International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 7 | ISSN : 2456-3307

Security Based Multi Factor Key Exchange Protocol for Data Communication

D. Nithya Devi[1*], P. Panimalar[2]
[1]Research Scholar, Department of Computer Science, A.V.C College, Mayiladuthurai, India
[2]Associate Professor, Department of Computer Science, A.V.C College, Mayiladuthurai, India

ABSTRACT

Authenticated Key Exchange (AKE) protocol permits a user and a server to authenticate each other for the first time. It generates a session key for the successive communications without any authentication. Many AKE protocols had been proposed to obtain person privateness and authentication for the duration of conversation. Other than secured consultation key established order, these AKE protocols offer a few other useful capability like two-thing user authentication and mutual authentication. But they have got few weaknesses along with vulnerability. Loss of smart card, offline dictionary assault, de-synchronization attack, person anonymity or untraceability. Also, AKE scheme the usage of symmetric key conversation doesn't suite nicely for light weight computational gadgets. In this thesis, a novel Multi Factor AKE protocol is proposed to overcome all the above mentioned weaknesses. This protocol supports revoked smart card transactions. The password that is available on the USB device will be overwritten once the user used it. Passwords can be updated without centralized storage. The average time to enter a password will be defined. The user has to type the password within the allocated time, failing which he / she have to enter it again. This security model of AKE supports user anonymity and resist lost card attack. Elliptical Curve Cryptography algorithm is used for encryption and decryption of the session key. The computational cost and the bandwidth cost for this proposed model are low, which makes it to use in pervasive computing applications and mobile communications. The proposed method is implemented in a bank application. The proposed AKE model is much secured when compared to the existing protocols.

Keywords : AKE, ECC, Offline attacks.

I. INTRODUCTION

NETWORK SECURITY BASICS

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

NETWORK SECURITY

Network security starts with authenticating, commonly with a username and a password. Since this requires just one detail authenticating the user name—i.e., the password—this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g., a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' is also used (e.g., a fingerprint or retinal scan).

Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) helps detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network like wire shark traffic and may be logged for audit purposes and for later high-level analysis. Newer systems combining unsupervised machine learning with full network traffic analysis can detect active network attackers from malicious insiders or targeted external attackers that have compromised a user machine or account. Communication between two hosts using a network may be encrypted to maintain privacy.

Honeypots, essentially decoy network-accessible resources, may be deployed in a network as surveillance and early-warning tools, as the honeypots are not normally accessed for legitimate purposes. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques. Such analysis may be used to further tighten security of the actual network being protected by the honeypot. A honeypot can also direct an attacker's attention away from legitimate servers. A honeypot encourages attackers to spend their time and energy on the decoy server while distracting their attention from the data on the real server. Similar to a honeypot, a honeynet is a network set up with intentional vulnerabilities. Its purpose is also to invite attacks so that the attacker's methods can be studied and that information can be used to increase network security. A honeynet typically contains one or more honeypots.

SECURITY MANAGEMENTS

Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

TYPES OF ATTACKS

Networks are subject to attacks from malicious sources. Attacks can be from two categories: "Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation or to conduct reconnaissance and lateral movement to find and gain access to assets available via the network.

TYPES OF NETWORK SECURITY

Access control

Not every user should have access to your network. To keep out potential attackers, you need to recognize each user and each device. Then you can enforce your security policies. You can block noncompliant endpoint devices or give them only limited access. This process is network access control (NAC).

Antivirus and antimalware software

"Malware," short for "malicious software," includes viruses, worms, Trojans, ransomware, and spyware. Sometimes malware will infect a network but lie dormant for days or even weeks. The best antimalware programs not only scan for malware upon entry, but also continuously track files afterward to find anomalies, remove malware, and fix damage.

Application security

Any software you use to run your business needs to be protected, whether your IT staff builds it or whether you buy it. Unfortunately, any application may contain holes, or vulnerabilities, those attackers can use to infiltrate your network. Application security encompasses the hardware, software, and processes you use to close those holes.

Behavioral analytics

To detect abnormal network behavior, you must know what normal behavior looks like. Behavioral analytics tools automatically discern activities that deviate from the norm. Your security team can then better identify indicators of compromise that pose a potential problem and quickly remediate threats.

Email Security

Email gateways are the number one threat vector for a security breach. Attackers use personal information and social engineering tactics to build sophisticated phishing campaigns to deceive recipients and send them to sites serving up malware. An email security application blocks incoming attacks and controls outbound messages to prevent the loss of sensitive data.

Firewalls

Firewalls put up a barrier between your trusted internal network and untrusted outside networks, such as the Internet. They use a set of defined rules to allow or block traffic. A firewall can be hardware, software, or both. Cisco offers unified threat management (UTM) devices and threat-focused next-generation firewalls.

Intrusion prevention systems

An intrusion prevention system (IPS) scans network traffic to actively block attacks. Cisco Next-Generation IPS (NGIPS) appliances do this by correlating huge amounts of global threat intelligence to not only block malicious activity but also track the progression of suspect files and malware across the network to prevent the spread of outbreaks and reinjection.

Mobile device security

Cybercriminals are increasingly targeting mobile devices and apps. Within the next 3 years, 90 percent of IT organizations may support corporate applications on personal mobile devices. Of course, you need to control which devices can access your network.

Network segmentation

Software-defined segmentation puts network traffic into different classifications and makes enforcing security policies easier. Ideally, the classifications are based on endpoint identity, not mere IP addresses. You can assign access rights based on role, location, and more so that the right level of access is given to the right people and suspicious devices are contained and remediated.

Security information and event management

SIEM products pull together the information that your security staff needs to identify and respond to threats. These products come in various forms, including physical and virtual appliances and server software.

Web security

A web security solution will control your staff's web use, block web-based threats, and deny access to malicious websites. It will protect your web gateway on site or in the cloud. "Web security" also refers to the steps you take to protect your own website.

Wireless security

Wireless networks are not as secure as wired ones. Without stringent security measures, installing a wireless LAN can be like putting Ethernet ports everywhere, including the parking lot. To prevent an exploit from taking hold, you need products specifically designed to protect a wireless network.

II. RELATED WORK

Bin Wang et al. [1] proposes a new protocol with two original approaches, which are the label sharing approach to protect customer and the removable central database approach to enhance system mobility is proposed in this paper. The security properties of the new scheme are verified by using Colored Petri Net (CPN) and algebra proofs. The significance of radio frequency identification (RFID) security is increasing explosively, leading to a research trend. The current most severe RFID security issues are privacy and authentication security. The renewable identity (ID) approach with a central database is the current dominating approach to achieve user privacy and authentication security. Although, the approach will cause more problems that renewable ID will increase RFID tag cost and will enable denial of service (DoS) attacks while the central database will reduce system mobility. To solve the dilemma, this paper is presented.

Chin-Chen Chang et al. [2] proposed a secure single sign-on mechanism that is efficient, secure, and suitable for mobile devices in distributed computer networks. User identification is an important access control mechanism for client–server networking architectures. The concept of single sign-on can allow legal users to use the unitary token to access different service providers in distributed computer networks. Recently, some user identification schemes have been proposed for distributed computer networks. Unfortunately, most existing schemes cannot preserve user anonymity when possible attacks occur. Also, the additional time-synchronized mechanisms they use may cause extensive overhead costs. To overcome these drawbacks, this paper is designed.

Chin-Chen Chang et al. [3] analyzes Yeh et al.'s security flaws and then proposes a protocol that overcomes all the weaknesses of the aforementioned protocol. Authentication and key agreement protocols are foundation for the security of distributed applications. In 2010, Yeh et al. proposed two authenticated key agreement protocols. The second protocol in Yeh et al. features user's anonymity. However, we found that the second scheme is vulnerable to replay attack, masquerade attack, and off-line password attack.

Guomin Yang et al. [4] scrutinizes the security requirements of this kind of schemes, and propose a new scheme and a generic construction framework for smart-card-based password authentication. We show that a secure password based key exchange protocol can be efficiently transformed to a smartcard based password authentication scheme provided that there exist pseudorandom functions and target collision resistant hash functions. Our construction appears to be the first one with provable security. In addition, we show that two recently proposed schemes of this kind are insecure. One of the most commonly used two-factor user authentication mechanisms nowadays is based on smart-card and password. A scheme of this type is called a smart-card-based password authentication scheme. The core feature of such a scheme is to enforce two factor authentications in the sense that the client must have the smart-card and know the password in order to gain access to the server.

Jongho Moon, et al.[5] proposed a new authentication and key agreement scheme using smart card. In addition, we demonstrate that proposed authentication scheme has strong resistance to the various attacks. Finally, we compare the performance and functionality of the proposed scheme with other related schemes.

Jue-Sam Chou et al. [6] designed an efficient RFID scheme based on Elliptic Curve Cryptography (ECC) to avoid these problems. After analyses, we conclude that our scheme not only can resist various kinds of attacks but also outperforms the other ECC based RFID schemes in security requirements, with needing only little extra elliptic curve point multiplications. Recently, Radio Frequency Identification (RFID) technique has been widely deployed in many applications, such as medical drugs management in hospitals and missing children searching in amusement parks. The applications basically can be classified into two types: non-public key cryptosystem (PKC)-based and PKC-based. However, many of them have been found to be flawed in the aspect of privacy problem. Therefore, many researchers tried to resolve this problem. They mainly investigated on how low-cost RFID tags can be used in large-scale systems. However, after analyses, we found those studies have some problems, such as suffering physical attack or de-synch attack. To rectify these problems, this work is done.

Min-Skiang Hwang, et al. [7] proposed a new remote user authentication scheme using smart cards. This scheme is based on the ElGamal's public key cryptosystem. This scheme does not maintain a password table for verifying the legitimacy of the login users. This scheme can withstand message replaying attack.

Vanga Odelu et al. [8] present a more secure and robust remote user authenticated key agreement scheme in order to remedy the security flaws found in Islam's scheme. Through the formal security analysis using the widely-accepted Burrows– Abadi–Needham logic (BAN logic), we show that our scheme provides secure mutual authentication. Furthermore, the formal and informal security analysis show that our scheme is secure against various known attacks including the offline password guessing attack when smart card of a user is lost/stolen, and our scheme also provides SK-security, user anonymity and avoids the time-synchronization problem. We further simulate our scheme for the formal security verification using the widely-accepted and widely-used Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. The simulation results clearly indicate that the proposed scheme is safe. Thus, our scheme provides high security along with more functionality features as compared to Li et al.'s scheme and Islam's scheme. As a result, our scheme is very suitable for practical applications.

Virlla Devi Soothar et al. [9] focuses on improving the security of RFID systems in IoT. RFID technology is an automatic data capturing technology which uses radio frequency to identify objects. Previously its application range was limited to management systems to identify the product, object or person and some payment systems. However, with the emergence of the smart world and IoT, the application areas of RFID technology have been spread widely. Now it is considered as one of the strong candidates for automating environment. With the increase in the use of RFID technology, reliability and security of the communication have become one of hot research topics. There have been many authentication protocols proposed for the secure communication in RFID systems. However, most of the approaches were presented when RFID tags were purely used in supply chain management as replacement of the barcode. So, these protocols assume that the communication medium between the server and reader is always secure. In IoT-based RFID systems such assumption is not always valid.

Yu-Jung Huang et al. [10] studies the radio-frequency identification (RFID) tag–reader mutual authentication (TRMA) scheme. Two improved authentication protocols for generating the PadGen function are described. A hardware design of these RFID authentication protocols conforming to the International Standards Organization 18000-6 Type-C protocol, also known as EPC C1G2 RFID protocol, is proposed. Since tags have an extremely limited computing power and storage capacity, the PadGen function based on exclusive-OR operation for low-cost hardware implementation is reported in this study. The proposed RFID TRMA protocol was simulated using Modelsim XE II and synthesized using Altera's Quartus II software. The functionality of these strengthening protocols was successfully verified in hardware using an Altera DE2 board that included an Altera Cyclone II field-programmable gate array.

III. PROPOSED SYSTEM

A novel Multi Factor AKE protocol is proposed to overcome all the weaknesses in the existing system. This protocol supports revoked smart card transactions. The password that is available on the USB device will be overwritten once the user used it. Passwords can be updated without centralized storage. The average time to enter a password will be defined. The user has to type the password within the allocated time, failing which he / she have to enter it again. This security model of AKE supports user anonymity and resist lost card attack. Elliptical Curve Cryptography algorithm is used for encryption and decryption of the session key. The computational cost and the bandwidth cost for this proposed model are low, which makes it to use in pervasive computing applications and mobile communications. The proposed AKE model is much secured when compared to the existing protocols.

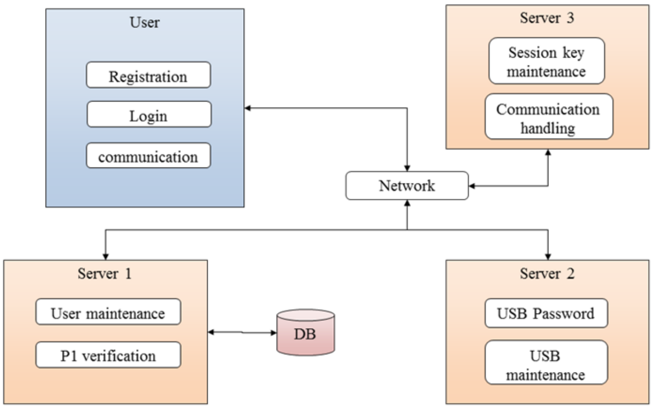

Fig 1 : System Architecture

ECC algorithm is used in the proposed dissertation while generating session key. This session key will be valid only once. If the session key is used for a single time, it will be expired. The session key for the next transaction will be mailed to the user separately. The transaction amount along with the public key generates the cipher text. This text will be sent to the receiver. The receiver has to decrypt the cipher text using the private key which is available with him. ECC is a kind of asymmetric cryptography algorithm. This method is a kind of public key encryption technique. In this type of technique, there will be two keys viz., public key and the private key. Public key along with the user data will produce the encrypted data. This data along with the encrypted data will be sent to the receiver. The user has to decrypt the data using the private key which is available with him.

IV. RESULT AND DISCUSSION

The proposed paper is deployed using C# .NET. This forms the front end. SQL SERVER acts the back end. Visual Studio is the IDE. Windows 7 is the implemented OS. The user has to create account with the required fields. While typing password, key stroke dynamics is implemented. The password should be typed for four times. Keystroke dynamics values will be stored. Proposed algorithm finds the difference between actual keystroke value stored in database and current value of login user. Here, threshold value is assumed to compare with time. These threshold values increase the efficiency of result. This value is compared to the current time of login user if the value will be matched according to the threshold value the person is accepted or called as an authenticated user. While registering, USB password is stored. While login, first the user credentials should be entered. If the user credentials matches, USB password should be entered. Once the password is entered, it gets expired and the updated password will be mailed to the user. After successful login, while transferring amount, session key will be generated. ECC algorithm is used to generate the session key. The public key along with the transferring amount will produce the cipher text. This will be decrypted by the receiver by using the private key which is available with him.

V. CONCLUSION

Multi-Factor AKE model provides security against various attacks including de-synchronization attack, lost-smart-card attack, user anonymity and untraceability. The proposed system maintains high efficiency in terms of storage requirement. Communication cost and computational complexity is less when compared to existing system. This system is suitable for deployment in the pervasive and mobile computing networks. In future, planned to improve the time complexity when compared to other authentication models. Replacing smart card by other small devices such as micro secure digital cards can be implemented. Other methods like biometrics, face detection and iris can be used for authentication.

VI. REFERENCES

[1]. B. Wang and M. Ma, "A server independent authentication scheme for RFID systems," IEEE Trans. Ind. Inf., vol. 8, no. 3, pp. 689-696,Aug. 2012.

[2]. C. Chang and C. Lee, "A secure single sign-on mechanism for distributed computer networks," IEEE Trans. Ind. Electron., vol. 59, no. 1, pp. 629-637, Jan. 2012.

[3]. C. Chang, H. Le, C. Lee, and C. Chang, "A robust and efficient smart card oriented remote user authentication protocol," Intelligent Information Hiding and Multimedia Signal Processing(IIHMSP), 2011 Seventh International Conference on, pp.252 - 255, 2011.

[4]. 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.

[5]. Jongho Moon, Donghoon Lee, Jaewook Jung and Dongho Won, “Improvement of Efficient and Secure Smart Card Based Password Authentication Scheme", International Journal of Network Security, Vol.19, No.6, PP.1053-1061, Nov. 2017.

[6]. Jue-Sam Chou, Yalin Chen, Cheng-Lun Wu, Chi-Fong Linv, “An efficient RFID mutual authentication scheme based on ECC", IACR Cryptology, 2011.

[7]. M. Hwang, and L. Li,"A new remote user authentication scheme using smart cards," IEEE Trans. Consum. Electron., 2000, 46(1):28-30.

[8]. Vanga Odelu, Ashok Kumar Das and Adrijit Goswami,“An Effective and Robust Secure Remote User Authenticated Key greement Scheme Using Smart Cards in Wireless

Communication Systems" , Wireless Personal Communications, October 2015, Volume 84, Issue 4, pp 2571-2598.

[9]. Virlla Devi Soothar, " Three Party Authentication Scheme For Rfid Systems In IOT" July 2017.

[10]. Y. Huang, W. Lin, and H. Li,(2012) "Efficient Implementation of RFID Mutual Authentication Protocol," IEEE Trans. Ind. Electron., vol. 59, no. 12, pp. 4784 - 4791, 2012.