RESEARCH ARTICLE OPEN ACCESS

Anonymous Two-Factor Authentication in Distributed Systems

Ashwani Vijayachandran [1], Kiran G Kumar [2]
Student [1], Professor [2]
Department of Computer Engineering
GISAT, Mahathma Gandhi University, Kottayam
Kerala -India

ABSTRACT
Two factor authentication or 2FA is a security process in which the user firstly authenticate with a physical token and then with the PIN number. This two-factor authentication is very secure one because when someone access our computer it very difficult. Two factor authentication is also known as Multi-Factor authentication which means an extra layer security. Currently authentication using smart card is common for mostly in banking .For more security each banking transaction like online banking must hold two-factor authentication. One of the main security mechanism is to ensure the identity of the client whether the user is legitimate or not. If the valid user has a smart card for authentication then it contains a valid user id and password then he can successfully login to the server. Proposed system gives more security for banking transactions and give a great barrier to the attackers. Proposed system will give more privacy, security and usability for the users.

Keywords-Two-factor authentication, Smart Card based authentication, Physical token, External security .

I. INTRODUCTION

With the quick development of wireless network technologies and micro-electronic transactions like online-banking, online shopping, online-voting, Pay-tv etc are processed through PDAs, laptop, mobile phones etc. Through this we can access these service anywhere at any time from different parts of the world. Using this users can be authenticated by the server and protected from attempting of unauthorized access against the services. As the name of the topic implies two factor authentication means two levels of security which means a user who has a valid smart card and password can successfully verified by the remote server. A smart card based authentication gives more security than all other methods because the smart cards contains the user name and password but it is only known by the valid user .All the users with valid smart card can access these services at anytime from anywhere from the world. In this smart based password authentication mechanism the main advantage is that it will give more security and users can use the banking transactions at any time**.**

Now a days smart card based password authentication is common mostly in the applications like e-banking,e-governance and e-health. Password authentication with smart card is one of the most suitable and effective two-factor authentication mechanisms in distributed networks, and it assures the identity and authenticity of one communicating party of the authenticity and identity of the nearby party by acquisition of supporting evidence. Although this technique has been widely used for various kinds of daily applications like e-banking, e-government and e-health, there are great objection regarding security, privacy and usability due to the open and difficult nature of distributed systems, as well as the resource-constrained characteristics of mobile devices.

II. RELATED WORKS

Smart card based authentication is now common for different online transactions. This type of authentication has more security than any other schemes. But there are many researches have been demonstrated for increasing the security .But early there are some related works are based on this scheme that are as follows.

At the early days the users simply store their password in the database ,But there is no such security for password and an attacker can easily attack the password that simply stored on the database.In 1999,Yang and Sheih introduced the first smart-card based two factor authentication schemes but the key advantage is that there is not a sensitive verification table stored on the server. But in case of password only schemes they contains a sensitive verification table is stored on the server for storing all the password details. But the disadvantage of this table is that once if the table is leaked then the entire system will damaged .Due to this millions of

users accounts has been leaked and also their secret data's and identity. Zero day attacks like recently happened security bug called "Heartbleed".

Yang and Sheih also introduced two-factor authentication schemes ,but it has certain problems such as user's identity is passed in plain text over the public network After the login process the user's identity may leak when logging process happened. It is the great violation against the user's privacy and data security. For example In e-commerce applications mainly like online purchasing the other user activities such as shopping patterns, about their account details and even their gender and age details are monitored .It is because of the users static identity the attacker can trace all the activities and even he knows the current location of the user. And the attackers may use this information for many purposes the main thing is to use this details abused for marketing purposes. These all problems are happening because of the static-user-ID-related issues and better choose "dynamic ID technique" or "anonymous".In 2004,Das has to be introduced that first anonymous two-factor authentication scheme mainly to protect the user's privacy and security .Das has been introduced different levels of security and different types attributes are also introduces for this two-factor authentication. Mainly Das's scheme is based on the security based on tamper-resistance assumptions based on the smart card .Then they think that the security components that stored on the smart card should not be extracted. But now a day's recent researches have shown that the secret information that stored in the smart card memory can be revealed by some important techniques such as power analysis, reverse engineering techniques or fault injection techniques.

III. PROPOSED SYSTEM

The Proposed System mainly focus on smart card based two-factor authentication. Smart card has an important role in this scheme .Because the main security component is this smart card in which this smart card contains a valid user Id and a password used for registration. Mainly focus on smart card based two-factor authentication in which it contains a set of users and a remote server. Mainly this scheme has to be followed by 3 steps such as registration, authentication and password change, as well as two supplementary phases like eviction and revocation. In registration phase user submit his personal information to the server then the server issues a smart card to the user .Smart card contains main important public and sensitive security parameter in which these information are further used for later authentication. But this phase is performed once if otherwise the users will re-register. During the registration phase, user can be able to access the server in the authentication phase. This can be performed for many times as the user needed. In truly the two-factor authentication scheme ensure that only the user who has a valid smart card and the genuine password can only be successfully verified by the server. But in password change phase the user can update his password and also he can update all the details by interacting with the server .There are 2 different phases are also used because when the malicious attack or revocation of lost card can be admired used by the phases eviction and revocation.

ALGORITHM - ANONYMOUS TWO-FACTOR AUTHENTICATION

Initialization:

Step 1: Two peer servers S1 and S2 jointly choose a secure hash function H, which maps a message of arbitrary length. S1 randomly chooses an integer and S2 randomly chooses an integer, and S1 and S2 exchange key.

Registration phase

Step 2: User Ui select her identity IDi, password PWi and a random number b.

Step 3: User Ui send Server ⇒ S : {IDi; h(PWi‖b)}.

Step 4: Upon receiving the registration message from user Ui, the server S computes a secret key V = h(IDi‖x) ⊕ h(PWi‖b).

Step 5: Server S send User ⇒ Ui: A security parameter V .

Step 6: Upon receiving V, Ui and server establish a secure connection after verifying keys.

Authentication phase

Step 7: When user Ui wants to access S, Ui retrieves h(IDi‖x) by computing h(IDi‖x) = V ⊕h(PWi‖b), selects a random number and send to server S.

Step 8: S retrieves IDi and h(IDi‖x) by computing IDi‖(h(IDi‖x)

Step 9: Server S authenticates User Ui and provides a session key $S_{k,}$

Step 10: A secure and anonymous communication channel is established using S_k.

There are different modules according to the 2 factor authentication scheme that are as follows:

A.Server intialization

The two servers S1 and S2 jointly choose a cyclic group **G** of large prime order q with a generator g1 and a secure hash function H, which shares a secret key between two server. Initialization process includes i.e. registration, authentication and password change. The server is registered, authenticated with a key and exchange the key between two server is done.

B.Client registration

Prior to authentication, each client C is required to register server through secure channels. The client gives smartcard identity and password for registration. Through a secure channel client shares password with server. After that, the client C should remember the password pwC only.

SYSTEM ARCHITECTURE

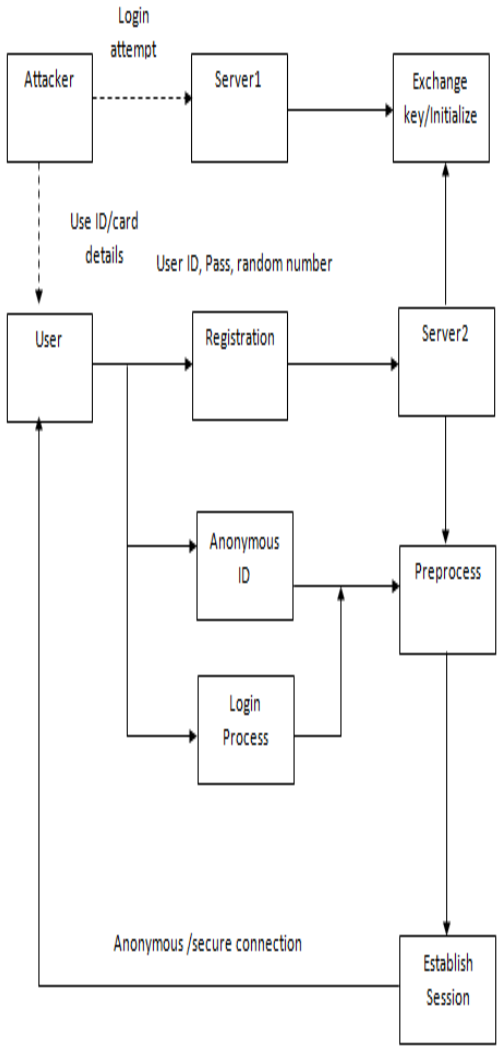

Fig. 1 System architecture

C.Client authentication and key exchange

During the registration the two servers S1 and S2 have received the password authentication information of a client C. The two servers S1 and S2 to authenticate the client C and establish secret session keys with the client C in terms of parallel computation. The client C randomly chooses an integer r value and q value using Diffie Helman key change.

D.Transaction processing

After authenticating the servers, client can handle a safe communication channel between servers. Client a give a query 'Q' requests to Server. Server upon receiving session key from the client, it will establish a communication channel and process the query and look into its database and reply the client.

E.Attacker model

Adversary A, who has compromised the server S2 and is able to play the role of S2 and monitor all communications between S1 and C, attempts to understand the secret session key established between the server S1 and the client C. The client session key value is checked by the servers and identify the attacker, if any found.

IV.CONCLUSION

An "ideal" anonymous two-factor authentication scheme is proposed. By cryptanalyzing two foremost 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. Results highly indicate a negative answer to the examined question. 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.

ACKNOWLEDGEMENT

It is with great pleasure that we acknowledge the enormous assistance excellent co-operation extended to by the following respected personalities. Firstly we would like to express our sincere thanks to our respected Principal of GISAT, Kottayam for providing us the necessary infrastructure, laboratories and requirement. We would like to express our sincere thanks to our respected Guide Prof. Kiran G Kumar., for his valuable guidance

REFERENCES

[1] About EMV (Europay, MasterCard, and Visa), EMVCo Ltd.,Sep.2013,available at http://www.emvco.com/approvals.aspx?id=91.

[2] P. Sean, LinkedIn Passwords Leaked Online: Hackers are beginning to decrypt 6.4 million passwords, June 6 2012, available at http://www.webpronews.com/linked in-passwords-leaked-online-2012-06.

[3] 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.

[4] M. Khan and S. Kim, "Cryptanalysis and security enhancement of a more efficient & secure dynamic ID-based remote user authentication scheme'," *Computer. Communication.*, vol. 34, no. 3, pp. 305–309, 2011.

[5] S. H. Wu, Y. F. Zhu, and Q. Pu, "Robust smart-cards-based user authentication scheme with user anonymity," *Secure. Communication .Network* .,vol. 5, no. 2, pp. 236–248, 2012.

[6] S. Kumari and M. K. Khan, "More secure smart card-based remote user password authentication scheme with user anonymity," *Secure. Communication. Network*., 2013, doi: http://dx.doi.org/10.1002/sec.916.

[7] R. Elayaraja and A. Anitha "SMARTCAERD WITH TWO FACTOR PASSWORD AUTHENTICATION", International Journal of Scientific Research and Modern Education (IJSRME), Volume I, Issue I, 2016.