An Improved Authentication Framework using Dynamic Access Code and Biometrics in Distributed Systems

Wasim Asad, Chandan Raj B R

Abstract— for enhancing security in distributed systems this paper explains a systematic approach for authenticating clients by three factors, namely password, biometrics and dynamic access code. The reason for replacing smart cards with the dynamic access code is based on the limitations experienced by the clients while using smart cards. The proposed framework not only assures securing information at low cost but also protects client privacy in distributed systems with the high level secured environment.

Index Terms— Authentication, distributed systems, dynamic access code, biometrics, security, privacy, password

1 Introduction

or thousands of years individuals have used passwords to Fauthenticate their identity. Passwords were the first security system implemented on computers 40 years ago and represent the most common, if inappropriate (when used alone), security technology used in today's computer and Internet environment. They are used in conjunction with ATM cards, funds transfer, credit/debit cards, access to personal and financial information, physical facility access and in other situations where basic personal identification must be verified.
In this paper, the three authenticating techniques used are:

- Password.
- Dynamic access code.
- Biometric characterist

Earlier mechanisms were based only on passwords, and to implement such mechanism is easy and have many vulnerabilities. Mostly the passwords selected are either poorly selected or are short strings. Due to these shortcomings hardware authentication tokens were introduced.

Common biological characteristics used for Biometric enterprise authentication are fingerprints, palm or finger vein patterns, iris features, and voice or face patterns. These last three involve no physical contact with a biometric sensor, which makes them less intrusive to use. The main benefit of using a biometric authentication] factor [2], [3],[4] instead of a physical token is that biometrics can't easily be lost, stolen, hacked, duplicated, or shared. They are also resistant to social engineering attacks – and since users are required to be present to use a biometric factor, it can also prevent unethical employees from repudiating responsibility for their actions by claiming an imposter had logged on using their authentication credentials when they were not presen
Third authenticating technique used in this paper is Dynamic access code, which is generated on the server side and is sent to the client either on the mobile phone or else to their mail ID.

1.1 Motivation

The motivation of this paper is overcome the limitations of using a smart card as the third authentification technique and replacing it with dynamic access code. A well designed three-factor authentication protocol can greatly improve the information assurance in distributed systems

1.2 Contribution

The main contribution of this paper is to overcome the limitations of using a smart card.

For higher security needs, a smart card is a not a tamper-proof device to store information. All data and passwords on a card are stored in the EEPROM and can be erased or modified by an unusual voltage supply. Therefore some security processors implemented sensors for environmental changes. However, since it is difficult to find the right level of sensitivity and there is a voltage fluctuation when the power is suplied to the card, this method is not widely used. Other successful attacks methods include heating the controller to a high temperature or focusing the UV light on the EEPROM, thus removing the security lock. Invasive physical attacks are the most destructive when the card is cut and processor removed. Then the layout of the chip can be reverse engineered.

Differential Power Analysis (DPA), is a statistical attack on a cryptographic algorithm which compares a hypothesis with a measured outcome and is often capable of extracting an encryption key from a smart card or other computing device. Simple Power Analysis (SPA), the direct analysis of the recorded power data to determine actions and data, is also useful.

First, we demonstrate how to incorporate biometrics in the existing authentication. Second, authentication protocols in our framework can provide true three-factor authentication, namely a successful authentication requires password, dy-

namic access code, and biometric characteristics. Last, in the proposed framework clients' biometric characteristics are kept secret from servers. This not only protects user privacy but also prevents a single-point failure (e.g., a breached server) from undermining the authentication level of other services.

1.3 Related Work

There has been several authentication protocols have been to integrate biometric authentication with password authentication and/or smart-card authentication. Lee et al. [5] designed an authentication system which does not need a password table to authenticate registered users. Instead, smart card and fingerprint are required in the authentication. However, due to the analysis given in [6], Lee et al.'s scheme is insecure under conspiring attack. Lin and Lai [7] showed that Lee et al.'s scheme is vulnerable to masquerade attack. Namely, a legitimate user (i.e., a user who has registered on the system) is able to make a successful login on behalf of other users. An improved authentication protocol was given by Lin and Lai to fix that flaw. The new protocol, however, has several other security vulnerabilities. First, Lin-Lai's scheme only provides client authentication rather than mutual authentication, which makes it susceptible to the server spoofing attack [8]. Second, the password changing phase in Lin- Lai's scheme is not secure as the smart card cannot check the correctness of old passwords [9]. Third, Lin-Lai's scheme is insecure under impersonation attacks due to the analysis given by Yoon and Yoo [10], who also proposed a new scheme. However, the n scheme is broken and improved by Lee and Kwon [11]. In [12], Kim et al. proposed two ID-based password authentication schemes where users are authenticated by smart cards, passwords, and fingerprints. However, Scott [13] showed that a passive eavesdropper (without access to any smart card, password or fingerprint) can successfully login to the server on behalf of any claiming identity after passively eavesdropping only one legitimate login. Bhargav-Spantzel et al. proposed a privacy preserving multifactor authentication protocol with biometrics [14]. Fan and Lin [17] proposed a three-factor authentication scheme with privacy protection on bi metrics. The essential approach of their 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 (close to the biometric template in the registration). As we shall show shortly, our framework employs a different approach. The client in our framework uses his/her biometrics to gene ate a random string. This leads to a generic three-factor authentication protocol from smart-card-based password authentication. Very recently, Li and Hwang [18] proposed another biometric-based remote client authentication scheme using

2. Three-Factor Verification

Three-factor authentication involves authenticating the client using a password, biometric scan and dynamic access code. A three-factor authentication protocol involves a client C and a server S, and consists of five phases.

3-Factor-Initialization:
S generates two system parameters PK and SK. PK is published in the system, and SK is kept secret by S. An execution of this algorithm is denoted by $3-Factor-Initialization(k) \longrightarrow (PK, SK)$, where k is system's security parameter.

3-Factor-Reg: A client C, with an initial password PW and biometric characteristics BioData, registers on the system by running this interactive protocol with the server S. The output of this protocol is a dynamic access code, which is given to C. An execution of this protocol is denoted by

$$C[PW, BioData] \xleftrightarrow{3-Factor-\mathrm{Re}g} S[SK] \rightarrow DMC$$

3-Factor-Login-Auth: This is another interactive protocol between the client C and the server S, which enables the clientto login successfully using PW, SC, and BioData. An execution of this protocol is denoted by

$$C[PW, DMC, BioData] \xleftrightarrow{3-Factor-Login-Auth} S[SK]$$

The output of this protocol is "1" (if the authentication is successful) or "0" (otherwise).

3-Factor-Password-Changing:
This protocol enables a client to change his/her password after a successful authentication.

3-Factor-Biometrics-Changing:
An analogue of password- changing is biometrics-changing, namely the client can change his/her biometrics used in the authentication, e.g., using a different finger or using iris instead of finger.

Error Tolerance and Non Trusted Devices:
One challenge in biometric authentication is that biometric characteristics are prone to various noise during data collecting, and this natural feature makes it impossible to reproduce precisely each time biometric characteristics are measured. A practical biometric authentication protocol cannot simply compare the hash or the encryption of biometric templates (which requires an exact match). Instead, biometric authentication must tolerate failures within a reasonable bound. Another issue in biometric authentication is that the verification of biometrics should be performed by the server instead of other devices, since such devices are usually remotely located from the server and cannot be fully trusted. The above two subtle issues seem to be neglected in a recent three-factor authentication protocol proposed by Li and Hwang [18].

Cost effectiveness.
To make three-factor authentication practical, biometric-related operations must be performed fast and accurately. As indicated in [16], the performance of extracting and authenticating certain types of biometrics (e.g., face and keystroke) is

not satisfactory, but others (e.g., fingerprint and iris) can satisfy practical requirements. (Examples include fingerprint recognition in laptops and biometric visa.)

Security requirements.

A three-factor authentication protocol can also face passive attackers and active attackers. A passive (an active) attacker can be further classified into the following three types.

Type I attacker has the dynamic access code and the biometric characteristics of the client. It is not given the password of that client.

Type II attacker has the password and the biometric characteristics. It is not allowed to obtain the data in the dynamic access code.

Type III attacker has the dynamic access code and the password of the client. It is not given the biometric characteristics of that client. Notice that such an attacker is free to mount any attacks on the (unknown) biometrics, including biometrics faking and attacks on the metadata (related to the biometrics).

2.1 Fuzzy Extractor

This section briefly reviews the fuzzy extractor introduced

2.1.1 Metric Space

A metric space is a set M with a distance function dis :

$M \times M \rightarrow IR^{+} = [0, \infty]$ which obeys various natural properties.

2.1.2 Statistic Distance

The statistical distance between two probability distributions A and B is denoted by

$$SD(A, B) = 1/2 \sum_{v} \left| \Pr(A = v) - \Pr(B = v) \right|$$

2.1.3 Entropy

The min-entropy $H_{\infty}(A)$ of a random variable A is $-\log(\max_{a} \Pr[A = a])$.

2.3.4 Fuzzy Extractor

A fuzzy extractor extracts a nearly random string R from its biometric input w in an error-tolerant way. If the input changes but remains close, the extracted R remains the same. To assist in recovering R from a biometric input w0, a fuzzy extractor outputs an auxiliary string P. However, R remains uniformly random even given P. The fuzzy extractor is formally defined as below.

Definition: An (M,m,l,t,e) fuzzy etractor is given by two procedures (Gen, Rep).

1. $\xrightarrow{BioData:w} Gen \rightarrow \begin{cases} R \\ P \end{cases}$

Where 'R' represents the random string and 'P' represents auxillary string. Gen is a probabilistic generation procedure, which on (biometric) input $w \in M$ outputs an "extracted" string

2. $\xrightarrow{BioData:w'} \text{Rep} \rightarrow R \text{ if dis}((w, w')) \leq t$

Rep is a deterministic reproduction procedure allowing to recover R from the corresponding auxiliary string P and any vector w' close to w

3 Comparison with previous models

The purpose of this paaper is to overcome the limitations of using a smartcard in three factor authentication and replace it with dynamic access code. This saves the time and effort on the design of three-factor authentication with those properties, and more importantly avoids the confusing "broken and I proved" process in the existing research on three-step verification.

.

4 Conclusion

Ensuring security in distributed systems can be difficult. This paper makes an effort forward in solving this problem by proposing 3 step verification process using dynamic access code. The authentication is based on password, biometric scan and dynamic access code. Our framework not only demonstrates how to obtain secure three-factor verfication from two factor authentication, but also addresses several prominent issues of biometric authentication in distributed systems. The future work is to fully identify the practical threats on three-factor authentication and develop concrete threefactor authentication protocols with better performances.

5. References

[1] D.V. Klein, "Foiling the Cracker: A Survey of, and Improvements to, Password Security," Proc. Second USENIX Workshop Security,1990.

[2] Biometrics: Personal Identification in Networked Society, A.K. Jain, R. Bolle, and S. Pankanti, eds. Kluwer, 1999.

[3] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. Springer-Verlag, 2003.

[4] Ed. Dawson, J. Lopez, J.A. Montenegro, and E. Okamoto, "BAAI: Biometric Authentication and Authorization Infrastructure," Proc. IEEE Int'l Conf. Information Technology: Research and Education (ITRE '03), pp. 274-278, 2004.

[5] 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.

[6] C.C. Chang and I.C. Lin, "Remarks on Fingerprint-Based
Remote User Authentication Scheme Using Smart Cards," ACM SIGOPS Operating Systems Rev., vol. 38, no. 4, pp. 91-96, Oct. 2004.

[7] 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.

[8] M.K. Khan and J. Zhang, "Improving the Security of 'A Flexible Biometrics Remote User Authentication Scheme'," Computer Standards Interfaces, vol. 29, no. 1, pp. 82-85, Jan. 2007.

[9] C.J. Mitchell and Q. Tang, "Security of the Lin-Lai Smart Card Based User Authentication Scheme," Technical Report RHULMA20051, http://www.ma.rhul.ac.uk/static/techrep/2005/RHUL-MA-2005-1.pdf, Jan. 2005.

[10] E.J. Yoon and K.Y. Yoo, "A New Efficient Fingerprint-Based Remote User Authentication Scheme for Multimedia Systems," Proc. Ninth Int'l Conf. Knowledge-Based Intelligent Information and Eng. Systems (KES), 2005.

[11] Y. Lee and T. Kwon, "An improved Fingerprint-Based Remote User Authentication Scheme Using Smart Cards," Proc. Int'l Conf. Computational Science and Its Applications (ICCSA), 2006.

[12] H.S. Kim, J.K. Lee, and K.Y. Yoo, "ID-Based Password Authentication Scheme Using Smart Cards and Fingerprints," ACM SIGOPS Operating Systems Rev., vol. 37, no. 4, pp. 32-41, Oct. 2003.

[13] M. Scott, "Cryptanalysis of an ID-Based Password Authentication Scheme Using Smart Cards and Fingerprints," ACM SIGOPS Operating Systems Rev., vol. 38, no. 2, pp. 73-75, Apr. 2004.

[14] A. Bhargav-Spantzel, A.C. Squicciarini, E. Bertino, S. Modi, M. Young, and S.J. Elliott, "Privacy Preserving Multi-Factor Authentication with Biometrics," J. Computer Security, vol. 15, no. 5, pp. 529-560, 2007. S. Goldwasser, S. Micali, and C. Rackoff, "The Knowledge Complexity of Interactive Proof-Systems," SIAM J. Computing, vol. 18, no. 1, pp. 186-208, Feb. 1989.

[15] U. Uludag, S. Pankanti, S. Prabhakar, and A.K. Jain, "Biometric Cryptosystems: Issues and Challenges," Proc. IEEE, Special Issue on Multimedia Security for Digital Rights Management, vol. 92, no. 6, pp. 948-960, June 2004.

[16] C.-I. Fan and Y.-H. Lin, "Provably Secure Remote Truly Three-Factor Authentication Scheme with Privacy Protection on Biometrics," IEEE Trans. Information Forensics and Security, vol. 4, no. 4, pp. 933-945, Dec. 2009.

[17] C.T. Li and M.-S. Hwang, "An Efficient Biometrics-Based Remote User Authentication Scheme Using Smart Cards," J. Network and Computer Applications, vol. 33, no. 1, pp. 1-5, 2010.

[18] P.C. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis,"Proc. Int'l Cryptology Conf. (CRYPTO), pp. 388-397, 1999.

[19] T.S. Messerges, E.A. Dabbish, and R.H. Sloan, "Examining Smart-Card Security under the Threat of Power Analysis Attacks," IEEE Trans. Computers, vol. 51, no. 5, pp. 541-552, May 2002.

[20] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (Eurocrypt), pp. 523-540, 2004.

[21] N.K. Ratha, J.H. Connell, and R.M. Bolle, "Enhancing Security and Privacy in Biometrics-Based Authentication Systems," IBM Systems J., vol. 40, no. 3, pp. 614-634, 2001.

[22] M.-H. Lim and A.B.J. Teoh, "Cancelable Biometrics," Scholarpedia, vol. 5, no. 1, p. 9201, 2010.