Vol 5 Issue 5 Nov 2015 ISSN No :2231-5063

International Multidisciplinary Research Journal

# Golden Research Thoughts

**Welcome to GRT**

**RNI MAHMUL/2011/38595** **ISSN No.2231-5063**

Golden Research Thoughts Journal is a multidisciplinary research journal, published monthly in English, Hindi & Marathi Language. All research papers submitted to the journal will be double - blind peer reviewed referred by members of the editorial board.Readers will include investigator in universities, research institutes government and industry with research interest in the general subjects.

## *International Advisory Board*



## *Editorial Board*



**Address:-Ashok Yakkaldevi 258/34, Raviwar Peth, Solapur - 413 005 Maharashtra, India**
**Cell : 9595 359 435, Ph No: 02172372010 Email: ayisrj@yahoo.in Website: www.aygrt.isrj.org**

Golden Research Thoughts
ISSN 2231-5063

Impact Factor : 3.4052(UIF)
Volume - 5 | Issue - 5 | Nov - 2015

# PASSWORD AUTHENTICATION SCHEME USING SMART CARD AUTHENTICATION

Sumit Chaudhary , Ravi Dhaundiyal , Jainendra Singh Rana

ABSTRACT:

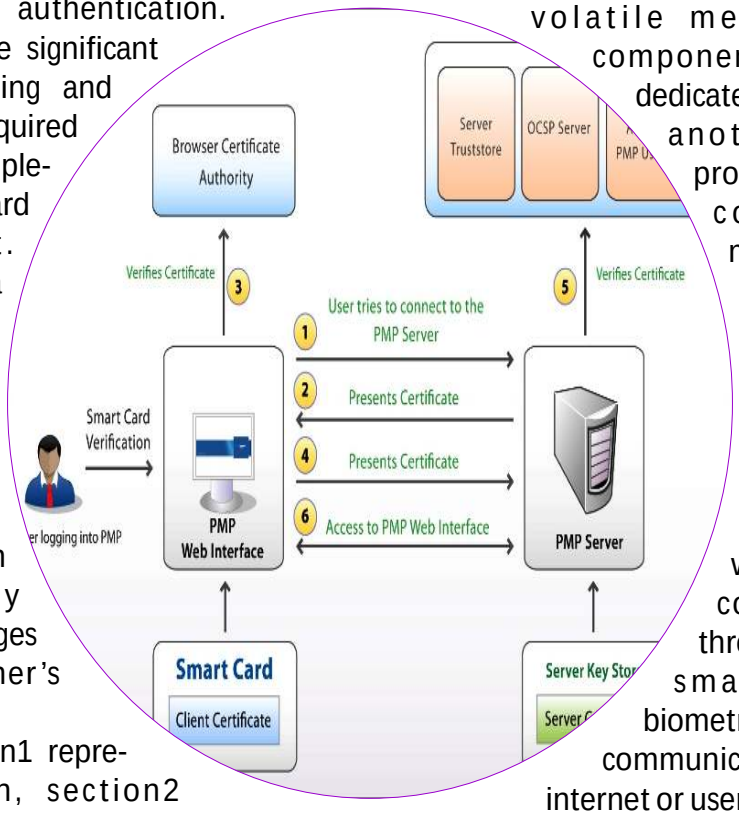
Security is very crucial issue in smart card especially due to the various independent parties involve throughout the card's life cycle leading to what is now called "splits" in trust. There is need to develop a method in which even without trust none of the parties can cheat one another. To overcome the lack of security provided by passwords or PINs for authentication and access control, some researchers believe that biometric is the best genuine means of authentication. However, due to the significant amount of processing and memory capacity required by this approach, implementing it in smart card remains difficult. Hence, this area needs to be further evaluated to make it suitable for built-in smart card applications. This paper represent that how this security issue can be overcome by bringing certain changes on some researcher's scheme.

In this paper, section1 represent introduction, section2 represents literature review, section3 represent the weakness of earlier work, section4 represent security analysis and section5 conclude the paper.

KEY WORDS: network security, password authentication protocol, smart card.

## INTRODUCTION:

Smart card is a temper proof computer e.g. a secure crypto processor and secure file system and provide security services (protect in memory location). It is a chip card or integrated circuit card (ICC) ,is any pocket sized card with embedded integrated circuit . here the ICC contain memory card which contain only non volatile memory storage components and perhaps dedicated security logic and another is a micro processor card which contain volatile memory and microprocessor .smart card provide a strong security authentication.




Authentication is the most serious issues for the issuer where the computer communicate user through the password , smart card or the biometrics devices. Insecure communication channel like internet or user's friend or the close family relatives can easily get and crack the password ,so the password based authentication scheme are susceptible by this type of attack.

This paper organize as follows .in Section 2, the literature review is classified as the analysis of Liao et all's password authentication ,the technology used in public transport industry ,the analysis of Liao's password authentication. in Section 3,the security analysis ,in section 4,the conclusion and in section 5,the references from where include the materials

## 2. LITERATURE REVIEW

### A. ANALYSIS OF RESEARCHER'S PASSWORD AUTHENTICATION:

Some of the researchers password based authentication mechanism is categorizes into four phases which are following

1.Registration phase
2.Login phase
3.Verification phase
4.Password change phase

1. Registration phase- the user Ui and its identity IDi. The server S compute Ni password verifier information H(Pi) by xor operation with the concatenation ! of secret key of the remote server S and identity Idi

Ni = H(Pi) ⊕H( x ! IDi )

2. Login phase- the user Ui insert his smart card into card reader to login on the server S, and then submit his password Pi. So ,smart card computes

CiDi =H(Pi) ⊕H(Ni ⊕y ⊕T)
Ei =H( CIDi ⊕H(Pi))
Ci =H( T ⊕Ni ⊕Ei ⊕y), here the T denotes to current date and time of input device and sends the login request message and ( Ci Di, Ni, Ci, T) to the service provider server S.

3.Verification phase- Service provider server S check the validity of time stamp T by checking (T1 - T) <= ?T, where DE denote the server 's current time stamp and T2 is expected time interval for the transmission delay. The server S compute H(Pi) = CIDi ⊕H(Ni ⊕y ⊕T)

Ei= H(CIDi ⊕H(Pi))
Ci= H(T ⊕Ni ⊕Ei ⊕y)

And then compares the computed value of CI S with received value of CI. If they are not equal the server S rejects the login request and terminate the session. And if they are equal, the server S computes.

Di= H(T2 ⊕Ni ⊕Ei ⊕y), where the T2 is the current time stamp and send the message (Di ,T2) back to the smart card of user Ui on receiving the message (Di, T2). Smart card check validity of timestamp T2 by checking ( T3 – T2) <= δT .where T3 is the client's smart card which compute Di =(T2 ⊕ Vi ⊕Ei ⊕y) , and compare with the received value of Di.

4. Password change phase- the client can change the password without the server S help. User directly insert his smart card into card reader and enter the old password Pi and then request to the new password Pinew . Then smart card compute
Ninew =Ni ⊕H(Pi) ⊕H(Pinew) and update the value of Ni with Ninew in its memory.

## B. TECHNOLOGY USED IN PUBLIC TRANSPORT INDUSTRY :

Smart cards are in use from last thirty years. It offers exciting prospects for convenience, accuracy, customization, data and cost reduction for individuals and organizations. Yet due to security reasons it has to establish its wide acceptability among the masses .There are many security risks such as transaction anonymity, fraud, data security etc. Unfavourably , the standards and specifications, created so far for the card hardware and the micro processing system have not been completely secure. There is no assurance for secured information and access control.

Smart card are utilized in a wide range of sectors including finance , telecommunication ,health government and transport. if we talk about public transport application freight monitoring ,weight plying ,poll collection. The advantage is it reduces the delays at entry gate, improve cash handling procedures, reduce staff handling cost and improve etc.

## C WEAKNESS OF ABOVE PASSWORD AUTHENTICATION

There were some weakness on above password authentication. in 2006, yoon and yoo showed the reflection attack on Lioa's et al that breaks the mutual authentication. Ku and chang's showed the impersonation attack on liao's et al. this liao's et al scheme does not maintain the user's anonymity. This approach divided his password authentication into four phases ,where the password change phase is insecure.

Attacker can extract the stored values by the reverse engineering technique which the Koacher et al's showed .mallicious privillaged user Uk can intercept the login request phase (CIDi, Ni, Ci, T) of the user Ui . Uk compute the password verifier information

H(Pi) = CIDi ⊕H(Ni ⊕y ⊕T) ,where the malicious user know the value of Ni, y and T .
CIDi* = H( Pi) ⊕H(Ni ⊕y ⊕T)
Ei* = H(CIDi* ⊕H( Pi))
Ci* = H(T* ⊕Ni ⊕Ei* ⊕y)
Now, it fabricated the login request phase = (CIDi* , Ni, Ci*, T*)

## 3. SECURITY ANALYSIS

After the analysis of above password authentication scheme. showed that effective password authentication scheme are those scheme where attacker could not break the password in different phases. The attacker can extract the smart card password by different method such as reverse engineering methodology. messerger's et al already pointed out that the existing smart card cannot prevent the information stored in them and the attacker can extract through being monitoring them by the power consumption.

Koacher's malicious attack showed that privileged user Uk can intercept login request phase (CIDi , Ni, Ci, T) to (CIDi* , Ni ,Ci*, T*)

Yoon and yoo demonstrate reflection attack on liao's et al where the login request message (CIDi , Ni , Ci , T) response message (Ci ,T ) of a false server. User Ui authenticate itself to the server after successful authentication. User Ui and server S agree on the common seesion key.

H(IDi ! Yi ! H(x) ! T)

Therefore is no any possibilities of reflection attack. So security analysis shows that the effective password is that which save themselves from the different attack.

## 4.CONCLUSION:

Smart technology has been widely recognized as providing the strongest security features of any identity token or payment card technology, benefiting from application. this technology is further divided into contact smart card technology and contactless smart card technology. The contactless smart card technology protects data stored on the contactless device. Contactless smart chip based device can encrypt the information stored on them and encrypt communication between the contactless device and the reader. Smart chip technology can also “lock” the personal information stored on the contactless device. Releasing it only after the owner provide unique information such as personal identification number (PIN), password or fingerprint (biometrics devices).

In this paper we just showed the critical analysis of password authentication scheme where they have made their password authentication into four phases ,the registration phase ,the login phase, the verification phase and the password change phase. Their has some critical issues which explain through different researcher method. Sandeep K sood, anil k.sarje and kuldeep singh ,978/1-4244-4791-6/10 , worked on liao et al and improved the liao et al password authentication scheme.

Security is very crucial issue in smart card especially due to the various independent parties involve throughout the card’s life cycle leading to what is now called “splits” in trust. There is need to develop a method in which even without trust none of the parties can cheat one another. Further, to overcome the lack of security provided by passwords or PINs for authentication and access control, some researchers believe that biometric is the best genuine means of authentication. However, due to the significant amount of processing and memory capacity required by this approach, implementing it in smart card remains difficult. Hence, this area needs to be further evaluated to make it suitable for built-in smart card applications.

Other important security issues involve further investigation of elliptic curve and quantum cryptography on smart cards.

## 5. REFERENCES:

1. L. Lamport, "Password Authentication with Insecure Communication", Communications of the ACM, vol. 24, no. 11, pp. 770-772, November 1981.

2. C. M. Chen and W. C. Ku, "Stolen Verifier Attack on Two new Strong Password Authentication Protocols", IEICE Transactions on Communications, vol. E85-B, pp. 2519-2521, November 2002

3. P. Koacher,J. Jaffe & B. jun,” Differential power analysis” , pro crypto 99,springer-verlag, pp. 388-397,August 1999.

4. E.J.yoon and K.Y.yoo, “improving the dynamic ID- based remote mutual authentication scheme ” proc. OTM workshop 2006, LNCS 4277,pp. 499-507, july2006.

5. I.E.Liao,CC Lee and M.S. Hwang ,” Security enhancement for a dynamic ID- based remote user authentication scheme, “proc. Conference on next generation web service practice, pp 437-440, july 2005.

6. Sandeep K. Sood , Ani! K.Sarje2 and Kuldip Singh ,” Cryptanalysis of Password Authentication Schemes: Current Status and Key Issues”, International Conference on Methods and Models in Computer Science, 2009

# Publish Research Article
# International Level Multidisciplinary Research Journal
# For All Subjects

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication,you will be pleased to know that our journals are

## Associated and Indexed,India

- International Scientific Journal Consortium
- OPEN J-GATE

## Associated and Indexed,USA

- EBSCO
- Index Copernicus
- Publication Index
- Academic Journal Database
- Contemporary Research Index
- Academic Paper Databse
- Digital Journals Database
- Current Index to Scholarly Journals
- Elite Scientific Journal Archive
- Directory Of Academic Resources
- Scholar Journal Index
- Recent Science Index
- Scientific Resources Database
- Directory Of Research Journal Indexing

Golden Research Thoughts
258/34 Raviwar Peth Solapur-413005,Maharashtra
Contact-9595359435
E-Mail-ayisrj@yahoo.in/ayisrj2011@gmail.com
Website : www.aygrt.isrj.org