A Survey On Authenticated Key And File Exchange Protocol For Secure Network Communication

Reshmi Vijayan

PG Student , Information & Technology

Govt .Engg College Barton Hill ,

Trivandrum , India.

reshmivijayan30594@gmail

Sreedivya R S

Assistant Professor,

Information & Technology

Govt .Engg College Barton Hill Trivandrum , India.

rssreedivya@gmail.com

**ABSTRACT**

Authenticated Key Exchange (AKE) protocol allows a user and a server to authenticate each other and generate a session key for the subsequent communications. However, most of them have one or more weaknesses, such as vulnerability against lost-smart-card attack, offline dictionary attack, de- synchronization attack, or lack of forward secrecy, user anonymity or untraceability. Furthermore, an AKE scheme under the public key infrastructure may not be suitable for lightweight computational devices, and the security model of AKE does not capture user anonymity and resist lost-smart-card attack. Understanding security failures of cryptographic protocols is the key to both patching existing protocols and designing future schemes. Then, we analyze an efficient dynamic ID-based scheme without public- key operations. This proposal attempts to overcome many of the well-known security and efficiency shortcomings of previous schemes and supports more functionalities than its counterparts. In this paper, we propose a novel dynamic ID-based Anonymous Two-Factor AKE

protocol which addresses all the above issues. The low computational and bandwidth cost indicates that our protocol can be deployed for pervasive computing applications and mobile communications in practice.

**1. INTRODUCTION**

With the rapid development of low-power and highly efficient networks, mobile users can pay bills, buy goods online, and carry out electronic transactions by subscribing to various remote services. Though mobile computing devices are highly portable, they are usually unprotected and easy to be stolen or get lost. Unless precautions are taken, an unauthorized person may gain access to the information stored on them. For instance, illegal access may be acquired by intruders if the data is "sniffed out of the air" in wireless communications or some malware is installed. The lack of authentication and privacy may cause even more severe results like crippled devices, personal data loss, disclosure of non-public data, or charge of abused usage against the device owner. Mobile computing devices are of great security concern not only because of

the data stored on them, but also for that they may provide access to other services that store or display non-public data. For almost all these transactions, mutual authentication and user privacy are required in the key exchange before remote servers start providing services to users. In particular, authentication and privacy play an important role in applications for industrial networks, wireless sensor networks , distributed networks, as well as RFID systems . Due to the advantages on portability and usability, most proposed authenticated key exchange (AKE) protocols support two factor authentication using passwords and smart cards ,especially with the evolution of contactless smart card towards the NFC (near-field communication) technology recently. There are two main attacks that a secure two-factor AKE protocol has to defend against: Lost-Smart-Card Attack and Offline Password Dictionary Attack.

Informally, user privacy refers to the anonymity and untraceability of a user’s identity as well as the corresponding smart card in the protocol executions. Anonymity aims to protect the location and activities of the user, while untraceability prevents an adversary from linking two sessions to the same user. Though traceability may not allow an adversary to identify a user directly, it may help the adversary to profile a user, for example, reveal the email server and the bank account of the user, or the online shopping mall that the user used to visit . Hence the main research problem on two- factor AKE nowadays is to construct a scheme that supports user anonymity and untraceability and preserves security against both lost-smart-card attack and offline dictionary attack. A dynamic ID-

based remote user authentication scheme using smart cards to remedy the weaknesses in the password-based authentication schemes. The scheme allowed users to choose and change their passwords freely and did not need to maintain any verifier table. They claimed that their scheme was secure against ID- theft, and could resist forgery attacks, replay attacks, insider attacks, guessing attacks and stolen verifier attacks.

**2.** **LITERATURE REVIEW**

In 2005, Fan et al. [1] proposed a two-factor authentication protocol that fails to achieve user anonymity and session key establishment. As it is based on Rabin’s public key cryptosystem, Fan et al.’s scheme is less efficient when compared with recent results based on elliptic curve cryptosystems.

In 2004 Das et al.[2] proposed a dynamic ID-based password authentication scheme. Password-based authentication schemes are the most widely used techniques for remote userauthentication. Many static ID-based remote user authentication schemes both with and without smart cards have been proposed. Most of the schemes do not allow the users to choose and change their passwords, and maintain a verifier table to verify the validity of the user login. In this paper present a dynamic ID-based remote user authentication scheme using smart cards. The scheme allows the users to choose and change their passwords freely, and do not maintain any verifier table. The scheme is secure against ID-theft, and can resist the reply attacks, forgery attacks, guessing attacks, insider attacks and stolen verifier attacks.

In 2013 Wang et al.[3] showed that many recently proposed dynamic ID-based Anonymous Two-factor AKE protocols have one or more weaknesses, such as vulnerability against lost-smart-card attack, offline dictionary attack, or lack of forward secrecy, anonymity and untraceability . It is worth noting that, in order to provide user anonymity, almost all dynamic ID-based two-factor authentication protocols need an additional synchronization mechanism to maintain the consistency of the one-time identity between the user and the server. However, this consistency is broken easily, and the user may no longer be able to login the server.

In 2015, 2016 Chaudhry et al. proposed two schemes [4],[5] that are claimed to achieve anonymity and many other desirable properties, but both of them don’t support smart card revocation, and the second scheme [5] does not provide password change mechanism. Besides, we found that the first scheme [4] failed to achieve forward secrecy even though it claimed so, because its previous session keys can be recovered if the adversary gets access to the user’s password, smart card and protocol transcripts of previous sessions. There are also some other schemes based on biometric techniques or adjusted for the setting of multiple servers [6], [7], which is of independent interest but out of the scope of this paper. Furthermore, the schemes under public key infrastructure may not be suitable for lightweight computation devices. Therefore, it is still an open problem to design a secure and efficient Anonymous Two-Factor AKE scheme without using public keys.

**3. FUNCTIONALITY AND PERFORMANCE COMPARISONS**

**3.1 Functionality Comparison**

In comparison of functionalities, we focus on the security against offline dictionary attack, anonymity and untraceability, mutual authentication and key exchange, forward secrecy, support of password change, and dependence on the public key infrastructure.

**3.2 Performance Comparison**

In the Login and Authentication phase of our scheme, it requires three elliptic curve scalar multiplications to compute(e; c), where e can be pre-computed; and six hash operations.. It requires three elliptic curve scalar multiplications to compute (d; c), where d can be precomputed; two block encryptions and five hash operations for getting and verifying in the server.

|  |  |  |  |
| --- | --- | --- | --- |
|  | Anonymity  enhanceme nt on Robust and efficient password- authenticate d key agreement scheme using smart cards | Preserving  privacy for free  Efficient and  provably secure two- factor authenticatio n scheme with user anonymity. | Provably  Secure Dynamic ID-based  Anonymous Two-factor Authenticate d Key Exchange Protocol  with Extended Security Model |
| No  password table | **Y** | **Y** | **Y** |
| No server’s  public key | **N** | **N** | **Y** |

**REFERENCES**

[1] C. Fan, Y. Chan, and Z. Zhang, "Robust remote authentication scheme with smart cards," Comput. Secur., vol. 24, no. 8, pp. 619- 628,

|  |  |  |  |
| --- | --- | --- | --- |
| Mutual  authenticatio n and Key agreement | **Y** | **Y** | **Y** |
| Forward  secrecy | **N** | **N** | **Y** |
| Anonymity  or untraceabilit y | **Y** | **Y** | **Y** |
| Password  change | **Y** | **N** | **Y** |

Nov. 2005..

**CONCLUSION**

The proposed an anonymous two-factor AKE scheme which preserves security against various attacks including de- synchronization attack and password guessing attack, and supports several desirable properties including perfect forward secrecy, anonymity or untraceability, adaptively password change, no centralized password storage, and no long-term public key. Furthermore, our protocol maintain high efficiency in terms of storage requirement, communication cost as well as computational complexity. The protocol requires only a few number of message flows and all the transmitted messages are short in size. Additional, the proposed scheme is provably secure in our extended security model of AKE. Therefore, the proposed scheme is suitable for deployment in various low-power networks, in particular, the pervasive and mobile computing networks. The enhanced scheme also ensures privacy and anonymity. Although the scheme incurs some extra memory, communication, and computation cost because of storage and communication of user’s pseudo-identity, yet it is only because of this additional burden that the proposed scheme is able to resist user anonymity violation attack and smart card stolen attack.

[2] M. L. Das, A. Saxena, and V. P.

Gulati, "A dynamic ID-based remote user authentication scheme," IEEE Trans. Consum. Electron., Vol. 50, no. 2, pp.629-631, 2004.

[3] S. Chaudhry, M. S. Farash, H. Naqvi, S. Kumari, and M. K. Khan, "An enhanced privacy preserving remote user authentication scheme with provable security", Security Comm. Networks, 8:3782-3795, 2015.

[4] S. Chaudhry, H. Naqvi, K. Mahmood, H. F. Ahmad, and M. K. Khan, "An Improved Remote User Authentication Scheme Using Elliptic Curve Cryptography", Wireless Pers. Commun., DOI

10.1007/s11277-016-3745-3, 2016.

[5] S. Chaudhry, "A secure biometric based multi-server authentication scheme for social multimedia networks", Multimed Tools Appl.,

75:12705-12725, 2016.

[6] A. Irshad, M. Sher, O. Nawaz, S.

Chaudhry, I. Khan, and S. Kumari, "A secure and provable multi-server authenticated key agreement for TMIS based on Amin et al. scheme", Multimed Tools Appl., DOI 10.1007/s11042-016-3921-1,

2016.

[7] F. Wen, and X. Li, "An improved dynamic ID-based remote user authentication with key agreement scheme," Computers and Electrical Engineering, 38(2):381-387, 2012

[8] W. Juang, S. Chen, and H. Liaw, "Robust and efficient password authenticated key agreement using smart cards," IEEE Trans. Ind. Electron., vol. 15, no. 6, pp. 2551-

2556, Jun. 2008

[9] G. Yang, D. S. Wong, H. Wang and X. Deng, "Two-factor mutual authentication based on smart cards and passwords," Journal of Computer and System Sciences,

74(7): 1160-1172, 2008

[10] M. Khan, S. Kim, and K.

Alghathbar, "Cryptanalysis and security enhancement of a more efficient and secure dynamic ID- based remote user authentication scheme. Computer Communications, 34:305-309, 2011.