International Conference on
Contemporary Technological Solutions towards fulfillment of Social Needs

Analysis of Recent Smart Authentication Schemes

Priyank Nayak[1], Ravi Singh Pippal[2]

[1]*Research Scholar, Computer Science and Engineering*

[2] *Professor, Computer Science and Engineering*

RKDF University, Bhopal, India

[2] ravesingh@gmail.com

Abstract — During the past few years several smart card based authentication schemes have been proposed. However, none of them fulfils the necessary requirements to achieve a secure and efficient scheme. With respect to the present security needs and essential desires of users, the objective of this paper is to validate the efficiency of smart card based authentication schemes found in the literature on the basis of computation cost and security features provided.

Keywords — *Smart Card, Attacks, Computational Complexity, Password, Security.*

I INTRODUCTION

This paper focuses on smart card based remote user authentication for contact smart cards. When separately compared these methods have vulnerabilities. The combination of any two factors provides a stronger authentication. The scope of this work is the use of contact smart card as one factor and password as other factor. There are various security attacks which can be mounted on authentication schemes. This work covers the potential attacks which includes user impersonation attack, password guessing attack, replay attack, parallel session attack, reflection attack, privileged insider attack and attack on password change phase. In this context, Chang and Wu [1] first proposed password based smart card authentication scheme without verification table. Subsequently, authentication based on smart card has been employed continuously in several applications like cloud computing [2], healthcare [3], key exchange in IPTV broadcasting [4], wireless networks [5], authentication in multi-server environment [6], wireless sensor networks [7] and many more.

The rest of the paper is organized as follows: section II presents comparison based on various security attacks, section III deals with comparison based on various security features provided, section IV shows comparison of smart card authentication schemes in terms of computational complexity and finally, section V concludes the paper.

II COMPARISON BASED ON VARIOUS SECURITY ATTACKS

In order to measure the security in terms of potential attacks, numerous well known timestamp based smart card authentication schemes [8-21]. Table 1 shows that the comparison among various schemes. The parameters used in Table I are:

- Impersonation attack (SA1)
- Replay attack (SA2)
- Password guessing attack (SA3)
- Reflection attack (SA4)
- Parallel session attack (SA5)
- Privileged insider attack (SA6)
- Attack on password change phase (SA7)

TABLE I
COMPARISON BASED ON SECURITY ATTACKS

S. No.	Security Attacks	SA1	SA2	SA3	SA4	SA5	SA6	SA7
1	R. Song [8]	Secure	Secure	Insecure	Secure	Secure	Insecure	Secure
2	Hwang-Li [9]	Insecure	Secure	Secure	NA	NA	NA	NA
3	H. M. Sun [10]	Secure	Secure	Insecure	NA	NA	NA	NA
4	Chien et al. [11]	Secure	Secure	Insecure	Insecure	Insecure	Insecure	NA
5	Ku-Chen [12]	Insecure	Secure	Insecure	Secure	Insecure	Secure	Insecure
6	Yoon et al. [13]	Insecure	Secure	Insecure	Secure	Secure	Secure	Secure

7	Wang et al. [14]	Secure	Secure	Insecure	Secure	Secure	Secure	Secure
8	Das et al. [15]	Secure	Secure	Insecure	NA	NA	Insecure	Insecure
9	Liao et al. [16]	Insecure	Secure	Insecure	Insecure	Secure	Secure	Insecure
10	Wang et al. [17]	Insecure	Secure	Insecure	Secure	Secure	NA	Insecure
11	Hao-Yu [18]	Secure	Secure	Insecure	Secure	Secure	NA	Secure
12	Liaw et al. [19]	Insecure	Secure	Secure	Secure	Secure	Insecure	Insecure
13	Liu et al. [20]	Insecure	Secure	Insecure	Secure	Secure	Insecure	NA
14	Pippal et al. [21]	Secure	Secure	Secure	Secure	Secure	Secure	Secure

III COMPARISON BASED ON VARIOUS SECURITY FEATURES PROVIDED

Further, a comparison is additionally given in Table II on the basis of essential security features that need to be offered by any authentication scheme. The parameters used for comparison are:

- User is allowed to choose the password (SF1)
- User is allowed to change the password (SF2)
- Provides early wrong password detection (SF3)
- Provides mutual authentication (SF4)
- Provides session key generation (SF5)
- Free from server involvement during password change (SF6)

TABLE III
COMPARISON BASED ON SECURITY FEATURES PROVIDED

S. No.	Security Features	SF1	SF2	SF3	SF4	SF5	SF6
1	R. Song [8]	Yes	Yes	No	Yes	Yes	No
2	Hwang-Li [9]	No	No	No	No	No	NA
3	H. M. Sun [10]	No	No	No	No	No	NA
4	Chien et al. [11]	Yes	No	No	Yes	No	NA
5	Ku-Chen [12]	Yes	Yes	No	Yes	No	Yes
6	Yoon et al. [13]	Yes	Yes	No	Yes	No	Yes
7	Wang et al. [14]	Yes	Yes	Yes	Yes	Yes	Yes
8	Das et al. [15]	Yes	Yes	No	No	No	Yes
9	Liao et al. [16]	Yes	Yes	No	Yes	No	Yes
10	Wang et al. [17]	No	Yes	No	Yes	No	Yes
11	Hao-Yu [18]	No	Yes	No	Yes	No	Yes

12	Liaw et al. [19]	Yes	Yes	No	Yes	Yes	Yes
13	Liu et al. [20]	Yes	No	No	Yes	No	NA
14	Pippal et al. [21]	Yes	Yes	Yes	Yes	Yes	Yes

IV Comparison based on Computational Complexity

Due to the resources constraints of smart card, the authentication scheme must take efficiency evaluation into consideration. Computational cost related to authentication schemes is an imperative issue for performance analysis. The efficiency comparison among these schemes is listed in Table III. In worst case, the time complexities for performing the Modular Exponentiation (ME) and Modular Multiplication (MM) are O((log n)3) and O((log n)3) respectively. As the time complexity for performing the one-way hash function depends on what cryptographic primitive it employed i.e. XOR operations and rotation operations (in case of SHA), the time complexity of calculating a hashing value is O(1).

TABLE IIIII
Comparison based on Computational Complexity

S. No.	Authentication Schemes	Time Complexity	Registration Phase	Login & Authentication Phase	Password Change Phase	Total Operations
1	R. Song [8]	$O((\log n)^3)$	2HF+1ME	8HF+1ME+2E/D	5HF+1ME+2E/D	15HF+3ME+4E/D
2	Hwang-Li [9]	$O((\log n)^3)$	1ME	2HF+6ME+2MM	-	2HF+7ME+2MM
3	H. M. Sun [10]	O(1)	1HF	3HF	-	4HF
4	Chien et al. [11]	O(1)	1HF	5HF	-	6HF
5	Ku-Chen [12]	O(1)	2HF	6HF	2HF	10HF
6	Yoon et al. [13]	O(1)	2HF	6HF	2HF	10HF
7	Wang et al. [14]	O(1)	3HF	8HF	4HF	15HF
8	Das et al. [15]	O(1)	2HF	7HF	2HF	11HF
9	Liao et al. [16]	O(1)	2HF	9HF	2HF	13HF
10	Wang et al. [17]	O(1)	2HF	6HF	2HF	10HF
11	Hao-Yu [18]	O(1)	3HF	7HF	9HF	19HF
12	Liaw et al. [19]	$O((\log n)^3)$	1HF	3HF+4ME+2E/D	-	4HF+4ME+2E/D
13	Liu et al. [20]	$O((\log n)^3)$	1HF+2ME	5HF+6ME+2MM	-	6HF+8ME+2MM
14	Pippal et al. [21]	$O((\log n)^3)$	2HF+1ME	8HF+13ME+2MM	2HF+2ME	12HF+14ME+2MM

V Conclusion

Security and efficiency ate the main factors for any authentication scheme. This paper describes a comparative analysis of major smart card authentication schemes in terms of security features provided, security attacks defended and computational complexity. This effort will assist the researchers to work in different directions towards design and development of secure and efficient smart card authentication scheme.

References

[1] Chang CC, Wu TC. Remote password authentication with smart cards. IEE Proceedings E: Computers and Digital Techniques. 1991, 138:165-168.

[2] Pippal RS, Jaidhar CD, Tapaswi S. Enhanced time-bound ticket-based mutual authentication scheme for cloud computing. Informatica. 2013; 37(2):149-156.

[3] Hu J, Chen HH, Hou TW. A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations. Computer Standards and Interfaces. 2010; 32(5-6):274-280.

[4] Pippal RS, Jaidhar CD, Tapaswi S. Secure key exchange scheme for IPTV broadcasting. Informatica. 2012; 36(1):47-52.
[5] He D, Ma M, Zhang Y, Chen C, Bu J. A strong user authentication scheme with smart cards for wireless communications. Computer Communications. 2011; 34(3):367-374.
[6] Pippal RS, Jaidhar CD, Tapaswi S. Robust smart card authentication scheme for multi-server architecture. Wireless Personal Communications (Springer). 2013; 72(1):729-745.
[7] Fan R, He DJ, Pan XZ, Ping LD. An efficient and DoS resistant user authentication scheme for two-tiered wireless sensor networks. Journal of Zhejiang University SCIENCE C (Computers and Electronics). 2011; 12(7):550-560.
[8] R. Song, "Advanced smart card based password authentication protocol," Computer Standards and Interfaces, vol. 32, no. 5-6, 2010, pp. 321-325.
[9] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, vol. 46, no. 1, 2000, pp. 28-30.
[10] H. M. Sun, "An efficient remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, vol. 46, no. 4, 2000, pp. 958-961.
[11] H. Y. Chien, J. K. Jan and Y. M. Tseng, "An efficient and practical solution to remote authentication: smart card," Computers and Security, vol. 21, no. 4, 2002, pp. 372-375.
[12] W. C. Ku and S. M. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, vol. 50, no. 1, 2004, pp. 204-207.
[13] E. J. Yoon, E. K. Ryu and K. Y. Yoo, "Further improvement of an efficient password based remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, vol. 50, no. 2, 2004, pp. 612-614.
[14] X. M. Wang, W. F. Zhang, J. S. Zhang and M. K. Khan, "Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards," Computer Standards and Interfaces, vol. 29, no. 5, 2007, pp. 507-512.
[15] M. L. Das, A. Saxena and V. P. Gulati, "A dynamic ID-based remote user authentication scheme," IEEE Transactions on Consumer Electronics, vol. 50, no. 2, 2004, pp. 629-631.
[16] I. E. Liao, C. C. Lee and M. S. Hwang, "Security enhancement for a dynamic ID-based remote user authentication scheme," In Proceedings of the International Conference on Next Generation Web Services Practices (NWeSP'05), Seoul, Korea, 2005, pp. 437-440.
[17] Y. Y. Wang, J. Y. Liu, F. X. Xiao and J. Dan, "A more efficient and secure dynamic ID based remote user authentication scheme," Computer Communications, vol. 32, no. 4, 2009, pp. 583-585.
[18] Z. Hao and N. Yu, "A security enhanced remote password authentication scheme using smart card," In Proceedings of the 2nd International Symposium on Data, Privacy and E-Commerce (ISDPE'10), Buffalo, USA, 2010, pp. 56-60.
[19] H. T. Liaw, J. F. Lin and W. C. Wu, "An efficient and complete remote user authentication scheme using smart cards," Mathematical and Computer Modelling, vol. 44, no. 1-2, 2006, pp. 223-228.
[20] J. Y. Liu, A. M. Zhou and M. X. Gao, "A new mutual authentication scheme based on nonce and smart cards," Computer Communications, vol. 31, no. 10, 2008, pp. 2205- 2209.
[21] Ravi Singh Pippal, Jaidhar C. D. and Shashikala Tapaswi, "Highly secured remote user authentication scheme using smart cards," In Proceedings of the 7th IEEE Conference on Industrial Electronics and Applications (ICIEA'12), Singapore, 2012, pp. 988-992.