International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 7
July 2017

Decentralizing Identity Credentials to Safeguard Digital Identity

Uzair Ahmad Khan
Department of Computer Science
JamiaMilliaIslamia
, Jamia Nagar, Delhi, India

Khurrram Mustafa
Department of Computer Science
JamiaMilliaIslamia
Jamia Nagar, Delhi, India

Abstract-Privacy and security are two key challenging areas inthe world of internet. Researchersand industry professionals are working in this direction to address these issues. There are various approaches employed to address these concerns,but each have certain limitations. Identity objects are kept and stored at the server side. Whenever user logs in to the website, she supplies these object through client device, typically through a web browser. These identity objects are static in nature and they are encapsulated in the form of userid and password. Eavesdropper/ Hacker can steal these information from the client device by installing the key logger software, phishing emails etc. Most of the sensitive websites are deployed to be accessed through HTTP/SSL. Thisensures that the data that is being communicated with the server are safe and encrypted over the HTTP session. This only ensures the security of identity object on the server side and in the SSL session, but do not ensure security of these credentials when user passes this object through client device.

Keywords- Privacy,Security, Identity, Authentication and Authorization, Decentralization.

I. INTRODUCTION

Protecting digital identity of the user in online world is highly desirable.Digital identity are typically stored in the form of userid and password, user authenticates herself in the online world through her digital identity. When we store the digital identity in this form (userid/password),we are making identity object static. Bad guys/Hackers exploit this vulnerability and employ various mechanisms to steal this *static identity object* and make illegal and unsolicited transaction on behalf of user. To ensure more secure authentication process, we are proposing an approach wherein user can add a factor of dynamism to the existing identity object. In this way, it would be very difficult for the attacker/ eavesdropper to steal these login credentials.

Attacker steals user credentials by various mechanismslike installing the physical key logger on the client machine/users machine, key logger software which traps all the keys pressed; phishing emails which asks user to supply her credentials in the link provided in the email and many more.There are two parts of securing the identity object of the user, which are

1. First securing the identity object that is kept on the server.
2. Second securing this identity object when users supply the identity object as part of login process or when she initiates any transaction on the website.

There isvarious identity management software that is in place to ensure the security of the identity object on the server. We are proposing an approach to secure identity object at client side, hence addressing the later

A. Definition of the problem

Protecting the digital identity by decentralizing authentication credentials

This work mainly focuses to answer the following research questions:

RQ1. *How addition of more authentication attributes/credential increases the level of security?*

RQ2. *Impact of decentralizing the authentication attributes/credentials on security?*

RQ3. *What is the impact of proposed solution to the overall security?*

B. Key Contributions

There are following key contributions of the proposed work:

- Enhanced security of the identity object at client side.
- Configurability to the number of decentralization channel (users with basic requirement can have the default

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 7
July 2017

authentication attributes; user with advanced requirement can set more attributes to safeguard the identity).

- Protection from the spywares if they are present on the client device.
- Users confidence on the login mechanism and no worries whether she is accessing the website from home or through a public domain.

II. RELATED WORK

Privacy and identity management is a pressing concern in the world of internet today. Various approaches has been proposed and employed to address these concerns. In [1] author proposed an open ID framework which is a platform for user centric identity management, as this is an open source framework this can be plugged in and coupled with other identity management solution, open ID provides a standard way for the identity management. Other approach in which identity is being protected are through encryption and decryption Dan Boneh[5] has proposed an identity based encryption technique which is based on Diffie --Hillman encryption approach, in the same direction Taejon[6] worked on identity based signature which is again based on Diffie-Hellman encryption approach.

In [3], authors discuss about decentralizing the trust management wherein they talk about the security policy and security credential in a way that it can be shared over to third parties during the transaction and security credentials should be designed in a way that during the handshake to third parties for authentication the original credentials neednot tobe available to the third parties. We are in the era of distributed computing where the infrastructural components are distributed in multiple places and not relying on the monolithic application where all components are centered in one place. So in a distributed environment ensuring the security and identity is another concern. On the same line [7] authors have proposed the trust management solution in distributed environment and highlights the role of trust in such environment.

With the inception of cloud computing where the infrastructure, applications are not under the direct control of the application owner, we need to look at the security aspects differently in the cloud setup. Security is one of the key challenges in the adoption of cloud computing and people are still reluctant to deploy the sensitive applications in the cloud environment. [2,8] discuss and propose some of the solution which is applicable from cloud computing security. There are various security threats in the cloud environment with respect to user privacy and data protection .In [4] authors did a survey on the potential security threats in the cloud environment. So it gives a nice survey to the people who wishto work in the direction of cloud security to see whatall prevailing challenges in cloud environment are. No matter what kind of service delivery platform is there, security and privacy is a growing concern and it needs to be addressed.

III. PROPOSED APPROACH

In this approach we are distributing and decentralizing the identity object attributes, so that all the attributes are not present at one place and they are not static. Few of the identity object attributes (userid,password) will be provided by the user always and these attributes are static in nature. Rest of the configurable attributes isdynamic in nature and will be generated on the fly and will be valid for one session and will be applicable for one time only.

These on the fly dynamic attributes will be sent to the user through different channels which may not be invaded by the hacker/eavesdropper who are trying to steal the user credential.

One on the fly password will be sent to the user through mobile sms, other can be sent to the different email account and many more , that depends how many channels has been configured by the user to receive on the fly dynamic attributes.

Once user have all the attributes (static and dynamic on the fly attributes), she will be able to login to the website. This approach ensures that even though someone other than the user has the static user credential (userid/password) then also she will not be able to login to the account on users' behalf as she cannot have dynamic on the fly attributes that will be generated on the fly and will be sent to user through different channel. The proposed approach has been depicted in the following figure.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 7
July 2017

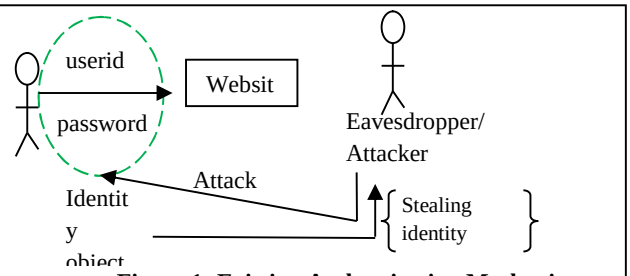

Figure 1: Existing Authentication Mechanism

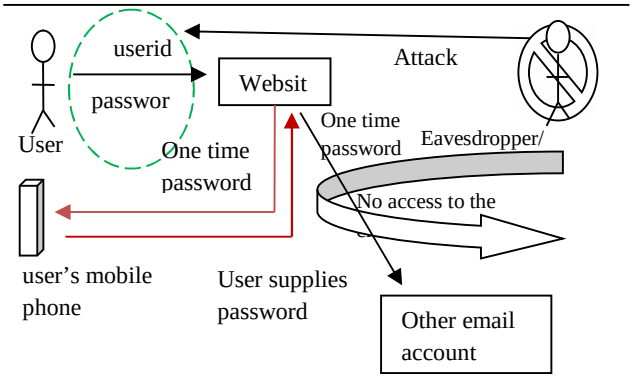

Figure 2: Proposed Authentication

Figure 1 shows the current authentication mechanism where user supplies userid/password combination and the hacker attack these objects on the client machine and steals the same.

In Figure 2 we have shown how the proposed authentication mechanism is more robust than the existing one. Even though Hacker/Eavesdropper can intercept the channel, place spywares in the client browser , but that will not work as she will require on the fly one time dynamic attributes in order to complete the authentication process.

IV. CONCLUSION

In this paper we propose an enhanced authentication mechanism which ensures the safety of user identity object on the client side. By decentralizing the identity object credentials to multiple channel we ensures that even in presence of eavesdropper (who are constantly monitoring the user session) the user identity object cannot be stolen by the hacker or eavesdropper as this willjust be partial information required for authentication, rest of the dynamicattributes that gets generated on the fly will be made available to the user through other channels that will not be under the control of the hacker.

The other benefit of this approach is that user need not to worry much about her userid and password details and user will have a confidence that she can perform any kind of transaction from home or through public internet as by merely hacking the userid and password will not help the hackers to login on users behalf. Hence no transaction can be initiated by the hacker on users' behalf.

REFERENCES

[1] D. Recordon and D. Reed, "Openid 2.0: a platform for user-centricidentity management," in Proceedings of the second ACM workshop on Digital identity management. ACM, 2006, pp. 11–16.

[2] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation computer systems, vol. 28, no. 3, pp. 583–592, 2012.

[3] M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized trust management," in Security and Privacy, 1996. Proceedings. 1996 IEEESymposium on. IEEE, 1996, pp. 164–173.

[4] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of network and computerapplications, vol. 34, no. 1, pp. 1–11, 2011.

[5] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in Advances in Cryptology CRYPTO 2001. Springer, 2001,pp. 213–229.

[6] J. C. Choon and J. H. Cheon, "An identity-based signature from gap diffie-hellman groups," in Public key cryptographyPKC 2003. Springer,2002, pp. 18–30.

[7] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. D. Keromytis, "The role of trust management in distributed systems security," in Secure InternetProgramming. Springer, 1999, pp. 185–210.

[8] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On technical security issues in cloud computing," in Cloud Computing, 2009.CLOUD'09. IEEE International Conference on. IEEE, 2009, pp. 109– 116.