International Journal of Scientific Research and Modern Education (IJSRME)
ISSN (Online): 2455 – 5630
(www.rdmodernresearch.com) Volume I, Issue I, 2016

SMARTCAERD WITH TWO FACTOR PASSWORD AUTHENTICATION

R. Elayaraja* & A. Anitha**

* PG Scholar, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

** Assistant Professor, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

Abstract:

The password verification of smart card is the convenient of two factors. Thus the two factors are "dynamic ID-based" or "anonymous". The two factor anonymous scheme to prevent the user privacy, a common feature of these schemes is that their security is based on the tamper-resistance assumption about smart cards. The smart card may contain some public and sensitive security parameters. The secret information stored in the smart cards memory could be revealed by power analysis, reverse engineering techniques. The smart card verification is securely implemented on this method. The previous methods are stored the user information into the database that can be easily attack to the person. This technique has been widely deployed for various kinds of daily applications, such as e-banking, e-government and e-health and etc. Thus the methods have to maintain a sensitive password table on the server. The feature of no password-related table on the server is highly appealing when considering the unending catastrophic leakages of millions of user accounts in prominent service providers, and the prevalence of zero-day attacks. The user's identity is transmitted in plain text over public networks during the login process. A number of anonymous schemes based on non-tamper-resistance assumption about the smart cards are put forward, and each is claimed to meet a self-imposed list of ambitious design goals. a truly two-factor scheme can ensure is that, only the user who possesses both a valid smart card and the corresponding password can be successfully verified by the server.

Index Terms: Password, Two Factor Authentication & Smart Card

1. Introduction:

Network security consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. . Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. 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 way of protecting a network resource is by assigning it a unique name and a corresponding password.

The Password authentication with smart card is one of the most convenient and effective two-factor authentication mechanisms in distributed systems. Although this technique has been widely deployed for various kinds of daily applications, such as e-banking, e-government and e-health, there are severe challenges regarding security,

privacy and usability due to the open and complex nature of distributed systems, as well as the resource constrained characteristics of mobile devices. In the first smartcard- based password authentication scheme without a sensitive verification table stored on the server, which is a key advantage of two-factor schemes over common password-only schemes, for the latter have to maintain a sensitive password (or salted password) table on the server

The feature of no password-related table on the server is highly appealing when considering the unending catastrophic leakages of millions of user accounts in prominent service providers and the prevalence of zero-day attacks like the recent "Heart bleed". In most of the previous two-factor schemes, user's identity is transmitted in plaintext over public networks during the login process, which may leak the identity of the logging user once the login transcripts are eavesdropped, resulting in violation of user privacy and raising legal issues in some scenarios, e.g., electronic auditing or secret online-order placement. In many cases, an attacker may exploit the static user identity to link different login sessions together to trace user activities. For example, in e-commerce applications, once user activities are traced, the sensitive information such as shopping patterns, individual preferences, even age and gender, etc., can be learned and abused for marketing purposes, typically facilitating annoying advertisement flooding. What's more, the disclosure of user identity and activities may also facilitate an unauthorized entity to trace the user's login history and even current location. To address such static-user-ID-related issues, a feasible approach is to adopt the "dynamic ID technique": the user's real identity is concealed in session-variant pseudo-identities. And two factor schemes employing this technique are known as "dynamic ID-based" or "anonymous" ones.

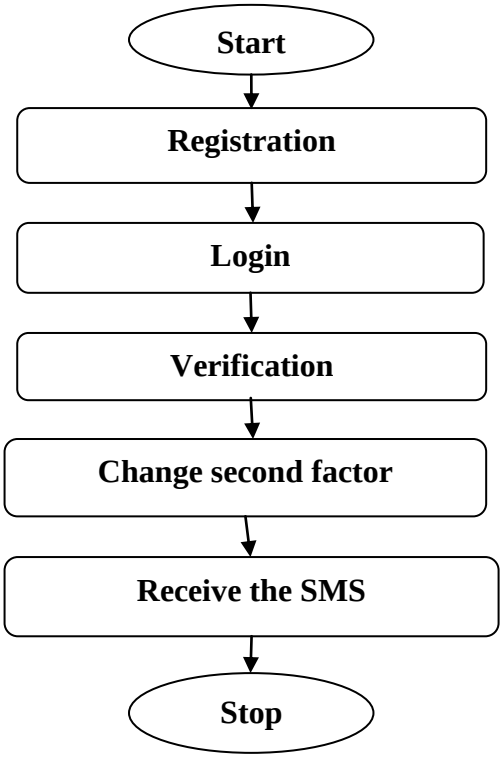

Figure 2: System Flow Diagram

The reminder of this paper is organized as follows. Section II, describes the Related Works. Section III, describes the Proposed Work. Section IV, describes the

Experimental Evaluation and Results. Section V summarizes the Conclusion and Future Enhancement.

2. Related Works:

Official Gates is a leading global IT solutions provider that enables your business grows with the use of cutting-edge technology in online applications. Established with the objective of providing precise, user-friendly and cost-effective IT solutions of unsurpassing quality, OG has carved a niche for itself in the field for providing software solutions that help increase the productivity and operational efficiency of our clients.

Official Gates is an ISO 9001:2008 Certified Company has over 8+ years of experience in providing Software Development, Web Application Development, E-Commerce Development , Payment Gateway Integration Services , PHP Web Application Development , Open Source Customization ,Online Shopping Cart Development , Content Management Systems ,Web Development, Mobile Application Development, Android Application Development, Iphone Application Development , BlackBerry Application Development ,Windows Application Development ,HTML5 Application Development ,Phone Gap Development and Web Designing for off shoring / outsourcing services to its various clients in the India, Australia, US, UK, Europe, Germany, Netherland , Norway, Canada, Japan, Singapore, Malaysia, Italy, Asia and Middle East region. Official Gates is specializes in providing a wide array of IT services to customers worldwide. Official Gates has a state-of-the-art offshore development facility in Chennai, Tamilnadu, India with a global team of growing professionals, Official Gates continuously endeavors to exceed customer expectations in all engagements with an optimal mix of technical strength and execution capability, while ensuring high employee morale.

OG is a unique Offshore Development Company that specializes in providing customized online applications. We cater to a multitude of industries including, B2B / B2C Ecommerce Portals, Social Networks and Communities, Enterprise Intranets/ Extranets, Content Management Systems, Digital Media Distribution, Electronic Communication, Workflow Automation, Customer Relationship Management, Supply Chain Management, Collaborative Tools, Knowledge Management, Document Management, Ecommerce & E-Business, Mass Media, Real Estate, Travel and Entertainment, IT Managed Services, Education, Software Publishing, Advertising, Finance, Healthcare, Telecommunications, As a leading IT solution provider, we deliver an extensive range of services of matchless quality at an amazingly affordable cost including The right blend of resources- technical, financial and human - coupled with a keen understanding of global market trends and needs make OG a unique Offshore Development Company that offers reliable and consistent IT solutions which exceeds the expectations of our clients. A technically strong team, committed to the mission of emerging as an unrivaled leader among IT solution providers, is at the helm of affairs in OG. We also take pride in the fact that the domain expertise of our personnel, especially in PHP, MySQL, AJAX and JavaScript, DOT Net, Mobile Applications and their technical know-how in the fields of B2B / B2C Ecommerce Portals, Social Networks and Communities, Enterprise Intranets/ Extranets, Content Management Systems, Digital Media Distribution, Electronic Communication, Workflow Automation, Customer Relationship Management, Supply Chain Management, Collaborative Tools, Knowledge Management, Document Management, Ecommerce & E-Business, Mass Media, Real Estate, Travel and Entertainment, IT Managed Services, Education, Software Publishing, Advertising, Finance, Healthcare, Telecommunications, has placed us in the forefront of IT solution providers. Added to this is their exposure to global culture, which sets OG apart from others as a peerless Offshore Development Company. OG also enjoys a wide

global presence. The user-friendly online applications facilitate easy accessibility from any part of the world, making OG a truly global IT solution provider. Moreover, with us offering services 24/7, our clients can reach us any time - for neither distance nor time, only quality matters to us.

3. Proposed Work:

The proposed system is challenge to design a practical anonymous two-factor authentication scheme. Numerous solutions have been proposed, yet most of them are shortly found either unable to satisfy some critical security requirements or short of a few important features. The password authentication system is one of the most convenient and effective of two factor authentication mechanisms in distributed systems. The most general case of smart-card-based password authentication in which the participants involve a set of users and a single remote server. The first smartcard-based password authentication scheme without a sensitive verification table stored on the server, which is a key advantage of two-factor schemes over common password-only schemes, for the latter to maintain a sensitive password table on the server. Once this table is leaked, the entire system collapses. The feature of no password-related table on the server is highly appealing when considering the unending catastrophic leakages of millions of user accounts in prominent service providers. This process has to be developed a new set of design goals for fairly evaluating this type of schemes. It mainly deals with security threats and challenges in two-factor authentication and leaves over another Interesting open problem as to "whether or not there exist secure smart-card-based password authentication protocols and the password-changing phase does not need any interaction with the server. The users have some changes of the smart cart registration, authentication and password change, as well as some supplementary phases like eviction and revocation. In the registration phase, a user submits some personal information to the server, and the server issues a smart card to the user. The smart card may contain some public and sensitive security parameters, which will be used later for the authentication. This phase is carried out only once unless the user re-registers. Thus the method has to be securing the user data, and secure verification of the login to the account in the smart cart process.

Enrollment: The first module is a registration phase. Thus the phase can be registering the user details into the database. The details are name, username, password, age, gender, and etc. thus details are very sensitive, it is stored on the server. More users are accessing the same login phase so create the password on unique for each member. Thus the password is using to identify the user certification process. The registration process has to be allocating the access control of the server page. All the registered users have been login to the page.

Factor Verification: The login page is used for logging in the site authenticate person allows for existing user. The user must be entering the first factor correctly. And enter the second factor then login to the account. The two-factor protocol achieving semantic security or the so-called "AKE security" under the non-tamper resistance assumption about the smart card can provide a basic level of security, such as resistance to impersonation attack and offline password guessing attack, even if the card has been lost and breached. The general rationale that lies behind a proof of semantic security in ROM is: (1) Modeling any hash functions as an oracle which outputs a random value for each new query and the same value for every identical query; (2) Supposing A can break the semantic security of the target protocol P.

Change the Factor: The user can be login to the account and then change the second factor automatically. The changed password is send to the user mobile number. The

factor is generated on random process on the admin side. The attacker (A) is generally assumed to be able to eavesdrop, block, alter or insert messages exchanged between the communicating parties in the full control of communication channel. The secret key may be also learnt by A due to the variety of reasons like improper erasure. To capture the notion of forward secrecy, A may also be allowed to corrupt legitimate parties to learn long-term secrets. The secret data stored in the smart card, which was once believed to be free from breach, could be extracted by state-of-the art side-channel attacks. In addition, malicious card readers also contribute to the security failures of such schemes. A user input password may be easily intercepted by the malicious card reader. The attacker is unlikely to extract the secret information stored in the card while intercepting a user input password through malicious card readers, for the victim is on the scene and the little chances for A to perform abnormal operations such as side-channel attacks. The smart card is sufficiently tamper-resistant such that the cost of attack is prohibitively high for an attacker; it is trivial to design an "ideal" scheme. It is practical to assume that a determined attacker can somehow know the user identity. When having obtained the user card. Firstly, user's identity is static and generally confined to a predefined structure, and thus it is of little cryptographic strength and can be easily guessed. Secondly, it probably can be harvested from popular forums and other open resources. The previous password has to be changed and the transferred to the user mobile phone.

Verification: The user is login to the account on next time using the normal first factor and the second factor is modified password. Thus the password is referred from the user mobile phone. And thus the password has to be used to the next login process.

4. Experimental Analysis and Results:

Implementation is the process of translating design specification in to source code. The primary goal of implementation is to write source code and internal implementation. So that conformance of code to its specification can be easily verified, So that debugging, testing and modification are eased. The source is developed with clarity, simplicity and elegance.

The coding is done in a modular fashion giving such importance even to the minute detail so, when hardware and storage procedures are changed or now data is added, rewriting of application programs is not necessary. To adapt or perfect use must determine new requirements, redesign generate code and test exiting software/hardware. Traditionally such task when they are applied to an existing program has been called maintenance.

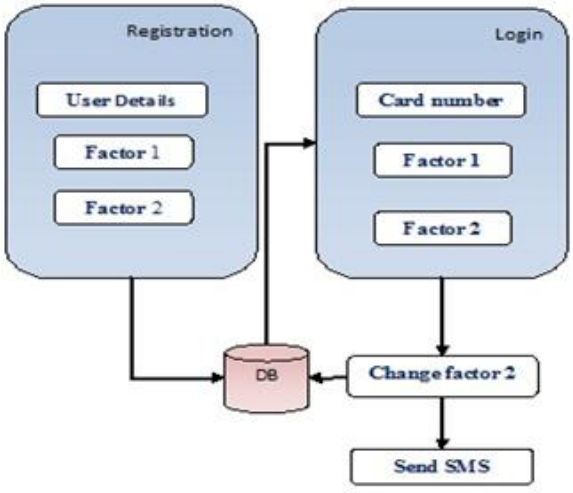

Figure 2: Architecture of two factor authentication

5. Conclusion and Future Enhancement:

The anonymous two-factor schemes as case studies; we uncover several subtleties and challenges in designing this type of schemes, and explore the relationships among the criteria. Our results highly indicate a negative answer to the examined question. Most essentially, we find that, a scheme supporting local user password change is unlikely to achieve "SR6: resistance to smart card loss attack", while a scheme not supporting local user password change is unlikely to provide the property of "DA10: timely typo detection". This presents an unavoidable usability security tradeoff, thereby also suggesting a negative answer to the open question raised. We believe this work provides a better understanding of the underlying evaluation metric for anonymous two factor schemes, which is of fundamental importance for security engineers to make their choices correctly and for protocol designers to develop practical schemes with better usability-security tradeoffs. We leave for future work the question of evaluating practical effectiveness of the proposed "fuzzy-verifiers" by using recently disclosed large-scale real-life password data-sets like the 50 million "Ever note" dataset and the 6.4 million "LinkedIn" dataset.

6. References:

1. M. Bond, O. Choudary, and S. Murdoch, "Chip and skim: cloning EMV cards with the pre-play attack," in Proc. IEEE S&P 2014. IEEE Computer Society, 2014, pp. 1–15.
2. D. Wang and P. Wang, "On the anonymity of two-factor authentication schemes for wireless sensor networks: Attacks, principle and solutions," Comput. Netw., 2014, doi: 10.1016/j.comnet.2014.07.010.
3. N. Gunson, D. Marshall, H. Morton, and M. Jack, "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking," Comput. Secur., vol. 30, no. 4, pp. 208–220, 2011.
4. W.-H. Yang and S.-P. Shieh, "Password authentication schemes with smart cards," Comput. Secur., vol. 18, no. 8, pp. 727–733, 1999.
5. M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in Proc. EUROCRYPT 2000, ser. LNCS, B. Preneel, Ed. Springer/Berlin Heidelberg, 2000, vol. 1807, pp. 139–155.
6. J. Katz, R. Ostrovsky, and M. Yung, "Efficient and secure authenticated key exchange using weak passwords," J. ACM, vol. 57, no. 1, pp. 1–41, 2009.
7. X. Li, W. Qiu, D. Zheng, K. F. Chen, and J. Li, "Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards," IEEE Trans. Ind. Electron., vol. 57, no. 2, pp. 793–800, 2010.
8. X. Huang, Y. Xiang, A. Chonka, J. Zhou, and R. H. Deng, "A generic framework for three-factor authentication: Preserving security and privacy in distributed systems," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 8, pp. 1390–1397, 2011.
9. Y. G. Wang, "Password protected smart card and memory stick authentication against off-line dictionary attacks," in Proc. SEC 2012, ser. IFIP AICT, D. Gritzalis, S. Furnell, and M. Theoharidou, Eds. Springer Boston, 2012, vol. 376, pp. 489–500.
10. Y. Wang, J. Liu, F. Xiao, and J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme," Comput. Commun., vol. 32, no. 4, pp. 583–585, 2009.
11. M. Khan and S. Kim, "Cryptanalysis and security enhancement of a more efficient & secure dynamic ID-based remote user authentication scheme'," Comput. Commun., vol. 34, no. 3, pp. 305–309, 2011.