International Journal of Information Technology and Knowledge Management
July-December 2010, Volume 3, No. 2, pp. 719-721

SECURITY AND PASSWORD MANAGEMENT ISSUES FOR REMOTE-USER AUTHENTICATION USING SMART CARDS

Ajay Jangra[1], Vedpal Singh[2], Priyanka[3] & Chander Diwakar[4]

Smart card works as passive, fixed size, low memory and small microprocessor carrying portable data carrier. Day by day no. of smart card user increasing rapidly because of its high secure and good quality multi-application utilities. In this paper we analysis various pins and password management policies applied in smart cards. We enlisting the various policies with respect to password security threats by study the pros and cons of all password management policies. We try to know, Is the password policies safe? , What are the open threats to password? , Is password travelling from CAD to server secure?
Intended Audience: This work is helpful for those for use smart cards or those who wants to use it and those who wants to be update himself aware to new technologies. This work specially needs the attention of the researchers (working in area of smart cards) and anyone to understand the functionality and basic password security related issues in smart cards.
Keyword: Password, Card Acceptance Device (CAD), Remote user Authentication, Encryption

INTRODUCTION

Smart card (also called, integrated chip card (ICC), memo-card) functions as portable data carrier, e-purse with VLSI enabled memory and microprocessor can be used as intelligent certificate of identity generally size of smart card (85.60mm * 53.98mm * 0.80mm). Smart cards are tamper resistant passive device. But in magnetic strip exhibits large number of security problems which gives prosperity and popularity to smart cards because security, functionality and applicability of smart cards are much superior than ordinary magnetic strip cards. New generation smart card contains inbuilt electronic circuitry (local memory, small processing unit and respective operating system) to perform the function of data security and security related operations.[1]

When a smart card enters into card reader (called card acceptance device (CAD) physically interface with the card provide power to the card and enabled it to perform read/ write application dependent operations. Standard protocols use to communicate between the smart card and smart card reader. [1] During manufacturing smart card equipped with EEPROM (electronically erasable programmable read only memory) memory unit. Smart card contains the three types of files a.) master file (MF), b.) dedicated file (DF), c.) elementary file (EF) for information storage. Master file at the top, may contain many numbers of dedicated files and elementary files. Dedicated files may contain elementary files and dedicated files also. The bottom level information group and stored in elementary files.[9,10]

[1, 2, 4] CSE Deptt. U.I.E.T., Kurukshetra University, Kurukshetra

[3]ECE deptt. Kurukshetra Institute of Technology & management, Kurukshetra

Email: er_jangra@yahoo.co.in, vedpalsiet101@gmail.com, priyanka.jangra@gmail.com, chander_cd@rediffmail.com

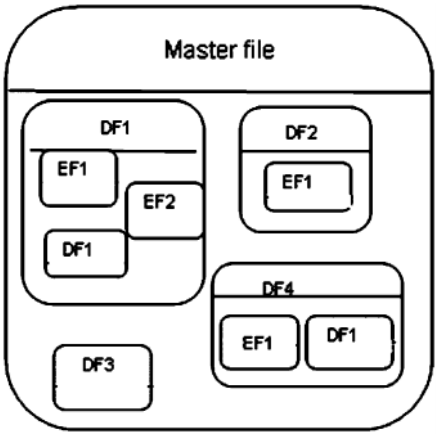

Fig.1: Different Information Storage Files in Smart Card

Smart card also contains some unassembled components like printed circuit, microcontroller, glue and plastic support to deal efficiently as portable data carrier used for collection and distribution of information into remote and rural areas.[2,11] Smart card may be multi-application smart cards used for multiple applications with hardware constraints such as low power CPU, low memory, low data write, serial I/O, etc. . [3]. smart card life cycle consists of five phases (i) user requirement phase, user involve directly in smart card life cycle by providing his requirement because for good development a great knowledge of requirement and security demands are required. The final requirement based design is embedded into printed cards. (ii) In manufacturing phase, hardware and software manufacturing performed at different places. (iii)A complete testing occurs for security and integrated circuit complete after manufacturing. (iv)In issuance phase, card issues to corresponding authority and issuer permits applications may be placed on the card using space. Card is use with supporting software in CAD and at last (v) end of card life, Each smart card has date of expiry.

[3] The major application areas of smart cards are health care, financial, telephony, identification, secure information storage, network applications, network applications, affinity programs, cellular phones, set top boxes etc.

Types and Technology of Smart Cards

Smart cards are of the two type memory cards and microprocessor card. Memory card use to store the data and user can't modify the data but in microprocessor card user can store the data as well as modify the data[5]. Smart cards also categories as contactless smart card where the card circuitry enabled with an antenna to make electro-magnetic wireless link with smart card reader for a range of 10cm (approximate) and contact oriented smart cards are those which works only when a physical contact established between smart card and smart card reader. Card Acceptance Device (CAD) provides the external power source to smart card. CAD integrated within smart card reader. Magnetic pin controller of smart card established a physical connection through CAD perform internal processing of data and communicate with smart card reader.

Authentication and Security Policies

Very first Lamport proposed first authentication scheme which followed by Hwang and Li's proposal for remote user authentication scheme based on discrete logarithmic difficulty problem. Registration phase, login phase and authentication phase are sequentially required in case of authentication where a secret key 'x' maintained by the system. When a user 'Ui' with identity 'IDi' apply for registration system automatically generate password 'Pwi'. [12]

Where $Pwi = (IDi)^x \bmod p$

Where public parameters (p,h) are used more over, 'h' is the one way hash function in next step (login phase). When user 'Ui' login by attaching card into input device with identity 'IDi' and password 'Pwi' following sequence of operations are perform as in [12]:

(1) Generate a random number r.

(2) Compute $C1 = (IDi)^r \bmod p$.

(3) Compute t = h (T (XOR) Pwi) mod (p-1), where T is the current date and time of the input device and XOR denotes the exclusive operation.

(4) Compute $M = (IDi)^t \bmod p$.

(5) Compute $C2 = M (Pwi)^r \bmod p$.

(6) Send a message C = (ID, C1, C2, T') to the remote system.

(7) Compute $C2 = M (Pwi)^r$

After accepting authentication message C system authentication user in following manner:

(1) Verifying user IDi.

(2) Check time interval T and T' to inspect transmission delay.

(3) Compute $Pwi = (IDi)^x \bmod p$ and t = h ((T (XOR) Pwi) mod (p-1).

If $C2 (C1^x)^{-1} \bmod p = (IDi)^t \bmod p$, then the system accepts the login request. Otherwise, it rejects the login request.

Recently, open smart card operating system with new technology and infrastructure applied new methods for extra securing the information [4]. Smart card govern under ISO / IEC 7816 and ISO / IEC 14443 international standards.[6]. Encryption policies / technology make high security in smart card, in general authentication of user to the remote server has required which based on password where password generates some secret information and server validates the remote user [9, 10].

Pin and Password use to improve the security level of smart card where the pin (second layer) (of length 4-12 digit) generates by issuer authority. User can only control the password (maximum length up to 20 characters) periodically changing the password makes good secure practice.

Password management policies are divided into following categories

Case I : a.) When password travel across the network (keeping a password table at the server side): Authentication server checks the validity of remote user login request. Lamport proposed the scheme where authentication server (AS) stores the password table and all login requests are verified with password table (server side). This scheme (as CASE 1-a in fig.2) exhibits the travelling of password user to server and reverse acknowledgement, it invites high hash overhead and high risk of password resetting.[12]

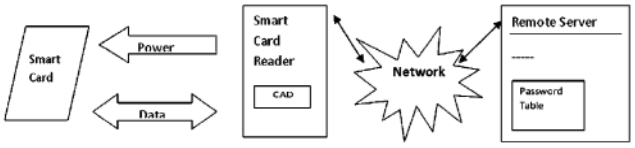

Fig.2: Smart Card Remote Server with Password Table (CASE I-a)

CASE-1 b.) When password travel across the network (without password table) :In this case during user login request password is transmitted to authentication server. as CASE-1b shown in fig.3 server process the password to generate new authentic key if calculated authentic key is valid then user gets the permission to access the server. It makes a lengthy and complex password calculation.

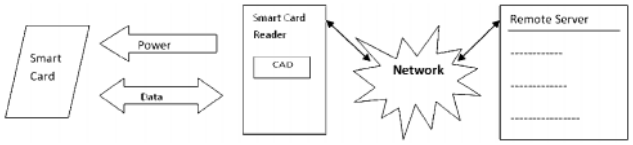

Fig.3: Smart Card Remote Server without Password Table (CASE I-b)

In new ID based authentication system a unique authentication ID of the user is used to overcome the disadvantages of previous policies such as password stolen, modification…etc attacks. Further more in a new advance scheme an ID+password based authentication to proposed where encrypted ID and password are sent to authentication server for verification and server grants the smart card functionality to the authentic user.

Case II : When password is not travel across the network: As shown in fig.4 password never travels from user to server for authentication. ID and other parameters are send to server these parameters include some constants (C, B, etc.) and time parameters T and T'. T is the time of sending login request, T' is the time of receiving the login request.[13]

When T' – T> = valid time interval for transmission delay server issues the authentication.

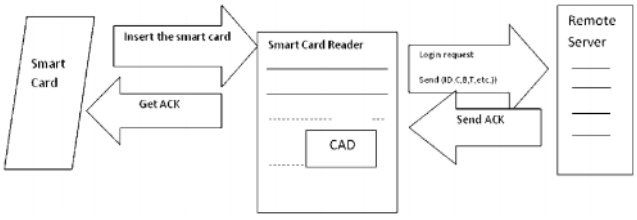

Fig. 4: Smart Card Remote Server Process without Password Traveling

Comparative Analysis of Various Password Management Policies

From the above cases when password travels across the network the risk of password hacking, modification etc. attacks are high if server maintains a password tables that can also be afraid from these attacks and required unnecessary memory space, time consuming password verification process but in second case where password is not traveling to the network no need to maintain and protect the password table which make system faster but the attacks of password guessing and hacking still there [7,8].

CONCLUSION

Although smart cards posses intelligent, portable, self processing authentication policy but security and privacy are remains the prime issues of research and applications interest. Some threats like (password hacking, guessing, modification attacks) can be reduced by using encryption policies. Password travelling across the network can invites threats and (ID +password) policy reduces some of these attacks but still a full proof high security oriented password management system still required to use in smart card for high security required application areas.

REFERENCES

[1] S.K.Sinha "Smart Card Technology and e-Governance" e-notes.

[2] Ryutaro Toji, Yoshinori Wada "A Multi-card Architecture for Smart Card Management Systems", NTT Technical Review, 1, No.6, Sept.2003.

[3] Ashutosh Saxena, Aditya Gaiha "A Framework for Smart Card Payment Systems" IDRBT's Working, Paper no.6, Jan.2001.

[4] Denis Praca, Claude Barral "From Smart Cards to Smart Objects: the Road to New Smart Technologies" Elesvier Science B.V. Computer Network, 36, pp381-389, 2001.

[5] John abbott "Smart Cards: how Secure are they?" GSEC Practical, v1.3 SANS Institute, 2003.

[6] White Paper on "What Makes a Smart Card Secure?" Smart Card Alliance, 2008. www.smartcardalliance.org

[7] Manoj Kumar "Security Analysis of a Remote User Authentication Scheme with Smart Cards".

[8] Manjula Sandirigama, A. Shimizu, M.T.Noda "Simple and Secure Password Authentication Protocol (SAS)", IEICE TRANS. COMMUN, E83-B, No.6, June 2000.

[9] Smart Card Industry Association (SCIA) www.scia.org, "Smart Card Overview" 1998.

[10] www.smartcard.com "Smart Card: Technology".

[11] L.A.Mohammed, Abdul Rahman, V. Prakash and Mohamed B. Daud "Smart Card Technology: Past, Present and Future" International Journal of the Computer, the Internet and Management, 12, # 1 Jan-april 2004, pp12-22.

[12] Hung-Min Sun "An Efficient Remote use Authentication Scheme using Smart Cards" IEEE Transactions Con Consumer Electronics, 46, No.4, Nov.2004.