Nagaram Pradeep Kumar Goud* et al.
(IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH
Volume No.4, Issue No.4, June – July 2016, 3406 – 3408.

A Robust Primitive for Avoiding Data Attacks Using Cryptography

NAGARAM PRADEEP KUMAR GOUD
M.Tech Student, Dept of ECE
DVR College of Engineering and Technology
Hyderabad, T.S, India

P.RAMESH REDDY
Assistant Professor, Dept of ECE
DVR College of Engineering and Technology
Hyderabad, T.S, India

Abstract: **Within our plan, a session secret is only accessible towards the interacting parties (user and server), which is unknown either to the registration center varieties. Within this paper, we first evaluate He-Wang's plan and reveal that their plan is susceptible to a known session specific temporary information attack and impersonation attack. Additionally, we reveal that their plan doesn't provide strong user's anonymity. In addition, He-Wang's plan cannot supply the user revocation facility once the wise card sheds or taken or user's authentication parameter is revealed. While using Burrows-Abadi-Needham logic, we reveal that our plan provides secure authentication. Additionally, we simulate our plan for that formal security verification while using broadly recognized and used automated validation of Internet security software methods and programs tool, and reveal that our plan is safe against passive and active attacks. Our plan provides high security together with low communication cost, computational cost, and number of security measures. Aside from these, He-Wang's plan has some design flaws, for example wrong password login and it is effects and wrong password update during password change phase. Then we propose a brand new secure multi-server authentication protocol using biometric-based wise card and ECC with increased security benefits. Consequently, our plan is extremely appropriate for battery-limited mobile products as in comparison with He-Wang's plan.**

Keywords: **Smart Card, BAN Logic, Security, Authentication, Revocation And Re-Registration.**

I. INTRODUCTION

The consumer revocation and re-registration with similar identity could cause the consumer impersonation attack, when an authentication plan distributes the static secret tokens. It helps to ensure that an authentication plan must supply the secure mutual authentication with the existence of the shared secret credentials. Using the rapid growth and development of the wireless communication systems and e-commerce programs, for example e-banking and transaction-oriented services, there's an increasing demand to safeguard the consumer credentials privacy [1]. Thus, the authentication methods end up being the reliable components inside a communication system. Within the recent handful of decades, increasingly more transactions for that mobile products happen to be implemented on the web or wireless systems because of the portability property of mobile products, for example laptops, wise cards and wise phones. To be able to safeguard the sensitive information against a malicious foe, a number of security services for example mutual authentication, user credentials privacy and SK-security have to be considered. We think about the following two real-existence situations for that wise card based authentication schemes where the registered customers may revoke and re-register with similar identity: (i) when suddenly the key token of the legal user is revealed and (ii) when the wise card of the legal user is stolen or lost. Hence, the authentication schemes must offer the user revocation and re-registration with similar identity [2]. Therefore, creating a competent method of tackle the issue of user revocation while supporting strong user traceability has turns into a challenging problem. Consequently, the consumer revocation and re-registration with similar identity is recognized as fundamental security functionality for that wise card-based authentication schemes. Hence, the foe A can see, modify or delete all of the authentic messages sent between customers and server. Additionally, A can have the secret information through the session exposure attacks. Thus, an authentication plan should fulfill the following security qualities. An authentication plan should ensure the security from the session key, known as the session key security (SK-security), within the following two cases: (i) the leakage of the session key or session-specific temporary information may have no effects around the security of other sessions. (ii) The leakage from the crucial lengthy-term secrets, like the private keys of customers or servers that are used over the multiple sessions won't always compromise the key information all past sessions, referred to as perfect forward secrecy. It helps to ensure that A cannot derive a person credentials, for example authentication parameter, user password and identity. Within our plan, a session secret is only accessible towards the interacting parties (user and server), which is unknown either to the registration center varieties. Provides user credentials privacy even when the session-specific temporary information is suddenly leaked. But the majority of the existing schemes don't provide credentials

privacy such as the lately suggested He-Wang's plan. It offers the SK-security, whereas He-Wang's plan has lots of drawbacks once the session temporary information are leaked towards the foe. Our plan efficiently props up password change phase. However, He-Wang's plan has some. The registration center RC stores the consumer identity information to prevent many customers to join up with similar identity and therefore, our plan prevents the numerous recorded-in customers attack.

II. PREVIOUS WORK

Yoon and Yoo suggested a multi-serve authentication plan while using biometrics-based wise card and ECC. Several two-party authentication schemes happen to be suggested within the literature. In one-server atmosphere, a person must register with every server individually. However, it's impossible to directly apply two-party authentication techniques devised for any single server atmosphere to some multi-server atmosphere. Further, they suggested a superior plan to be able to withstand the safety flaw present in Yoon-Yoo's plan. Lately, He and Wang suggested a strong biometrics-based authentication plan for multi-server atmosphere to be able to withstand these security issues, and stated their plan is safe against all possible known attacks. However, within this paper, we reveal that He-Wang's plan does not prevent known session temporary information attack, and for that reason, their plan cannot avoid the reply attack and impersonation attack. Additionally, we reveal that their plan cannot supply the strong user anonymity. Within this paper, we advise a manuscript and secure biometrics-based multi-server authentication mechanism using ECC for those battery-limited products. Our contributions within this paper are outlined below. Within our plan, a session secret is only accessible towards the interacting parties which are unknown either to the registration center varieties [3]. Our plan provides user credentials privacy even when the session-specific temporary information is suddenly leaked. But the majority of the existing schemes don't provide credentials privacy such as the lately suggested He-Wang's plan and offers the SK-security, whereas He-Wang's plan has lots of drawbacks once the session temporary information are leaked towards the foe. Our plan efficiently props up password change phase. However, He-Wang's plan has some design flaws, for example wrong password login and it is effects and wrong password update during password change phase. Within our plan, the registration center (RC) authenticates the consumer and server individually whenever they would like to establish the session key. However, in He-Wang's plan, the RC cannot find out the user and also the server individually. Thus, in He-Wang's plan, a legitimate malicious server may behave as a legitimate user and relish the services in the other servers. Our plan efficiently props up fundamental security property from the revocation and re-registration with similar identity because of the use of random number in computation of authentication parameter of the legal user [4]. Within our plan, the registration center RC stores the consumer identity information to prevent many customers to join up with similar identity and therefore, our plan prevents the numerous recorded-in customers attack. Our plan provides high security plus a number of features as in comparison to He-Wang's plan. Therefore, our plan is extremely appropriate for those battery-limited mobile products because the ECC is much more efficient for that battery limited products.

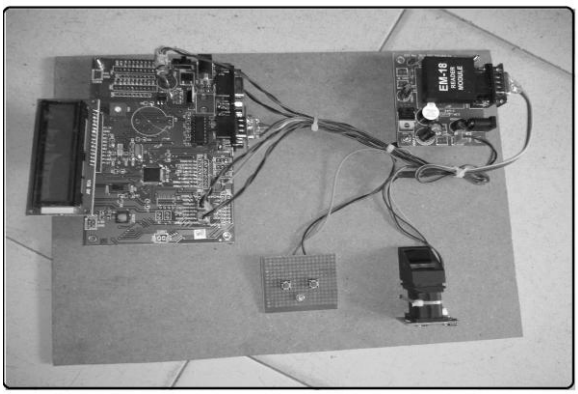

Fig.1.Proposed System

III. THE PROPOSED SCHEME

In Initialization Phase, the registration center chooses a non-singular elliptic curve on the finite filed. In Registration Phase, to prevent a brand new user registration using the existing legal user identity, we make use of an identity verifier table, say T. In Server Registration Phase, a web server selects his/her unique identity and transmits the registration request to RC using a secure funnel. After receiving this request, RC inspections if the hash value matches with any of the records within the identity-verifier table T. Whether it matches, RC rejects the request by proclaiming it as being invalid. Otherwise, RC at random creates several and computes. User Registration Phase, Think that the wise card continues to be pre-configured with public parameters Login Phase. In Authentication and Key Establishment Phase, both Ui and Sj execute the steps to mutually authenticate one another and agree with a session type in to communicate over insecure public channels later. We advise a brand new biometrics-based multiserver authentication protocol using wise card and ECC, which withstands the safety pitfalls of He-Wang's plan. Our plan includes the six phases, namely, initialization phase, registration phase, login phase, authentication and key agreement

phase, password change phase, and revocation and re-registration phase. In Password Change Phase, Ui can alter his/her password without further contacting the RC [5]. In Revocation and Re-Registration Phase, we explain the consumer revocation and re-registration with similar identity when his/her authentication secret is compromised or even the wise-card shedsOrtaken. We evaluate our plan while using broadly-recognized BAN logic and reveal that our suggested plan provides secure authentication. Next we discuss informally the potential attacks on the plan.

IV. CONCLUSION

Our plan thus provides high security together with low communication cost, computational cost, while offering a number of features. Also, we've shown the drawbacks in He-Wang's plan while disbursing the static authentication parameters along with the wrong password entry. Within this paper, we've first reviewed the lately suggested He-Wang's plan after which proven their plan is susceptible to the known session-specific temporary information attack and therefore, their plan does not prevent reply attack and can't provide strong user anonymity. To resist these drawbacks, we've suggested a manuscript and efficient multi-server authentication protocol using biometric-based wise card and ECC. We've proven our plan is safe and offers more functionality as in comparison to He-Wang's plan. While using BAN logic, we've demonstrated our plan provides secure authentication with the formal security analysis. Additionally, with the informal security analysis, we've proven our plan is safe against various known attacks. Consequently, our plan is especially appropriate for battery-limited mobile products. We've further simulated our plan for that formal security verification while using broadly-recognized AVISPA tool, and proven our plan is safe. We've proven the functionality analysis in our plan with He-Wang's plan. It's observed our plan outperforms as in comparison to He-Wang's plan as our plan supports additional features listed and it is safer than He-Wang's plan. Consequently, our plan is a lot appropriate for practical programs as in comparison towards the lately suggested He-Wang's plan.

V. REFERENCES

[1] E. Brickell and J. Li, "Enhanced privacy ID: A direct anonymous attestation scheme with enhanced revocation capabilities," IEEE Trans. Dependable Secure Compute., vol. 9, no. 3, pp. 345–360, May/Jun. 2012.

[2] L.-H. Li, I.-C. Lin, and M.-S. Hwang, "A remote password authentication scheme for multiserver architecture using neural networks," IEEE Trans. Neural Netw., vol. 12, no. 6, pp. 1498–1504, Nov. 2001.

[3] S. Wu, Y. Zhu, and Q. Pu, "Robust smart-cards-based user authentication scheme with user anonymity," Secur. Commun. Netw., vol. 5, no. 2, pp. 236–248, 2012.

[4] D. He and D. Wang, "Robust biometrics-based authentication scheme for multiserver environment," IEEE Syst. J., to be published.

[5] R.-C. Wang, W.-S. Juang, and C.-L. Lei, "User authentication scheme with privacy-preservation for multi-server environment," IEEE Commun. Lett., vol. 13, no. 2, pp. 157–159, Feb. 2009.

AUTHOR's PROFILE

Nagaram Pradeep Kumar goud received his b.tech

in S V college of engineering and technology moinabad ,ranga reddy district,telangana in 2012.He is currently a m tech candidate at DVR college of engineering.His current research interests include embedded system design , security,crypotography and additionally hands on experience in hardware design.

P.Ramesh Reddy received the M.Tech. degree in

VLSI from TRR college of engineering, Hyderabad, India, in 2012. He is currently an Assistant Professor in DVR college of engineering. He has authored 4 papers in international journals and conferences. His interests include Ph.D. in VLSI.

