Middle-East Journal of Scientific Research 24 (Techniques and Algorithms in Emerging Technologies): 215-219, 2016
ISSN 1990-9233;

DOI: 10.5829/idosi.mejsr.2016.24.TAET23430

Random Key Updation for Certificateless Remote Authentication Protocol with Anonimity in Wban Domain: Network Security

Haobijam Jina Devi and E. Menaka

Department of Computer Science and Engineering,
Vivekananda Institute of Engineering and Technology for Women, India

Abstract: In WBAN, it is very important to secure the extra-body communication between the smart portable device held by the WBAN client and the application providers (the hospital, physician or medical staff) so that the security and privacy of the patient's health status in the wireless body area networks (WBANs) is secure. Based on Certificateless cryptography, this paper proposes a remote authentication protocol featured with non repudiation, client anonymity, key escrow resistance and revocability for extra-body communication in the WBANs. Here, Certificateless encryption scheme and a Certificateless signature scheme with efficient revocation against short-term key exposure, which are of independent interest is used. Thereby, a Certificateless anonymous remote authentication with revocation is introduced.

Key words: Anonymity · Remote authentication · Revocation · Certificateless cryptography · Wireless body area network

INTRODUCTION

Network Security: Network security [1] has become very essential to personal computer users, organizations and the military. The advent of the internet has made security a major concern and the history of security allows a better understanding of the emergence of security technology. Many security threats are allowed internet structure itself all. The appropriate security emerge after knowing the attack methods. Network security includes certain policies to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves mainly the authorization of access to data in a network, which isusually controlled by the network administrator.

An ID and a password or other authenticating information is assigned to Users which allows them to access an information and programs within their authority. A variety of computer networks like private and public is covered by Network security that are used in everyday jobs such as conducting transactions and communications among businesses, government agencies and individuals. 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.

The activities are used to protect the usability, reliability, integrity and safety of your network and data. Effective network security targets a variety of threats and stops them from entering or spreading on your network.

Threats of Network Security: There are various threats of network security, some of are as follows:-

- Viruses, worms and Trojan horses
- Spyware and adware
- Zero-day attacks, also called zero-hour attacks
- Hacker attacks
- Denial of service attacks
- Data interception and theft
- Identity theft

Common Types of Network Attacks: Some of the common types of network attacks are as follows:-

- Eavesdropping
- Data Modification
- Identity Spoofing (IP Address Spoofing)

Corresponding Author: Haobijam Jina Devi, Department of Computer Science and Engineering, Vivekananda Institute of Engineering and Technology for Women, India.

- Password-Based Attacks
- Denial-of-Service Attack
- Man-in-the-Middle Attack
- Sniffer Attack

Security Services: A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms. Network Security Services (NSS) consists of a set of libraries which supports cross-platform development of security-enabled client and server applications with optional support for hardware TLS/SSL acceleration on the server side and hardware smart cards on the client side. A complete open-source implementation is provided by NSS for cryptographic libraries that support the Transport Layer Security (TLS) / Secure Sockets Layer (SSL).

Security Mechanism: The process to implement the security properties is known as security mechanism. The various type of mechanism on the basis of properties is as follows

- Attack Prevention
- Attack Avoidance
- Attack Detection
- Attack Prevention:

Attack Prevention can be defined as a series of security mechanism implemented to prevent or defend against various types of attack before they can actually reach and affect the target systems. An important mechanism is access control which is defined as the process of limiting the access to the resources of the Information System.

Attack Avoidance: The expansion of connectivity of computers makes the need of protecting the message and message from tampering reading important. This is the technique in which the information is modified in a way that makes is unusable for the attacker.

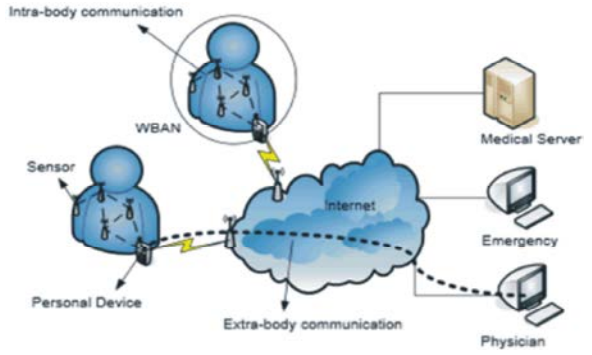
Attack Detection: In this mechanism it is assumed that the attacker is able to bypass the installed security measures to access the desired target/information. When such incidents happens attack detection takes the responsibility to report someone that something went wrong somewhere in the system.

Wireless Body Area Network: A Wireless Body Area Network (WBAN) [2] connects independent nodes (e.g. sensors and actuators) which could be situated in the clothes, on the body or under a person's skin. The network is expanded over the whole human body and the nodes are connected through a wireless communication channel. Because of the increasing use of wireless networks and the miniaturization of electrical devices(such as sensors) has empowered the development of Wireless Body Area Networks (WBANs). In these networks various sensors are attached on clothing or on the body or even implanted under the skin. Numerous new, practical and innovative applications are offered by the wireless nature of the network and the wide variety of sensor thereby helping to improve health care and the Quality of Life. The sensors of a WBAN measure certain parameters of the humanbody such as the heartbeat, the body temperature or record a prolonged electrocardiogram. By using a WBAN [3], the patient could experiences a greater physical mobility and is no longer compelled to stay in the hospital.

The rapid development in intelligent physiological sensors and wireless communication technology has the help to improve the quality of life significantly by allowing chronically ill, children and elderly to be monitored and treated continuously and remotely. With the tiny medical sensor nodes implanted inside or worn on human body and the smart portable device (SPD) held by the patient, a self-organized wireless body area network (WBANs) can be formed to monitor the health status and the surrounding environments of human bodies. In WBAN, there are two basic modes of communication which are Intra-body communications and extra-body communications and respectively they allow sensors to communicate with each other and the SPD and enable SPD to communicate with the remote application providers (APs) such as the hospital, physician or medical staff.

Three Types of Entities

WBAN Client: First, the WBAN clients should be registered with KGC and preloaded with the public parameters before accessing the wide range of services offered by the APs. A WBAN client must be revoked from the system in case KGC detects the misbehavior of users or this user declares that his/her Private Key is compromised for security purpose.



AP: Likewise, the APs, such as hospitals, clinics, medical institutions or even weather forecast centers, should also be registered with KGC and preloaded with public parameters before they provide pervasive healthcare monitoring and treatment remotely to WBAN clients. The revocation of the APs is necessary as well in case the APs violate the system rules.

KGC: KGC [4] is responsible of the enrollment and eviction of WBAN clients and APs.The KGC cannot be fully trusted since it is usually acted by a commercial Organization. By considering the commercial benefits, it is natural for the KGC to misbehave such as illegally collecting clients' sensitive health information or accessing the services provided by APs free of charge. Therefore, the key escrow problem, where the KGC impersonates the clients or APs without being observed, should be avoided in our protocol.

Modules:

- Remote authentication
- KGC Service
- Certificateless cryptography
- Anonymity detection
- Authentication access
- Random key generation - [Future Proposed Module]

Remote Authentication: It is a basic registration model with client and doctor. Remote authentication protocol, was initially introduced by Lamport, which enables a (roaming) mobile client to authenticate to a remote server over a public channel and then a shared session key will be generated to secure [5] their later communications. From the time since the seminar work of Lamport, a number of remote authentication protocols have been suggested. In the public key infrastructure (PKI)-based remote authentication protocols, each party (e.g. a client or a remote server) is initially preloaded with a private/public key pair and a corresponding public key certificate issued by a semi-trusted certificate authority (CA). Before the authentication process is performed, to bind users to their public keys the public key certificate must be verified. The remote authentication protocol has been investigated in the identity-based public key cryptography (ID-PKC) after considering the time and cost consuming certificates management. Since the public key of the user can be readily calculated from his publicly known identity (e.g., an email address or social insurance number) the necessity of the certificate have been avoided for the identity-based remote authentication protocols. Meanwhile, a fully trusted private key generator (PKG) is involved to generate private key for each user in the system, which certainly incurs the key escrow problem.

KGC Service

KGC: KGC is in charge of the enrollment and eviction of WBAN clients and APs. In general, KGC cannot be fully trusted since it is usually acted by a commercial organization. By considering the commercial benefits, it is natural for the KGC to misbehave such as illegally collecting clients' sensitive health information or accessing the services provided by APs free of charge. Therefore, the key escrow problem, where the KGC impersonates the clients or APs without being observed, should be avoided in our protocol.

Certificateless Cryptography: Certificateless public key cryptography (CL-PKC) [6] model avoids the inherent escrow of identity-based cryptography for the use of public key cryptography and which does not require certificates to guarantee the authenticity of public keys. The absence of certificates and the presence of an opponent who has access to a master key necessitate the careful development of a new security model. The focus is on certificateless public key encryption (CL-PKE), showing that a solid pairing-based CL-PKE scheme is secure [7] provided that an underlying problem closely related to the Bilinear Diffie-Hellman Problem is hard.

Anonymity Detection: By eavesdropping the communicating activities of this client, the adversary may establish the profile of a particular WBAN. Thus, it is important to protect the anonymity of the WBAN clients and any failures to do so may result in violation of WBAN clients privacy and raise legal issues; Mutual authentication: On one hand, the malicious adversary can access the service free of charge by impersonating as the

legitimate WBAN clients. by the AP impersonation attack, the malicious attacker may extort the sensitive personal health data from the target WBAN client. Thus, between the WBAN clients and requested remote AP the mutual authentication should be offered.

Authentication Access

Session Key Establishment: Due to the sensitive nature of the data collected by the medical sensors, a session key should be established between WBAN client and the requested AP to secure their subsequent communication. A semi-trusted authority distributes the private keys to the individual clients and collecting the service fee from the clients according to a certain business model such as pay-as-you-go business model. The TA can be considered as a collaborator or a management agent for a company (or several companies) and thus shares certain level of mutual interest with the company. However, the company and TA could collude to obtain private health data from client [8,9].

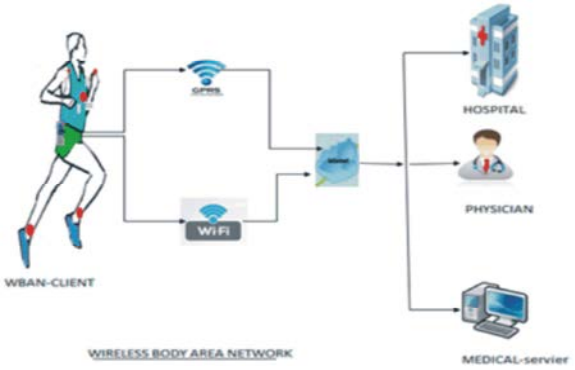
Random Key Generation: Random [10] password generators the output string of symbols of specified length. These can be individual characters from some character set, syllables designed to form pronounceable passwords, or words from some word list to form some letter symbols and numbers. The program can be customized to ensure the resulting password complies with the local password policy, say by always producing a mix of letters, numbers and special characters.

The Password strength of a random password against a particular attack (brute-force search), can be calculated by computing the information entropy of the random process that produced it. If each symbol in the password is produced independently and with uniform probability, the entropy in bits is given by the formula

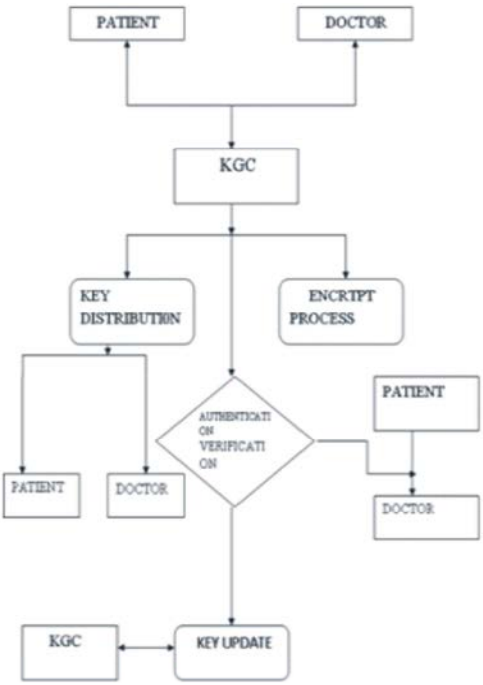
$$H = L \log_2 N = L\frac{\log N}{\log 2}$$

Where N is the number of possible symbols and L is the number of symbols in the password. The function $\log_2$ is the base-2 logarithm. H is typically measured in bits.

Architecture Diagram: This system comprises of WBAN client, AP (Hospital, Physician and Medical-Servier). With the tiny medical sensor nodes implanted inside or worn on human body and the smart portable device (SPD) held by the patient, a self-organized wireless body area network (WBANs) can be formed to monitor the health status and the surrounding environments of human bodies. Intra-body communications and extra-body communications are two basic communication modes in WBANs, which respectively allow sensors to communicate with each other and the SPD and enable SPD to communicate with the remote application providers (APs) such as the hospital, physician or medical staff. Possible applications of WBANs range from long-term daily living monitoring to location tracking and medical status monitoring [11,12].



Data Flow Diagram:



CONCLUSIONS

The conclusion is the proposing of an anonymous Certificateless remote authentication protocol with efficient revocation for WBANs in this paper and the major Contributions are as follows:

- The revocable Certificateless encryption (R-CLE) scheme against decryption key exposure and a revocable Certificateless signature (R-CLS) scheme against signing key exposure which is also the first in the literature.
- A Certificateless remote anonymous authentication protocol based on the combination of the new encryption scheme and signature scheme is present.

ACKNOWLEDGMENT

This research was supported by my Head of the Department, Prof.T.R.Srinivasan. I thank Mr. Chandra Mohan for assistance with a technique and Mr. Sathish for comments that greatlyimprovedthemanuscript

We thank famous persons Dr.Karunanithi and Dr.K.C.K.Vijaykumar, for sharing their pearls of wisdom with us during the course of this research and we thank Mrs.E.Menaka and Mr. R. Rajagopal reviewers for their so-called insights. Mrs.Leema Mathayi helped with some technical stuff. We are also immensely

REFERENCES

1. Alemdar, H. and C. Ersoy, 2010. "Wireless sensor networks for healthcare: A survey," Comput. Netw. 54(15): 2688-2710.
2. Chen, M., S. Gonzalez, A. Vasilakos, H. Cao and V.C.M. Leung, 2011. "Body area networks: A survey," Mobile Netw. Appl., 16(2): 171-193.
3. Latré, B., B. Braem, I. Moerman, C. Blondia and P. Demeester, 2011. "A survey on wireless body area networks," Wireless Netw., 17(1): 1-18.
4. Tan, C.C., H. Wang, S. Zhong and Q. Li, 2009. "IBE-Lite: A lightweight identity-based cryptography for body sensor networks," IEEE Trans. Inf. Technol. Biomed., 13(6): 926-932, Nov. 2009.
5. He, D., C. Chen, S. Chan, J. Bu and P. Zhang, 2013. "Secure and lightweight network admission and transmission protocol for body sensor networks," IEEE J. Biomed. Health Inform, 17(3): 664-674, May 2013.
6. Li, Yu, S., J.D. Guttman, W. Lou and K. Ren, 2013. "Secure ad hoc trust initialization and key management in wireless body area networks," ACM Trans. Sensor Netw., 9(2), 2013, Art. ID 18.
7. Malasri, K. and L. Wang, 2009. "Design and implementation of a securewireless mote-based medical sensor network," Sensors, 9(8): 6273-6297.
8. Lamport, L., 1981. "Password authentication with insecure communication,"Commun. ACM, 24(11): 770-772.
9. Hwang, M.S. and L.H. Li, 2000. "A new remote user authentication scheme using smart cards," IEEE Trans. Consum. Electron., 46(1): 28-30, Feb. 2000.
10. Madhusudhanan, B., S. Chitra and C. Rajan, 2015. Mobility Based Key Management Technique for Multicast Security in Mobile Ad Hoc Networks, The Scientific World Journal, Hindawi Publishing Corporation.
11. Lu, R., X. Li, X. Liang, X. Shen and X. Lin, 2011. "GRS: The green, reliability and security of emerging machine to machine communications," IEEE Commun. Mag., 49(4): 28-35, Apr. 2011.
12. Rajan, C. and N. Shanthi, 2013. Misbehaving attack mitigation technique for multicast security in mobile ad hoc networks (MANET). Journal of Theoretical and Applied Information Technology, 48(3): 1349-1357.