Authenticated Key And File Exchange Protocol For Secure Network Communication

**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. With the rapid development of low-power and highly efficient networks like pervasive and mobile computing network in recent years, many efficient AKE protocols have been proposed to achieve user privacy and authentication in the communications. Besides secure session key establishment, those AKE protocols offer some other useful functionalities like two-factor user authentication and mutual authentication. 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. In this paper, propose a novel dynamic ID-based Anonymous Two-Factor AKE protocol which addresses all the above issues. The proposed scheme is provably secure in extended security model .The low computational and bandwidth cost indicates that our protocol can be deployed for pervasive computing applications and mobile communications in practice. In the proposed system file transfer are added and give more security to when transferring the file and authentication protocol are used in the proposed system . SQL database are used as the back end and front end as csharp.net .The proposed sytem give more importants to the file transfer and security to the network.

**Chapter 2**

**2.1 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 . Detectable online dictionary attack is applicable to all of the password-based protocols. It can be prevented because a failed online password guess will be detected by the server and the server can limit the number of the password re-entered. Undetectable online dictionary attack . and offline dictionary attack are great threats to the password AKE protocols. There are a number of password based AKE protocols in the literature, which fail to resist the offline dictionary attack . Actually, in practice, a human-memorable password combined with a smart card are often used in authentication and key exchange protocols to achieve secure trade and secure communication. It is called two-factor authentication mechanism . A smart card is a credit card-sized plastic card with a microprocessor chip embedded in the card. It can act as a memory storage device and a processor device. Clients can save some complex but confidential data in their smart cards. In two-factor mechanism, when authenticating, each client needs to provide the password and the smart card. Meanwhile, it is only learning both of the password and the smart card that an adversary is able to impersonate a legal client. Two-factor authentication offers more security than password only authentication, which makes it a perfect solution for e-commerce transactions and other Internet connection activities.

**Chapter 3**

**3.1 Literature Survey**

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.

In 2012 Xiaowei Li et al. proposed two-factor authenticated key exchange (AKE) protocols have been widely used in various networks to ensure communication security. In 2009, Sun et al. proposed an improved password authenticated key agreement scheme based on smart cards. It is efficient in two-factor authentication key exchange protocols. the scheme of Sun et al. was vulnerable to a password-guessing attack and a key compromise impersonation (KCI) attack. An improvement on the scheme of Sun et al. by using an elegant but simple trick to eliminate the security vulnerabilities. The improved scheme possesses untraceability, which is absent in the scheme of Sun et al. but important in anonymous communication. Moreover, the new scheme can also resist KCI attack, which is a strong secure property in AKE protocol. Proved the security of our protocol in the random oracle model provided that the Elliptic Curve Gap Diffie–Hellman assumption holds. The trick used in this paper can provide a new way for designing authenticated key agreement in two-factor authentication mechanism.

**Chapter 4**

**4.1 Existing System**

**4.1.1 Problem Definition**

The main problem in the existing system are only short messages are send at a time and there was no huge database to store the information . It was not possible to send the big file transfer .when OTP was produce while sending the message from sender to the receiver but it doesnot have well security while sending the message . From which IP address this message send it cannot recoginze after particular time it automatically logout so that while sending itself it may cause the time delay . In Dictionary attack there are 2 types. In First attack , the adversary launches password guessing attack against some short, non-uniformly distributed passwords. In second dictionary attack can usually be prevented in practice by resetting the user’s account .when the number of consecutive failed authentication attempts reached a threshold, while offline dictionary attack cannot be detected.

**4.1.2 Problem Solution**

The problem solution for the existing system are :

* Security against various attacks including desynchronization attack, and offline dictionary attack.
* Propose a dynamic ID based ananymous two – factor AKE protocol.
* Support user anonymity and untraceability.
* Perfect forward secrecy.
* No long-term public key.
* No centralized password storage.
* Support user password change.
* Provable security in extended security model.

**Chapter 5**

**System Design**