International Journal of Latest Trends in Engineering and Technology
Special Issue SACAIM 2017, pp. 582-586
e-ISSN:2278-621X

NEW AUTHENTICATION SCHEME USING SMART DEVICES

Santosh Kumar Gupta[1], Uma Shenoy[2] & Mr. Santhosh B[3]

Abstract- Authentication plays a critical role in securing any online system, and online systems and various services have long relied on username/password combos to verify users. It is very difficult and inefficient to memorize and remember passwords for a lot of accounts. Furthermore, traditional authentication methods have failed over and over, and they are not immune against a wide variety of attacks that can be launched against users, networks, or authentication servers. Over the years, data breach reports show that attackers have created many high-tech techniques to steal user's credentials, which poses a very serious threat. In this paper, we introduce an effective and efficient user authentication scheme using personal smart devices that utilizes cryptographic techniques, such as encryption and digital signature. This paper shows a study of how this new technique can be applied in online systems in order to enable users to execute a more secure authentication protocol. The proposed scheme does not require an authentication server to maintain static username and password tables for identifying and verifying the legitimacy of the login users. It not only is secure against password-related attacks, but also can resist replay attacks, shoulder-surfing attacks, phishing attacks, and data breach incidents.
Keywords – Security, authentication, one-time username, access control.

1. INTRODUCTION

Traditional authentication schemes such as the username/password combo pose a serious threat to the online banking services, financial systems, and their users. In the current authentication systems a static or unique user id is assigned or allowed to the user which acts as a label. This static label is typically attached to the user for a long time. Unfortunately, users usually use the same user id in many different websites and systems. Furthermore, many users keep on using the same password across different online accounts and systems. According to a recent study, 51% of the surveyed users reuse the same password across different websites, and more than 77% of the participants either slightly change or reuse existing passwords withsimple tricks. There are certain risks associated with this common practice such as insider attacks. Malicious administrators or insiders, who have access to username and password tables, can utilize the information to access other services and websites. This practice could let a phisher to use users' credentials on more than one website. A type of social engineering attack, Phishing in which a malicious user also known as a phisher could acquire user's credentials fraudulently from a trustworthy entity or a public organization. Use of static credentials is one of the main reasons why phishing attacks succeed with a high a rate. We can change this paradigm by abandoning the use of static usernames and password to get a better and a dynamic authentication scheme which is anti-phishing, in which the users do not have to be worried about their accounts being accessed by some un trustful being. In this paper, we present the idea and make a study of how one time username coupled with a verification code can give better security and also enhance user experience during each login session. There is no reason for the user to remember multiple usernames and complex passwords.Weoutlinethemaincontributionsofthispaperas follows:

• We introduce a new authentication scheme which integrates encryption and digital signature which does not need the users to remember usernames and passwords. This scheme enhances the level of security and eliminates the risks associated with traditional authentication methods.

• Introducing the concept of user-centric access control, which can play an important role in authentication and gives a better security. In user-centric access control, users can set their own permissions to their accounts every time they login.

• We make a study on how this new authentication stands tall against various hacking methods and tools such as phishing, password related attacks, shoulder surfing attacks, replay attacks and others and does not allow anyone to hack into the systems very easily.

• We discuss how this new authentication scheme followstheOne-TimePad(OTP) propertyforthesessionkeyandverificationcode,which increases the security during authentication.

2. MOTIVATIONS

The goal of this study is to introduce a new authentication scheme which uses dynamic usernames and to bid a goodbye to traditional techniques of storing user credentials at a centralized location.Many attacks and issues such as keylogger attacks, shoulder surfing attacks, data breach incidents, password reuse and other factors can be very well resisted with the help of this scheme. Static authentication schemes can be targeted by keylogger attacks which have become more complex. Keyloggers are either hardware device or a software program which resides in the victim's computer and acts as a malicious

[1] Department of MCA, AIMIT, St. Aloysius College, Mangalore
[2] Department of MCA, AIMIT, St. Aloysius College, Mangalore
[3] Department of MCA, AIMIT, St. Aloysius College, Mangalore

process.Keyloggers have the capability to observe and capture every keystroke type typed on the victim's computer which includes capturing authentication information like usernames and passwords.

There is another issue called shoulder-surfing attacks which targets and attacks these traditional authentication schemes. Shoulder-surfing attacks include direct observation techniques like looking over someone's shoulder or a hidden camera to get authentication information. Unfortunately, shoulder surfing has proved to be an effective way to target authentication methods and obtain username, PINS, passwords and other sensitive data.

Data breach is another important issue which has become more common now. Data breaches can have large impact on many users and financial sectors. According to many leading experts data breaches have become one of the biggest security problems faced by security professionals and system administrators because it requires disclosure of usernames and passwords. Data breach consequences have become more very severe and it is difficult to estimate the damage on the breached organization and accounts of the users in different online systems. These leaked credentials can be used to target online accounts of the users by a malicious attacker to perform malicious activities. For example, transferring money overseas or disclosing financial information. The username/password combo is one of the biggest data breachproblems.

3. MODELS AND GOALS

3.1 System Model

This system model has two major entities as shown in Fig. 1: client and server. The client side consists of the registered devices and the user's terminal. The primary function of each entity is summarized below.

• Registered devices: A registered device is a smart personal device such as a smartwatch or a smartphone, which canperformcryptographicoperations.In order to get server's services, each user is required to register a smart device with the server.

• User'sterminal:Auser'sterminalisanelectronicdevice such as a laptop, desktop or a smart phone which can be used to log in to the server to view or perform transactions.

• Server: The server belongs to an entity such as a bank, and it is connected with a hardware security module (HSM) that safeguards the private key and provides crypto-processing. Public key and verification code is distributed to the clients by the server. The server also provides other services.

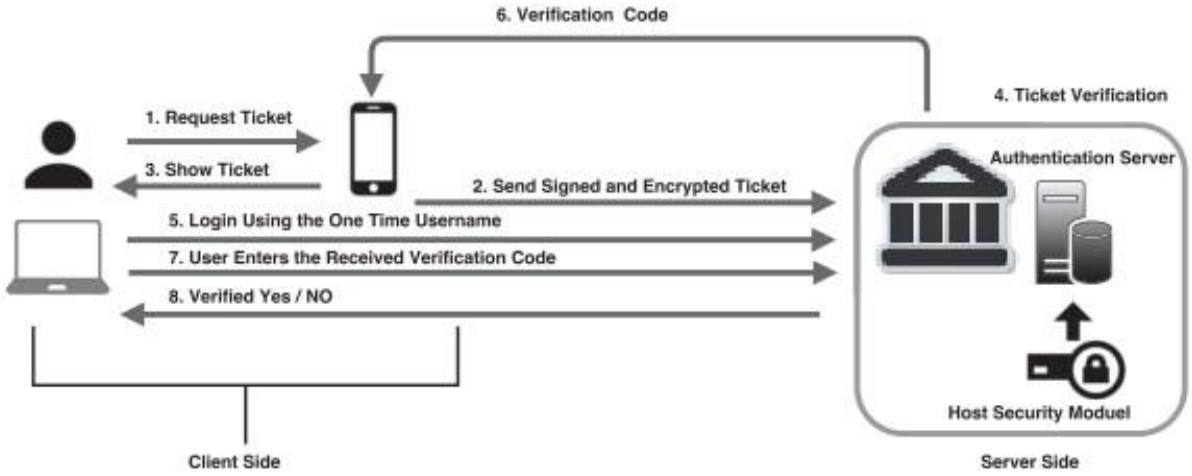

Figure 1. The system model of the proposed design.

3.2 Design Goals

• Correctness: The client and server can achieve a correct authentication result if both the client and server follow the protocol honestly.

• Security: The protocol can protect the privacy of the client'sdata.Ononehand,giventheencryptedmessage, theattackercannotgettheclient'soriginalinputdata.On the other hand, the correct result is also hidden from an attacker.

• Verification:Messageandverificationcode from the client must be successfully verified by the server.

4. AUTHENTICATION PROTOCOL DESCRIPTION

This section is dedicated to describing the proposed protocol, which can be used in different domains such as online banking, e-government, and e-Health systems. We are going tousetheonlinebankingsystemtodemonstrateourprotocol. We start by presenting the ticket information, then detailing the overall protocol steps.

4.1 Session Tickets

When the user wants to login, for each login session the user generates a ticket with the help of the registered device. A ticket is generated on the registered device and it is sent to the server for verification.Thetransmissionoftheticketfromthe registered device to the server is encrypted with the server's public key. A login ticket consists primarily of a one-time username OTU, a session key k, a ticket validity period TVP, a timestamp T, and an access control list ACL. The ticket information is described as below.

1) One-Time Username: It consists of 8 characters including capital letters, small letters,numbers,andspecialcharacters.Theone-timeusername shouldbegeneratedrandomlyusingtheregistereddevice. We chooseeightcharactersbecausemanysystemsareconfigured to handle eight characters.

2) Session Key:A registered device (e.g. smartphone) randomly generates a session key for each login session. The session key is asymmetric key that will be used to encrypt the verification code between the server and the user.

3) Ticket Validity Period: It is a security parameter that limits the lifespan of a ticket. Inourdesign,wegivetheuserthe ability tospecifytheticket validity period (e.g. 5 min); however, security administrators can set a maximum lifetime for tickets.

4) Timestamp:Atimestampisatimeinstanceatwhichtheregistereddevice issues a ticket. The timestamp is presented in a consistent format, allowing the server for easy comparison of two different tickets and for tracking users' login activities over time.

5) Access Control List: The access control list is specified by the user. With respect to this authentication scheme, it is a list of permissions attached to a ticket, and it can be different for each login session. For simplicity, we assume that there are two permission modes:

• Active mode permission: In this mode, users can perform actions on the account. For example, in an online banking system, when the user selects this permission, it gives him the ability to fully control the account.

• Passivemodepermission:In this mode the user is restricted to view the transactions, but cannot perform any active operation any further.

4.2 The Proposed Protocol

• A cryptographic technique is used to digitally sign the ticket.

• The registered device holds its public key p1 and private key q1, which is constructed based on the cryptographic algorithm.

• Theservergeneratesitspublickeyp2 andprivatekeyq2 whichisusedto guarantee the confidentiality.

4.3 Description

This protocol consists of four algorithms: Algorithm 1 provides the details regarding how to sign and encrypt the ticket information; Algorithm 2 describes the decryption and verification of the ticket information; Algorithm 3 is used by the server to verify the user based on the received ticket; and Algorithm 4 is employed by the user to decrypt the verification code. Before starting the protocol, a user should specify permissions as mentioned above.

Algorithm 1 Sign and Encrypt:

1) The registered device generates the ticket M
2) The registered device signs M using the using cryptographic technique.
3) The registered device encrypts M along with the signature.
4)The registered device sends encrypted M to the server.

Algorithm 2 Decrypt and Verify:

1) The server receives and decrypts M.
2) The server verifies the signature. If it is verified, the server waits for the user to login; otherwise, the request is discarded.

Algorithm 3 Server Verification:

1) The server receives an OTU (One Time Username) and checks whether or not this OTU has a valid, associated ticket.
2) The server generates VC(verification code).
3) The server encrypts VC
4) The server sends encrypted (VC) to the user.

Algorithm 4 User Verification: Once the user logs in using OTU.

1) The registered device receives the encrypted verification code (VC).
2) The registered device decrypts (VC).
3) The registered device shows the VC to the user.
4) The user enters the VC to login to the server, which can authenticate the user.

5. SECURITY ANALYSIS

In this section, we study and analyze the security of the proposed authenticationschemeunderdifferent attacks.

A. Phishing Attacks:There are many phishing attacks whose goal is to steal credentials like usernames and passwords by masquerading or impersonating a trustworthy entity. This proposed authentication scheme can contribute towards reducing the risks associated with these phishing techniques. Since there is no use of static username or password in this scheme, it would be safe enough to call this scheme an anti-phishing technique.Forevery login session a new username and password is

generated. We consider the proposed design an anti-phishing authentication protocol a username is generated to be used within one session by the user.

B. Password-Related Attacks:There are many password-related attacks such as shoulder surfing and direct observation and this authentication scheme provides direct protection from these attacks. In this authentication scheme, the client is not using static username and password which could have been recognized by thermal imaging or mechanical vibration analysis.Since we rely on a set of dynamic username and password that is unique for each login session, issues such as using the client's birthday as the password, using the same passwordeverywhere,orforgettingthepasswordareavoided.
Obviously there will be subtle risks if a user uses the same username and password for many different servers. Some services and service providers might not be as trustworthy as others, Username and password files can be easily accessed by a server admin or an internal employee with high privileges which can be used to gain access to user's accounts on the servers. Using this protocol many usernames and passwords are generated by the registered device each time a client wants to login.

C. Shoulder-Surfing Attacks:Shoulder surfing attacks can be easily achieved if we keep on using static usernames and passwords and an attacker can easily gravest sensitive information like passwords. A malicious attacker using different direct observation techniques observes the victim and obtains its credentials. Shoulder-surfing attacks can be achieved by looking over a victims shoulder to capture the password or using vision enhancing devices from a distance. Therefore, we can use dynamic credentials which are generated and used only one time which prevents the risk of shoulder-surfing attacks.

D. Replay Attacks:On the client side, a client enters its one-time username along with its session key for every authentication request. Also, the ticketexpiresafterithasbeenusedorafteraveryshortperiod of time. Timestamping is another important feature in this scheme along with the user login list gives an effective way to prevent replay attacks. Notice that a verification code is generated by the server which is valid only for a certain time period (e.g. 5min). Thus we claim that the server can resist the replay attacks.

E. Client Request Protection: Inourscheme,aclient'sauthenticationrequestissignedviaa signature, which is secure and can guarantee the authenticity and data integrity of the client's message. The client's authentication request an signature are encrypted using the server's public key.

F. Server Response Protection: When the server receives the message that includes the ticket information, the server decrypts the message to get theclient'srequestandsignature.Thentheserververifiesthe identity of the client. If it is an unauthorized user, the server discards the ticket; otherwise, the server waits for the user to login.WhentheuserlogsinusingOne Time Username (OUT),theservergenerates the verification code and encrypts it using the session key, thensendstheencryptedverificationcodetotheclient.After receiving the encrypted verification code, only the client can decrypt it to get the verification code because the shared session key is known only by the client and the server.Therefore during the response procedure, the confidentiality of the response message is ensured.

G. One-Time Pad Property:In the proposed protocol, the one-time username, session key, and verification code are updated for each login session; consequently, they have the property of One-Time Pad(OTP). It is well known that OTPs can guarantee confidentiality. Since the session key, one-time username, and verification code are randomly generated by the registered device and the server, they are unrelated to any previous session key and verificationcode.Therefore,anattackercannotdecryptthe ciphered response to any request.

6. CONCLUSION

The extra ordinary growth of online banking and e-commerce system shasledtoahuge in crease in the number of user names and passwords managed by individual users. Conventional static username and password protocols suffer from various security issues. Many users start using duplicated credentials overandoveragaininvariousaccountsandsystems.Leaking orcompromisingoneaccountcouldcauseanattackertoinfiltrate other systems and endanger users' security and privacy. In this paper, we introduce a new authentication scheme that allows users to get rid of many issues such as memorizing usernames and passwords for many different websites and systems. The proposed authentication scheme paves the way for user-centric access control that helps minimize the risks of many attacks. There are several research directions that can be further explored in our future research. First of all, we would like to investigateusinglightweightcryptographictechniquesin our scheme. Second, we plan to work on the design of different user-centric access control models. Also, we intend to study techniques for improving the authentication methods such as using visual decryption and visual signature verification. Finally, reporting on usability of the proposed authentication scheme should be further investigated in our future research.

7. REFERENCES

[1] K. Aravindhan and R. Karthiga, ''One time password: A survey,'' Int. J. Emerg. Trends Eng. Develop.vol. 1, no. 3, pp. 613–623, 2013.

[2] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, ''The quest to replace passwords: A framework for comparative evaluation of web authentication schemes,'' in Proc. IEEE Symp. Security Privacy (SP), May 2012, pp. 553–567.

[3] B.BorchertandM.Gunther,''IndirectNFC-login,''inProc.8thInt.Conf. Internet Technol. Secured Trans. (ICITST), 2013, pp. 204–209.

[4] J.Brainard,A.Juels,R.L.Rivest,M.Szydlo,andM.Yung,''Fourth-factor authentication: Somebody you know,'' in Proc. 13th ACM Conf. Comput. Commun. Secur., 2006, pp. 168–178.

[5] N. Chou et al., ''Client-side defense against web-based identity theft,'' presented at the 11th Annu. Netw. Distrib. Syst. Secur. Symp. (NDSS), San Diego, CA, USA. [Online]. Available: http://www.isoc.org/isoc/conferences/ndss/04/proceedings/

[6] FederalFinancialInstitutionsExaminationCouncil,''Authenticationinan internet banking environment,'' Federal Deposit Insurance Corp.(FDIC), Washington, DC, USA, Tech. Rep. FIL-103-2005, Mar. 2005.

[7] D. Damopoulos, G. Kambourakis, and S. Gritzalis, ''From keyloggers to touchloggers: Take the rough with the smooth,'' Comput. Secur., vol. 32, pp. 102–114, Feb. 2013. [15] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, ''The tangled webofpasswordreuse,''inProc.Symp.Netw.Distrib.Syst.Secur.(NDSS), 2014, p. 1.

[8] R. Dhamija, J. D. Tygar, and M. Hearst, ''Why phishing works,'' in Proc. SIGCHI Conf. Human Factors Comput. Syst., 2006, pp. 581–590.

[9] C. Herley and D. Florencio, ''How to login from an Internet café without worrying about keyloggers,'' in Proc. Symp. Usable Privacy Secur., 2006, p. 6.

[10] T. Holz, M. Engelberth, and F. Freiling, Learning More About the Underground Economy: A Case-Study of Keyloggers and Dropzones. Berlin, Germany: Springer, 2009.