$ is true the merchant M posts the arbitrary challenge c_M to the user U
3. The user U calculates and passes the reply r_U the merchant M
4. The merchant M checks r_U and if true, then the merchant M exchanges goods and an e-cash with r_U

Deposit Protocol

1. The merchant M passes $(m_U, s_B(m_U), c_M, r_U)$ to the bank B
2. The bank B checks the bank signature $(m_U, s_B(m_U))$ and the pair of the challenge and reply (c_M, r_U). The bank B saves $(m_U, s_B(m_U), c_M, r_U)$ in the database for future finding of over-spending and credits w to the bank account of the merchant M.

Over-Spender

1. When the certain e-cash is over-spending, the bank B obtains Id_U of over-spending from the two record information (c_M, r_U) and $(c_M^{'}, r_U^{'})$.

3. Insider Malicious

In this section we are going to describe the insiders malicious which are as follows:

3.1 Impersonation

One of important attacks by malicious bank is impersonation. For example, in the scheme presented by Chaum et al. the user's private key is kept in the database of the bank and in this example, the user's Id is the private key. This means the malicious bank might be capable to steal a private key of uncorrupt user. Thus, the malicious bank can withdraw e-cash from the uncorrupt user's account by impersonating the user with that private key, so the malicious bank can over-spend the e-cash without permission from the user. When the private key is kept in a database of the bank, this insider malicious is not easy to stop.

3.2 Framing Attack

In the framing attack, the malicious bank forges information of over-spending.

In the Hanatani et al scheme [6] is used to recognize over-spending and the malicious bank can misuse signatures to forge the information of over-spending as follows.

1. Assume d is the private key of the user
2. Suppose f is an arbitrary value selected by a user in the withdrawal
3. Assume m is an arbitrary challenge selected by the merchant
4. When the user over-spending the e-cash, the bank finds d and f by using the formulas $r_1 = dm_1 + f$; $r_2 = dm_2 + f$ and recognizes over-spending with d
5. The malicious bank can create another signature $r_1 = dm_3 + f$ by using d and the new arbitrary challenge m_3. Then the malicious bank can forge the new information of over-spending by viewing the

signatures r_1, r_2, r_3 and this can be difficult since the first over-spending may be happen because of software fault.

In the Schoenmaker scheme [7], a bank knows d and even when a user is not committed an over-spending e-cash, a bank can forge the information of the uncorrupt user's the over-spending by conspiring with the merchant as follows.

1. The bank conspires with the merchant. If the merchant posts an e-cash to the bank for the deposit, the bank knows the user d that spent the e-cash. For example $r = dm + f$ is a signature in the e-cash.
2. The bank calculates the arbitrary value selected by the user f from r, d, m.
3. The bank calculates a forged signature $r' = dm' + f$ from forged arbitrary challenge m'.
4. The bank claims that the user over-spending an e-cash by computed the two signatures r, r'. However the malicious bank wants to conspire with the merchant to revoke the anonymity, the bank can make the framing attack even on the uncorrupt user.

In the Miyazaki and Sakurai scheme [8] the user uses the same signing key and public key certificate in each payment. In this case, a merchant can differentiate the users, thus it might be capable to connect Id of the user with the public key certificate. Thus, when a bank and a merchant conspire, the bank can know the purchase record of the user by verifying the public key of an e-cash in a deposit and anonymity of a user can be broken. This occurs since the same keys are used in each payment. In the scheme presented by Wang et al. [9], the anonymity of the user is supported by using multiple diverse keys in the payment.

3.3 Solutions versus Insider Malicious

One of the graceful solutions of insider malicious by banks was presented by Hanatani et al. They employed the blind multi-signature scheme relied on the Abe's scheme [10]. In the scheme presented by Hanatani et al. the e-cash wants to be signed by multiple banks specified by a user and also the e-cash wants to contain the signature by a user. Thus, an e-cash cannot be generated without the agreement from the user and this method stops malicious banks from framing a user by making the non-agreed e-cash and forging an over-spending. Furthermore in the scheme introduced by Hanatani et al. the public key of a user is known to anybody. But, the private key of a user is not disclosed even if an over-spending is noticed. It means that the identity public key of a user is obtained from an over-spent e-cash. So, the malignant banks cannot impersonate the user, and the ideal assumption for avoiding the insider malicious is understood. For instance, in the Brands' scheme, the user creates the public key and the private key where the public key is $e = a_1^d$ and the private key is d. The bank saved the user's public key e in the bank database. When the e-cash is over-spending, a bank can get, from an over-spending e-cash, the private key d of an over-spender rather than a public key e. Then the bank can mistreatment the user's private key for impersonation, and also can frame the user by making another fact of over-spending.

4. Remarks

In this section, we are going to provide some remarks which are as follows:

1. The user's private key is straight stored in a database of the bank as Id embedded in the withdrawn e-cash. The hacker can impersonate the user without difficulty when he gets Id of the user saved in a database. In such scheme, the user has another private key for signing information with the bank, which stops the bank framing attack.
2. The user's public key is saved in the database of the bank as the Id while the related private key is known only to the user. This type has no certificate on the user's public key. For example, in the Chun et al. scheme [11], the user's public key is entered as a user Id and it is embedded in the withdrawn e-cash by the bank. The hacker can impersonate the user when he can get the private key related to the public key saved in the database of the bank.
3. The user enters the public key as Id and makes payments by the key and by the certificate of the public key. For a hacker to impersonate the user, he wants to get the fake certificate also to getting a related private key from a public key. Committed an impersonation in such scheme is harder.
4. The private key contains two elements. One is known to both the bank and to the user whilst the other is calculated by the user. But, the related public key and its certificate are known only to the user. The user

Id kept in the bank. Thus, this incomplete data can improve the anti-impersonation by a malicious bank. This can be makes the bank attacks more hard.

5. In the scheme presented by Brands [12], the tamper-proof device was proposed to store *Id* of the user that is known only to the bank. The bank provides this tamper-proof device to the user. The user's private key contains (v_1, v_2) with v_1 kept in the tamper-proof device is known only to the bank and v_2 is known only to the user. In this case, a tamper-proof device is considered to be the type of the trusted authority.
6. In the schemes introduced by Yacobi [13], the certificate authority exists and it issues the certificate for the user's private key such that the private key d contains *Id* and the arbitrary value y it means $d = Id \,||\, y$. When the certificate authority is malicious, the certificate authority can impersonate the user *Id* by issuing the certificate for the private key $d' = Id \,||\, y'$ with *Id* is public data and y' can be selected by the malicious certificate authority.
7. Blazy et al. [14] studied offline transferability. This means that a receiver of the e-cash can transfer it to another entity without communication with any authority. In such scheme, the trusted authority is presented and can obtain the identity of an over-spender after the bank notices the over-spending. The user creates the pair of public and private keys and gets the certificate from a trusted authority.
8. Canard et al. [15] also discussed the efficient transferable e-cash. In their scheme the public key of the user wants to be known to the bank, and the user gets the certificate from the bank.
9. Canard et al. [16] described two types of anonymity, full anonymity and perfect anonymity in the transferable e-cash assumption. Full anonymity means that a hacker cannot identify the e-cash he studied throughout the payment protocol between uncorrupt users, and perfect anonymity means that the hacker cannot make a decision if he has hold an e-cash he received.
10. Canard et al. [17] follows the design of their preceding work. They considered the divisible e-cash scheme by which e-cash is divided into multiple classes in the payment protocol. In this scheme any public key certified by a bank can be satisfied a user to registered in the scheme.
11. Au et al. [18] considered anonymous user suspension by introducing the new suspension user. The suspended user cannot achieve new transactions and when the user turns out to be blameless later, the user can be unsuspended without breaking anonymity. In this scheme the public key of the user wants to be known to the bank.

5. Conclusion

In the offline e-cash schemes, the insider malicious from un-trusted bank are not paid any attention. Fan et al. [19] first indicated that the study of the insider malicious against offline e-cash schemes was inadequate. Careful consideration to the insider malicious must be taken for offline e-cash schemes. Other countermeasures anti-insider malicious like logging and audit should be treated with forensics methods. Hanatani et al. offered a graceful solution to withstand the insider malicious from the bank. Possible future work will contain adding properties to manage illegal attacks like blackmailing and money laundering [20]. Digital rights management can be considered to be one of possible uses of an e-cash [21] and over-spending finding of an e-cash will be practical for access control with privacy defense.

References

[1] Chaum D, "Blind Signatures for Untraceable Payments", Proceeding of Advances in Cryptology (CRYPTO'82), pp. 199–203, 1982.

[2] Chaum D, Fiat, A. and Naor, M., "Untraceable Electronic Cash", Proceeding of the 8th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'88), LNCS, Volume 403, Springer, pp. 319–327, 1988.

[3] Ferguson N, "Single Term Off-line Coins", Proceeding of Workshop on the Theory and Application of Cryptographic Techniques, LNCS, Volume 765, Springer, pp. 318–328, 1993.

[4] Nishide T and Sakurai K., "Security of Offline Anonymous Electronic Cash Systems against Insider Attacks by Un-trusted Authorities Revisited", Proceeding of the 3rd International Conference on Intelligent Networking and Collaborative Systems, IEEE, pp. 656–661, 2011.

[5] Baseri Y., Takhtaei B., and Mohajeri J., "Secure untraceable off-line electronic cash system", Scientia Iranica, Volume 20, pp. 637–646, 2012.

[6] Hanatani Y, Komano Y, Ohta K and Kunihiro N, "Provably Secure Untraceable Electronic Cash against Insider Attacks", IEICE Transactions, Volume 90-A, No. 5, pp. 980–991, 2007.

[7] Schoenmakers B, "An Efficient Electronic Payment System Withstanding Parallel Attacks", CWI, Technical Report CS-R9522, March 1995.
[8] Miyazaki S and Sakurai K., "A More Efficient Untraceable E-cash System with Partially Blind Signatures based on the Discrete Logarithm Problem", Proceeding of the 2nd International Conference on Financial Cryptography, LNCS, Volume 1465, Springer, pp. 296–308, 1998.
[9] Wang C., Sun H., Zhang H., and Jin Z., "An improved off-line electronic cash scheme", Proceedings of the 5th International Conference on Computational and Information Sciences (ICCIS '13), pp. 438–441, 2013.
[10] Abe M., "A Secure Three-move Blind Signature Scheme for Polynomials Many Signatures", Proceeding of International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT'01), LNCS, Volume 2045, Springer, pp. 136–151, 2001.
[11] Chun-I Fan, Wei-Zhe Sun, and Hoi-Tung Hau, "Date Attachable Offline Electronic Cash Scheme", The Scientific World Journal, Volume 2014, 2014.
[12] Brands S., "Off-line Electronic Cash based on Secret-key Certificates", Proceeding of Theoretical Informatics, Second Latin American Symposium (LATIN'95), LNCS, Volume 911, Springer, pp. 131–166, 1995.
[13] Yacobi Y., "Efficient Electronic Money", Proceeding of the 4th International Conference on the Theory and Applications of Cryptology, LNCS, Volume 917, Springer, pp. 153–163, 1994.
[14] Blazy O., Canard S., Fuchsbauer G., Gouget A., Sibert H., and Traor´e J., "Achieving Optimal Anonymity in Transferable E-cash with a Judge", Proceeding of the 4th International Conference on Cryptology in Africa, LNCS, Volume 6737, Springer, pp. 206–223, 2011.
[15] Canard S., Gouget A., and Traor´e J., "Improvement of Efficiency in Anonymous Transferable E-cash", Proceeding of the 12th International Conference on Financial Cryptography and Data Security (FC'08), LNCS, Volume 5143, Springer, pp. 202–214, 2008.
[16] Canard S and Gouget A., "Anonymity in Transferable E-cash", Proceeding of the 6th International Conference on Applied Cryptography and Network Security (ACNS'08), LNCS, Volume 5037, Springer, pp. 207–223, 2008.
[17] Canard S and Gouget A., "Multiple Denominations in E-cash with Compact Transaction Data", Proceeding Of the 14th International Conference on Financial Cryptography and Data Security (FC'10), LNCS, Volume 6052, Springer, pp. 82–97, 2010.
[18] Au M., Susilo W., and Mu Y., "Electronic Cash with Anonymous User Suspension", Proceeding of the 16th Australasian Conference on Information Security and Privacy (ACISP'11), LNCS, Volume 6812, Springer, pp. 172–188, 2011.
[19] Fan C., Huang V., and Yu Y., "User efficient recoverable off-line e-cash scheme with fast anonymity revoking," Mathematical and Computer Modeling, Volume 58, pp. 227–237, 2013.
[20] Grier J., "Detecting Data Theft Using Stochastic Forensics", Proceeding of the 11th Digital Forensic Research Workshop (DFRWS'11), Volume 8, Elsevier, pp. S71–S77, 2011.
[21] Perlman R., Kaufman C., and Perlner R., "Privacy-Preserving drm", Proceeding of the 9th Symposium on Identity and Trust on the Internet (IDtrust'10), ACM, pp. 69–83, 2010