INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN: 2278 – 0211 (Online)

A Survey On Distributed System Security Using Three Factor Authentication

Amina Beevi.A
Dept. Of Computer Science&Engg, Sree Buddha College of Engineering, Pattoor Alappuzha(Dist), Kerala, India

Reeba. R
Dept. Of Computer Science&Engg, Sree Buddha College of Engineering, Pattoor Alappuzha(Dist), Kerala, India

Abstract:

As part of the security within distributed systems, various services and resources are distributed all over the network and they need protection from unauthorized users. Many of the information resources that are made available in distributed systems have a high intrinsic value to their users. Their security is therefore of considerable importance. To determine the identity of a remote client, remote authentication is most commonly used. This paper mainly investigates the systematic approaches for authenticating clients by three factors, namely password, smartcard and biometric. Most early authentication mechanism is solely based on password. While such protocols are relatively easy to implement, password has more vulnerabilities. Due to these concerns, hardware authentication tokens are used to strengthen the security in user authentication. Thus smartcard based password authentication mechanism has introduced. It could also fail if an attacker has successfully obtained the password and the data in the smart card. In this case, a third authentication factor, biometric characteristics can alleviate the problem and further improve the system's assurance. This survey on distributed Systems Security provides a holistic insight into current security issues, processes, and solutions, and maps out future directions in the context of today's distributed systems.

Keywords: *Authentication, Distributed Systems, Security, Biometric, Smartcard*

I. Introduction

Many of the information resources that are made available in distributed systems have a high intrinsic value to their users. Their security is therefore of considerable importance. Security for information resources has three components.

- Confidentiality – protection against disclosure to unauthorized individuals
- Integrity – protection against alteration or corruption
- Availability – protection against interference with the means to access the resources.

In a distributed system, various resources are distributed all over the distributed network. They are in the form of network services provided and managed by servers and accessed by clients. While considering the security within distributed systems, various services and resources need protection from unauthorized use. Most commonly used method to determine the identity of a remote client is the remote authentication. As part of remote authentication, there are three authentication factors:

- Something the client knows : password
- Something the client has: smart-card
- Something the client is : biometric characteristics

Most early authentication mechanisms are only based on password. Such protocols are relatively easy to implement, and so passwords (and human generated passwords in particular) have many vulnerabilities. As human generated and memorable passwords are usually short strings of characters and sometimes poorly selected, they are more vulnerable to get attack. Simple dictionary attacks can crack passwords in a short time by exploiting these vulnerabilities. Due to these reasons, hardware authentication tokens are introduced to strengthen the security in user authentication. And thus smart-card-based password authentication has become one of the most common authentication mechanisms. A successful login requires the client to have a valid smart card and a correct password by providing two factor authentication. While it provides stronger security guarantees than password authentication, it could also fail if both authentication factors are compromised (e.g., an attacker has successfully obtained the password and the data in the smart card). In this case, a third authentication factor can alleviate the problem and further improve the system's assurance.

Another authentication mechanism is biometric authentication where users are identified by their measurable human characteristics, such as fingerprint, voiceprint, and iris scan.

Biometric characteristics are believed to be a reliable authentication factor since they provide a potential source of high-entropy information and cannot be easily lost or forgotten. Despite these merits, biometric authentication has some imperfect features. Unlike password, biometric characteristics cannot be easily changed or revoked. Some biometric characteristics (e.g., fingerprint) can be easily obtained without the awareness of the owner. This motivates the three-factor authentication, which incorporates the advantages of the authentication based on password, smart card, and biometrics.

The main motivation of this survey is to investigate a systematic approach for authenticating clients by three factors, namely password, smart card, and biometrics. The three factor authentication is introduced to integrate the advantages of the authentication based on password, smart-card and biometric.

2.Literature Review

Most early authentication mechanisms are solely based on password. While such protocols are relatively easy to implement, passwords (and human generated passwords in particular) have many vulnerabilities. As an example, human generated and memorable passwords are usually short strings of characters and poorly selected. By exploiting these vulnerabilities, simple dictionary attacks can crack passwords in a short time.

In [1], Klein et al. mainly summarize the survey which outlines some of the problems associated with current password security by describing the way by which individual accounts may be broken. Also, various techniques used by crackers are outlined, and proposes one solution to this point of system vulnerability, a proactive password checker. The survey was done on the user's of Unix system. Initially, password encryption algorithms, DES algorithms are used to encrypt account and password. Since entire password file readable by all users, these encrypted passwords are vulnerable to cracking. One solution to this was to either make /etc/passwd unreadable, or to make the encrypted password portion of the file unreadable. The summary of the survey results that the problem with using passwords that are derived directly from obvious words.

A remote password authentication scheme needs a password table for verifying the legitimacy of the login users. If an attacker can gain access to this password table, and can modify the table, it may cause serious problems.

In [2], Hwang et al. proposed a new remote authentication mechanism using smartcard. Early smartcard based authentication mechanism is based on Shamir's ID based scheme

or based on simple geometric properties on the Euclidean plane. But these schemes have weaknesses in the security. The referenced scheme is based on the ElGamal's public key cryptosystem and it does not require to maintain any password table, also it can withstand message replaying attack.

The proposed system consists of three phases: registration phase, login phase, and authentication phase. Before accessing to a remote system, a new user should register his/her identity to the system. Then the registration centre will give the user a new smart card and a password through a secure channel. When a legitimate user wants to login into the system, he has to enter his smartcard into the login device and keys in his identity and password. The system generates password PW_i for a new user U_i as $PW_i = ID_i^{xa} \bmod P$, where xa is the secret key maintained by the system. Since Elgamal's public key cryptosystem is used, it is difficult to identify the secret key of the system from the above equation. Also the intruder cannot easily obtain the system generated random number during the login phase. The disadvantage of this proposed scheme is that it cannot prevent attack by impersonation.

In [3], Lee et al. proposed a more reliable and secure remote authentication mechanism, which is performed by removing the password table, and combining smartcard and fingerprint verification. This scheme is also based on Elgamal's public key cryptosystem which is used in [2]. In [2], the scheme requires only one secret key and does not have a password file. But this system cannot withstand against impersonation. To implement a scheme that can withstand impersonation, one more secret key is added in the proposed system than in [2]. Besides, to strengthen the system, the public elements used in the scheme is stored on a smartcard and each user can gain access to his own smart card by verifying himself using his fingerprint. Fingerprint verification method is based on minutia extraction and matching. Whenever a fingerprint is input, a different map of minutia is made. So a onetime random number for the ElGamal's public key cryptosystem can be generated using that map.

The proposed finger print based authentication system also consists of three phases: registration, login and authentication. To access a remote system, user should submit his ID to the system in the registration phase. Then system will pass the smartcard and password by a secure manner. To login in the system, user inserts his smartcard in the reader, types in ID and password, and imprints his fingerprint in the input device. Only if the fingerprint is verified successfully the smartcard will perform the remaining

authentication mechanism. Only if the authentication successfully ends, the system accepts login request, otherwise rejected.

Lin and Lee[4] showed that Lee et al.'s scheme is vulnerable to masquerade attack. Moreover the user is not allowed to choose and change their own password flexibly. The new proposed scheme is suitable for application with high security environment. This is also based on ElGamal's cryptosystem and the fingerprint verification. Also needs only to maintain one secret key. It can withstand masquerade attack evenif the intruder wangles a legal user's smartcard and password.

In the registration phase of this scheme, the user chooses his ID and password, where ID consists of some meaningful information related to user. User must personally imprint his fingerprint on input device and offer his ID and password in the registration centre. Then the centre issues user a smartcard with some information stored on the card. In the login phase, user insert his own smartcard and imprint the fingerprint. Then type the password. If the user passes fingerprint verification, then the smartcard will perform some operation based on the minutiae extracted from fingerprint and ID, and send the corresponding message to the remote system. The authentication phase perform the authentication procedure based on the received message. If the authentication being successful, the system accept login request, otherwise rejected. This paper also proposed a mechanism to change and choose their password very authorizedly.

The proposed scheme can be easily crypt analyzed. It performs only unilateral authentication(only client authentication) and there is no mutual authentication between user and remote system. So this scheme is susceptible to server spoofing attack.

There are applications that need authorization services in addition to authentication services. The combined use of authorization and authentication is termed as AAIs(Authorization and Authentication Infrastructures). But in certain situations, the physical presence of the individual for its identification is necessary. In [5], Dawson el al. solved this problem by using physical characteristics for recognition in a biometric system. That is, a biometric system is included in an AAI termed as BAAI(Biometric Authorisation and Authentication Infrastructure). This paper also describes the building technologies used in BAAI such as PMI(Privilege Management Ingrastructure), Stegnography and Biometrics(Face Recognition Tech).

The use of biometric eliminated the need of storage of secrets shared between system and user., since it uses intrinsic characteristics of the humans. In the proposed system, at the time of authentication itself, it is necessary to specify the privileges associated with

that user. Once the binding between the user's face image and his attributes is completed, the certificate is introduces inside the image by using stegnographic techniques. It allows having all authentication and authorization information in a single object called Visual Attribute Certificate.

There can be privacy issues related to biometric data. That is, how to protect biometric data. As biometrics cannot be easily changed, the breached biometric information will make the biometric authentication becomes meaningless.

In [6], Uludag et al. presents various methods that monolithically bind a cryptographic key with the biometric template of a user stored in the database in such a way that the key cannot be revealed without a successful biometric authentication.

The basic idea of biometric-based keys is that the biometric component performs user authentication (user authorization), while a generic cryptographic system can still handle the other components of containment (such as secure communication). This method of integrating biometrics into a cryptosystem is termed as the method of biometric-based key release. Thus, in such systems, a cryptographic key is stored as part of a user's database record, together with the user name, biometric template, access privileges, and the like, that is only released upon a successful biometric authentication.

This paper also briefly outlines the issues raised by the biometric-based key release system design, along with the possible solution mechanisms. The main characteristics of the biometric key release system design to be considered are: 1) it requires access to biometric templates for biometric matching and 2) user authentication and key release are completely decoupled. During enrollment in a biometric system, instead of storing the original biometric signal in the system database, only its transformed version is stored. Here, the transform is a change in the representation of an entity, where the new representation may comprise exactly the same information as in the previous one or may reflect a loss or augmentation of information contained in the original representation. During authentication, the biometric sensor would morph the signal using the same transform and the biometric matching would be carried out in the transformed space.

In [7], Wang et al., proposed a novel hash-based remote user authentication scheme. This scheme combines password, smart card, and fingerprint biometric, together with the two-variant hashing skill, to provide a secure solution with high efficiency. There are four phases in the proposed scheme namely registration, login, authentication and password change phase. The proposed system also perform security analysis on guessing attack resistance, DoS attack resistance, and providing strong protection on biometric data.

This scheme has following merits:(1)the required operations are only few hashing operations with low computation cost; (2)it allows users to choose and change their passwords freely and securely; (3)it provides mutual authentication between the user and the server; (4)there is no need to save the password table and biometric database on the remote server; (5) it can resist almost all the known attacks on smart card based authentication schemes; (6) it provides strong protection on user's password and biometrics; (7) A session key for private communication between user and remote server can be generated simultaneously during the authentication phase. The computation cost, security, and efficiency of the presented scheme are encouraging for the practical application in the resource-constraint environment.

Generally, a three factor authentication combines the biometric characteristics with password and smartcard based authentication mechanism. In this scheme, if biometric data is stored in the remote server, then it will not be secure. So some of the existing machanisms rely on smartcard to verify biometric data. But in this case, the remote server must trust the smart card to perform proper authentication which leads to various vulnerabilities.

In [8], Fan et al., proposed a truly secure three-factor authentication method that must keep the user's biometrics secret while still allowing the server to perform its own authentication. The proposed scheme fully preserves the privacy of the biometric data of every user, that is, the scheme does not reveal the biometric data to anyone else, including the remote servers. The biometric template and biometric samples of every user are protected while the server performs the matching algorithm, so that the server cannot learn biometric data in authentication processes. Moreover, the server itself or any adversary who has corrupted the server cannot still obtain users' biometric data even if users' cards have been stolen or lost and the data in the cards are leaked.

The method has three phases: 1) initialization, 2) registration, and 3) login and authentication. The essential approach of this scheme is as follows: 1) During the registration, the client chooses a random string and encrypts it using his/her biometric template; 2) The result (called sketch) is stored in the smart card; and 3) During the authentication, the client must convince the server that he/she can decrypt the sketch, which needs correct biometrics.

The proposed scheme is suitable for the smart-card environment due to the low-computation property. Especially, this approach does not reveal the users' biometric data to the server such that it is a truly three-factor authentication scheme with strong privacy

protection on the biometric data of every user against anyone else. And the soundness of the scheme is proved to be based on the security of the adopted underlying public-key and symmetric encryption schemes.

3.Conclusion

While designing a distributed system, preserving security and privacy is becoming a challenging design issue. This survey on distributes system security mainly outlines the problems and addresses solutions to the various remote authentication mechanisms. It is necessary to solve these issues to protect services and resources from unauthorized use. It can also makes a step forward in solving these issues by integrating the authentication based on password, smart card, and biometrics. A generic and secure framework is needed to upgrade two-factor authentication to three-factor authentication by this review. The three factor authentication can be introduced to integrate the advantages of the authentication based on password, smart-card and biometric. Also it should not only be greatly improve the information security in distributed computing at low cost but also should protects client privacy in distributed systems.

4.Reference

1. D.V. Klein, “Foiling the Cracker: A Survey of, and Improvements to, Password Security,” Proc. Second USENIX Workshop Security, 1990.
2. M.S Hwang and L.H Li, “A new remote user authentication scheme using smart card” , IEEE Transactions on Consumer Electronics, vol. 46, no 1, pp. 28-30 ,2000
3. J.K. Lee, S.R. Ryu, and K.Y. Yoo, “Fingerprint-Based Remote User Authentication Scheme Using Smart Cards,” Electronics Letters, vol. 38, no. 12, pp. 554-555, June 2002
4. C.H. Lin and Y.Y. Lai, “A Flexible Biometrics Remote User Authentication Scheme,” Computer Standards Interfaces, vol. 27, no. 1, pp. 19-23, Nov. 2004.
5. Ed. Dawson, J. Lopez, J. A. Montenegro, and E. Okamoto, “BAAI: Biometric Authentication and Authorization Infrastructure,” Proc. IEEE Intern. Conference on Information Technology:Research and Education (ITRE’03), pp. 274-278, 2004.
6. UMUT ULUDAG, SHARATH PANKANTI, SALIL PRABHAKAR, ANIL K. JAIN, “Biometric Cryptosystems: Issues and Challenges” IEEE 2004
7. Xiaomin Wang, Wenfang Zhang, “An efficient and secure biometric remote user authentication scheme using smart cards” IEEE 2008
8. Chun-I Fan and Yi-Hui Lin, “Provably Secure Remote Truly Three-Factor Authentication Scheme With Privacy Protection on Biometrics” IEEE 2009
9. Y. Dodis, L. Reyzin, A. Smith, “Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data,” Proc. Eurocrypt 2004, pp. 523-540, 2004.
10. X. Boyen, “Reusable Cryptographic Fuzzy Extractors,” Proc. CCS 2004, pp. 82-91, 2004.