ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 2, Issue 2 , February 2015

Improving Security on Smart-Based Password Key Agreement

Raja Iyappan P, Krishnaveni V, Karthika M

P.G student, Dept of CSE, Dhanalakshmi Srinivasan Engineering College, Tamilnadu, India

P.G student, Dept of CSE, Dr.Nagarathinam's College of Engineering, Namakkal, Tamilnadu, India

Assistant Professor, Dept of CSE, Dhanalakshmi Srinivasan Engineering College, Tamilnadu, India

ABSTRACT: In recent trends smart cards are used as electronic wallets. Because smart card brings comfortable to the users and also smart card increases the risk, when the card holder lost the card. If the smart card is affected by an attacker, the attacker will try to analyze the secret information within the smart card or break the entire authentication system. So we need smart card based password authentication scheme for providing the security to the smart card. Cryptographic protocols protect the exchange of money between the smart card and the machine. In our proposed scheme involves a server and a user, and typically consists of three phases. The first phase is called the registration phase, an initial password for the user is also determined (chosen by the user or by the server). Once the registration phase is completed, the user is able to access the server in the log-in phase, which can be carried out as many times as needed. A successful log-in requires the user to have the valid smart card and the correct password. In other words, the scheme provides two-factor (password and smart card) authentication. In the authentication phase, the user can freely change his/her password and also get update password information which generated by the server to the smart card accordingly. Due to the limitation of computational power, a smart card may not be able to afford heavy computations. Thus employ an additional pre-computation phase to speed-up the authentication process during the log-in phase.

KEYWORDS: Authentication, key exchange, offline-dictionary attack, online-dictionary attack, smart card

I. INTRODUCTION

A smart-card-based password authentication scheme involves a server and a user, and typically consists of three phases. The first phase is called the registration phase, where the server issues a smart card to the user. The smart card contains the personal information about the user, which will be used later for the authentication. In this phase, an initial password for the user is also determined (chosen by the user or by the server). Once the registration phase is completed, the user is able to access the server in the log-in phase, which can be carried out as many times as needed. A successful log-in requires the user to have the valid smart card and the correct password. In other words, the scheme provides two-factor (password and smart card) authentication. In the password-changing phase, the user can freely change his/her password and update the information in the smart card accordingly. Due to the limitation of computational power, a smart card may not be able to afford heavy computations.

Many smart-card-based password authentication schemes have been proposed, and various security goals and properties have been addressed, including (but are not limited to) low computation and communication cost, no password table, security against replay attacks, parallel session attacks, mutual authentication, session key agreement and security against adversaries with smart card. It is not trivial to design smart-card-based password authentication satisfying even the basic security requirements, and in fact many schemes have been found broken shortly after their proposals. It is a well-known problem that human memorable passwords only come from a small domain. This enables adversaries (with the smart card) to guess a user's password by using every "word" in a password dictionary, which is known as dictionary attack. Dictionary attack can be further divided into online (active) and offline (passive) dictionary attack. An online-dictionary attacker could try to log on the server by trying every possible password for a specific user.

II. METHODS

A) Smart Cards and Logical Access

Organizations of all sizes and in all industries are working to improve the process used to identify users to their networked systems. With the growing use of wired and wireless networks to access information resources and the increasing occurrence of identity theft and attacks on corporate networks, password-based user authentication is increasingly acknowledged to be a significant security risk. Both enterprises and government agencies are moving to replace simple passwords with stronger, multi-factor authentication systems that strengthen information security, respond to market and regulatory conditions, and lower support costs.

Smart-card-based logical access allows organizations to issue a single ID card that supports logical access, physical access, and secure data storage, along with other applications. By combining multiple applications on a single ID card, organizations can reduce cost, increase end-user convenience, and provide enhanced security for different applications. Smart card technology provides organizations with cost-effective logical access. Smart cards deliver a positive business case for implementing any authentication technology. Improved user productivity, reduced password administration costs, decreased exposure to risk, and streamlined business processes all contribute to a significant positive return on investment.

The need for stronger online identity authentication and established the National Strategy for Trusted Identities in Cyberspace (NSTIC) initiative. NSTIC broadly defines an Identity Ecosystem that would re-establish trust and better protect online identities. According to the Howard A. Schmidt on the White House blog, “Through the strategy we seek to enable a future where individuals can voluntarily choose to obtain a secure, interoperable, and privacy-enhancing credential.

B) Smart Cards and Physical Access

Smart cards are increasingly accepted as the credential of choice for securely controlling physical access. Standards-based smart ID cards can be used to easily authenticate a person’s identity, determine the appropriate level of access, and physically admit the cardholder to a facility. Through the appropriate use of contact or contactless smart card technology in the overall physical access system design, security professionals can implement the strongest possible security policies for any situation.

Smart cards are flexible, providing a migration path for which an organization’s requirements, not card technology, is the driving force. Multi-technology smart cards can support legacy access control technologies, as well as include new contact or contactless chip technology. When migration is planned carefully, organizations can implement new functionality, while accommodating legacy systems as may be required.

C) Identity Applications

Smart card technology is currently recognized as the most appropriate technology for identity applications that must meet critical security requirements, including:

1. Authenticating the bearer of an identity credential when used in conjunction with personal identification numbers (PINs) or biometric technologies
2. Protecting privacy
3. Increasing the security of an identity credential
4. Implementing identity management controls

D) Distributed System

As a distributed system increases in size, its capacity of computational resources increases. In a peer-to-peer system, all components of the system contribute some processing power and memory to a distributed computation.The very nature of an application may require the use of a communication network that connects several computers: for example, data produced in one physical location and required in another location.There are many cases in which the use of a single computer would be possible in principle, but the use of a distributed system is beneficial for practical reasons.

III. PROPOSED SYSTEM

The security of two password authenticated key agreement protocols using smart cards. While they were assumed to be secure, we showed that these protocols are flawed under their own assumptions respectively. In particular, we took into account some types of adversaries which were not considered in their designs, e.g., adversaries with pre computed data stored in the smart-card and adversaries with different data (with respect to different time slots) stored in thesmart-card. These adversaries represent the potential threats in distributed systems and are different from the commonly known ones, which we believe deserve the attention from both the academia and the industry. We also proposed the solutions to fix the security flaws. Once again, our results highlight the importance of elaborate security models and formal security analysis on the design of password-authenticated key agreement protocols using smart cards. Proposed System having different merits those are Improving high computation cost with pre-computation phase. Using session keyis used to establish a secure communication between the user and the server. Blocking from the common online-dictionary attack .Providing the counter measures to prevent the security threats and secure the protocols

A) Random Algorithm

To prove that the algorithm solves the problem correctly (always) and quickly (typically the number of steps should be polynomial in the size of the input). In addition to input algorithm takes a source of random numbers and makes random choices during execution

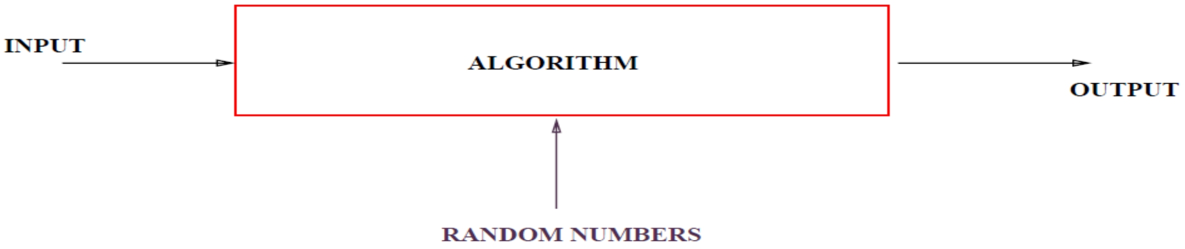

Figure 1: Random Algorithm diagram

If AB =C will always output AB = C ,If AB! = C will output AB =C with probability at most 1/|F|. Randomization and probabilistic analysis are themes that cut across many areas of computer science, including algorithm design, and when one thinks about random processes in the context of Computation, it is usually in one of two distinct ways. One view is to consider the world as behaving randomly one can consider traditional algorithms that confront randomly generated input. This approach is often termed *average-case analysis*, since we are studying the behavior of an algorithm on an “average” input (subject to some underlying random process), rather than a worst-case input. A second view is to consider algorithms that behave randomly: The world provides the same worst-case input as always, but we allow our algorithm to make random decisions as it processes the input. Thus the role of randomization in this approach is purely internal to the algorithm and does not require new assumptions about the nature of the input. It is this notion of a randomizedalgorithm. For many problems a randomized algorithm is the simplest the fastest or both.

IV. SYSTEM ARCHITECTURE

A) Login Phase

During this phase the user with identity IDi can login to the server with the smart card and the password the user and the server will authenticate each other and establish a session key is used to secure further communications between that user and the server the attacker can initiate a log-in request on behalf of the user, or act as the server by sending messages to the user. An active attacker can also request any session keys adaptively (if the protocol supports key agreement).

It is evident that an active attacker is more powerful than a passive attacker. On the other hand, smart-card-based password authentication provides two-factor authentication, namely something the user has: a valid smart card. Something the user knows: a correct password. Successful log-in requires a valid smart card and the correct password.

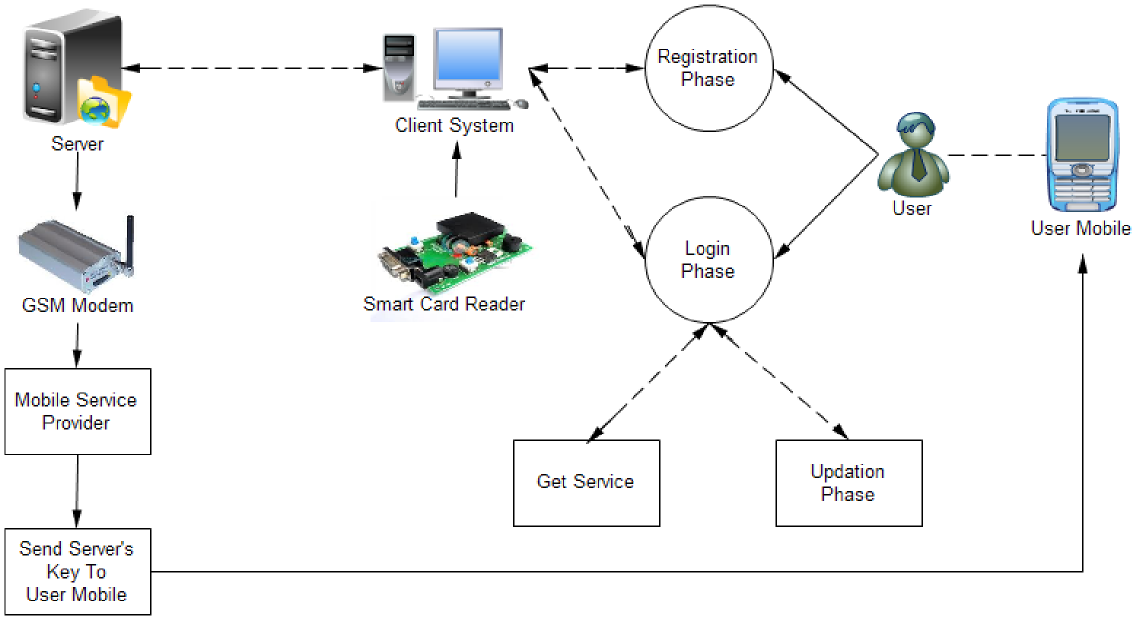

Figure2: System Architecture Diagram

B) Authentication Phase

This phase is invoked whenever the user U registers or reregisters to server we first show that a passive attacker with smart card can calculate the session key between the server and the user in the protocol At the end of the log-in phase, the session key between the user and the server It suffices to compute Sk with Vi, c, and u. are stored in the smart card before the log-in phase. The purpose of pre-computation is to speed up the computation in the authentication, which should be regarded as a separate phase from the log-in phase. Thus, to reduce the computational load in log-in phase in, the smart card must complete the calculation before the log-in phase, rather than performing the calculation. A smart-card-based password authentication protocol, the basic security requirement is that it should be secure against a passive attacker with smart card and a passive attacker with password. It is certainly more desirable that a smart-card-based password authentication protocol is secure against an active attacker with smart card and an active attacker with password.

A. User Authentication by a Security Server.

The user who needs to obtain access to resources connects to a trusted third party (security server) and provides authentication credentials, such as a username and a password. The server verifies the credentials and issues a ticket to the user. The ticket is signed and may be potentially encrypted by the security server so that the user cannot modify the content and may potentially not be able to read the content of the ticket.

B. Authentication to a Resource Server

Once the user has obtained a ticket, he can try to access a resource on the network. The user needs to present the ticket to the resource server. The resource server trusts the security server who issued the ticket to the user.

C. Code Verification

Intuitively, an attacker on a smart-card-based password authentication protocol should be unable to make a successful log-in only with the smart card (or the password), or compromise other additional properties (e.g., key agreement). To capture these requirements, we define the potential attacker from two aspects, namely the behavior of the attacker and the information compromised by the attacker. As an interactive protocol, a smart-card-based password authentication protocol may be faced with a passive attacker and an active attacker a passive attacker can obtain messages transmitted between users and the server. This is due to the fact that communication channels are generally insecure, and the attacker can observe messages by eavesdropping. A passive attacker cannot interact with any of the parties in smart-card-based password authentication protocols.

	Hwang & Li Scheme	Juang et al scheme	Fan et al scheme	Chien et al scheme	Juang scheme	Implementation
low communication and computation cost	X	A	A	A	A	A
no time-synchronization problem	X	A	X	X	A	A
utual authentication	X	A	A	A	A	A
identity protection	X	A	X	X	X	A
preventing offline dictionary attack	X	X	X	X	X	A

V. CONCLUSION

The security of two password-authenticated key agreement protocols using smart cards. While they were assumed to be secure, and these protocols are flawed under their own assumptions respectively. In particular, some types of adversaries which were not considered in their designs, e.g., adversaries with pre-computed data stored in the smart-card and adversaries with different data (with respect to different time slots) stored in the smart-card. These adversaries represent the potential threats in distributed systems and are different from the commonly known ones, which we believe deserve the attention from both the academia and the industry.Authenticated Key Exchange (AKE) protocols combined with One Time Password are proposed for wireless mobile networks that provide many security attributes in the distributed system. By implementing in the distributed system no other process has been implemented in as real-time and more efficiency when compared with Fan et al.'s protocol and Uang-Chen-Liaw's in the terms of communication costs and computational complexities.

REFERENCES

[1] AnamikaChouksey, Yogadhar Pandey "An Efficient password based Two-Server Authentication and Pre-shared Key Exchange System using Smart Cards" Int'l Prof Conf 2013.

[2] Chun-Ta Li, Cheng-Chi Lee "A Robust Remote User Authentication Scheme Using Smart Card" Int'l Conf Information Technology And Control, 2011.

[3] C.L. Hsu,"Security of Chien et al.'s "Remote User Authentication Scheme Using Smart Cards," Comput. Stand. Interfaces, vol. 26, no. 3, pp. 167-169, May 2004.

[4] C.-I. Fan, Y.-C. Chan, and Z.-K. Zhang, "Robust Remote Authentication Scheme with Smart Cards," Comput. Security, vol. 24, no. 8, pp. 619-628, Nov. 2005.

[5] Da-Zhi Sun, Jin-PengHuai, Ji-Zhou Sun, Jian-Xin Li, Jia-Wan Zhang "Improvements of Juang et al.'s Password-Authenticated Key Agreement Scheme Using Smart Cards" IEEE Transaction Industrial 2009.

[6] Debiao He, Jianhua Chen, and Jin Hu "Weaknesses of a Remote User Password Authentication Scheme Using Smart Card" Int'l of Network Security, 2011.

[7] Eun-Jun Yoon, Sung-Ho Kim and Kee-Young Yoo "A Security enhanced Remote User Authentication Scheme Using Smart Cards" Int'l Innovative Computing, 2012.

[8] H. Chien, J. Jan, and Y. Tseng, "An Efficient and Practical Solution to Remote Authentication: Smart Card," Comput. Security, vol. 21, no. 4, pp. 372-375, Aug. 2002.

[9] J. Xu, W.-T. Zhu, and D.-G. Feng, "An Improved Smart Card Based Password Authentication Scheme with Provable Security," Comput. Stand. Inter., vol. 31, no. 4, pp. 723-728, June 2009.

[10] Kai Chain, Wen-Chung Kuo and Jiin-Chiou Cheng "A Secure Password-Authenticated Key Agreement Using Smart Cards" Int'l Conf Hybrid Information Technology 2013.

[11] S.W. Lee, H.S. Kim, and K.Y. Yoo, "Improvement of Chien et al.'s Remote User Authentication Scheme Using Smart Cards," Comput. Stand. Interfaces, vol. 27, no. 2, pp. 181-183, Jan. 2005.

[12] Wen-Chung Kuo1, Kai Chain, Jiin-Chiou Cheng and Jar-Ferr Yang "An Enhanced Robust and Efficient Password-Authenticated Key Agreement Using Smart Cards" Int'l Security and Its Apps 2012.

[13] W.S. Juang, S.T. Chen, and H.T. Liaw, "Robust and Efficient Password Authenticated Key Agreement Using Smart Cards," IEEE Trans. Ind. Electron., vol. 55, no. 6, pp. 2551-2556, June 2008.