© 2018 IJSRSET | Volume 4 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
National Conference on Advanced Research Trends in Information and
g Technologies (NCARTICT-2018), Department of IT, L. D. College of Engineering,
Ahmedabad, Gujarat, India In association with
International Journal of Scientific Research in Science, Engineering and Technology

A Survey on Social Media Security

Khevana Shah[1], Prof. Mital Panchal[2]
Information Technology, L.D. College of Engineering, Gujarat Technological University, Ahmedabad, Gujarat, India

ABSTRACT

A user authentication scheme that uses any form of social knowledge, utilizes users' trust relationships, monitors users' social contexts, or records users' friend associations for granting or denying access to any resource is considered a social authentication scheme. "The direct or indirect utilization of social knowledge or trust relationships in human-computer authentication systems deployed in online or offline contexts." In this study we analyze the security of social media in basic prospective of type of authentication, possible threats and terms to protect authentication from that threat.

Keywords: Social Media, Security, Session Hijacking, Cookie

I. INTRODUCTION

Social media security is the process of analysing dynamic social media data in order to protect against security and business threats.Influencing factor in use of social media
(I) Ease of use, (II) Globally acceptable and (III) Used for faster, easier, better communication.

Type of data shared on social media can be of Profile data,
Pictorial data and Activity data. The main reason for the security risk can be of multiple degree depending on the type of data and priority for the person holding the same. The main reasons for this are (I) Third party application access, (II) Poor implementation and (III) Lack awareness

A user authentication scheme on social media, utilizes users' trust relationships, monitors users' social contexts, or records users' friend associations for granting or denying access to any resource is considered a social authentication scheme. "The direct or indirect utilization of social knowledge or trust relationships in human-computer authentication systems deployed in online or offline contexts."

In this study we analyse the security of social media in basic prospective of type of authentication, possible threats and terms to protect authentication from that threat.

The rest of this paper proceeds as follows. In Section 2, we present our secure cookie scheme in detail. In Section 4, we discuss the implementation of our secure cookie scheme and its performance. In Section 5, we review and examine existing cookie schemes. We give concluding remarks in Section 6.

II. METHODS AND MATERIAL

Many collaborative websites and social media networks utilize session cookies as a cheaper alternative to the wide utilization of the secure HTTPS protocol. The unprotected nature of cookies can compromise the collaborative environment. Evidently, the availability of social networks and collaboration websites where access to the website is extended to long durations has made this issue even more pressing. Although using a secure protocol (e.g. HTTPS) to connect to the web provides higher levels of security, it is not always applied by many web servers and is replaced by cookie protection. The nature of cookiesThe issue of session hijacking or 'side jacking' due to sniffing out of Internet cookies is one of the important Internet security concerns. Session

hijacking results from unlawful control over cookies during an ongoing internet session in an unprotected network where plaintext traffic is unencrypted. Cookies are vulnerable to attacks, which makes their current deployment questionable and warrants a search for more reliable and secure techniques. Several researchers have tried to solve the vulnerability of cookies. For example, the use of an external proxy where authentication and sensitive information management is carried out completely at the proxy or some other external device. However, this solution's implementation can pose difficulties as it might not be optimal in all situations. Specifically, if a user does not have access to the proxy for any reason or in case the external device is not available at the time when the service is desired (e.g. cell phone battery dead, no coverage…etc.), he will not be able to use the service.

A. Social Authentication: A Definition

As we focus on reviewing the user authentication schemes that leverage information extracted from users' social contexts or intermediate humans in their identity verification processes, all human-computer authentication techniques that rely on eliciting unique characteristics from individuals' social interactions with others are considered social authentication schemes.

B. Social Authentication Techniques:

A Review Previously developed socially aware authentication systems have either leveraged social knowledge to authenticate users

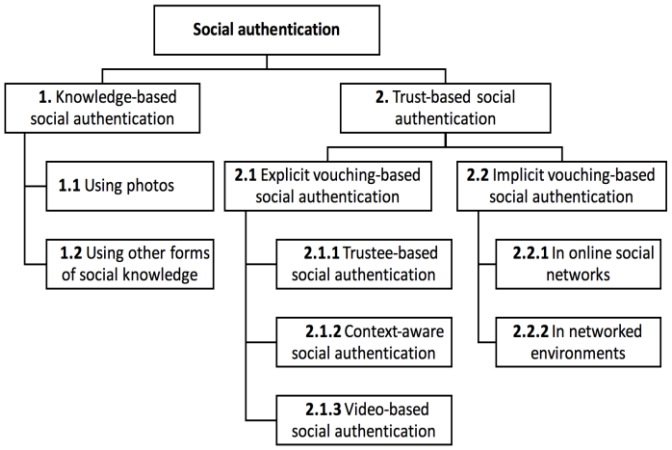

Figure 1. Taxonomy of social authentication schemes in the literature [1]

1) Knowledge-Based Techniques: Knowledge-based social authentication mechanisms rely on the design of the security questions that ask the user about his/her social context, such as social relationships, conversations, or shared knowledge. These mechanisms may require the user either to recognize or recall some information about people he/she knows. For challenge questions to be effective, their answers should be easily memorized, difficult to guess, and unreachable by unauthorized users. Techniques that can be built on top of Facebook's photo-based two factor social authentication system few research attempts have focused on investigating other types of social knowledge that can be uniquely used for authenticating people. This paucity could be linked to the difficulty in analysing individuals' social contexts, identifying the private social information that users can easily remember, and measuring the accuracy and uniqueness of social data. Since currently used knowledge-based social authentication schemes, which were developed as variants of some existing two-factor authentication systems (e.g. Facebook's Login Approval and Google 2-step authentication techniques)

As a sum of all techniques we can accumulate the list of all as (I) Photos Questionaries' (Node, Edge, Pseudo edge), (II) Vouch ID Choose trustees Trusted Contact tracking gestures and motions using wearable sensors Video Notarization Process and (III) User's digital certificate, Biometrics, PINs, sensor data, and e-mails.[1]

A novel protocol for protecting transmitted cookies using two dimensional one-way hash chains. In the first dimension, there is a hash chain that computes secret values used in the second dimension hash function. The optimal lengths of the chains are derived when the number of transactions in the session is known by adopting the position-indexed hashing protocol, energy consumption is reduced significantly especially with longer sessions making our protocol ideal for battery operated devices. Once the authentication credentials are used, they are recycled and never used again.

C. One-way Hash Cookie (OHC) Protection

Since we are using the one-way hash cookie protection Scheme as the backbone for our solution, it is worth illuminating its main aspects and how its hashing operation is carried out to protect cookies. In the OHC scheme, a one-way hash chain of length N is used to protect a stream of N transactions of a web session. During the initial HTTPS login step, the server and the client exchange a shared secret value S0, and a value N

which refers to the chain length or number of transactions expected to be handled during a session. The OHC protects the jth transaction by computing an authentication token VJ=HN-j+1(S0), where the notation Hm(x) implies applying the hash function m times, for example, H2(x) = H (H(x)). For instance, if N=100, then
The authentication tokens for the 1st, 2nd, and 3rd transactions are V1=H100 (S0), V2=H99 (S0), V3=H98 (S0), respectively.

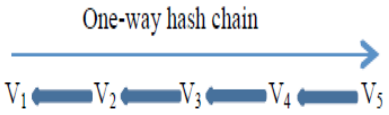

Figure 2. One-way hash chain [2]

Figure 2 illustrates how the one-way hash chains are configured. The straight arrow going from the left to the right corresponds to the length of the chain. In this specific figure, the length is 5 transactions. The small arrows going from the right to the left represent the points where authentication tokens are generated and checked. At each point in the hash chain, the server and client must be able to derive the same value of the authentication token. [2]

This solution achieves its goal by utilizing two one-way hash chains; one is responsible for updating the secret key and the other for creating the authentication tokens attached to the cookies using the secrets produced by the first chain. Use of SHA-1 for hash function to produce authentication tokens. Energy consumption is largely influenced by the cryptographic hash function used in the authentication scheme.

Table 1. Methodology with proposed one

Method	Description
HMAC (m ; k) Keyed-Hash Message Authentication Code	message m using key k
	Sk Server Key
	(m)k Encryption of message m using key k
High level confidentiality	Replay attack
	To provide authentication, integrity, and anti-replay.
HMAC (user name, expiration time, data, session ID, sk)	The cookie becomes session specific For example, in javex.net.ssl package, the function getID ()
	SSL session IDs are easier to obtain than SSL session keys.

The state-of-the-art secure cookie schemes was described by Fu et al. in their seminal paper [5]. In this section, we first examine this scheme, which we refer as Fu's cookie scheme. We show that this scheme has three major limitations, and we give a solution to each of them. Finally, we present our secure cookie scheme as shown in table 1.

III. RESULTS AND DISCUSSION

We prove that our cookie scheme is secure. First, our cookie scheme achieves authentication. A cookie created using our scheme can be used as an authentication token because no one can forge a cookie without knowing the server key sk, which is only known to the server. Note that HMAC is a one-way collision resistant hash function.

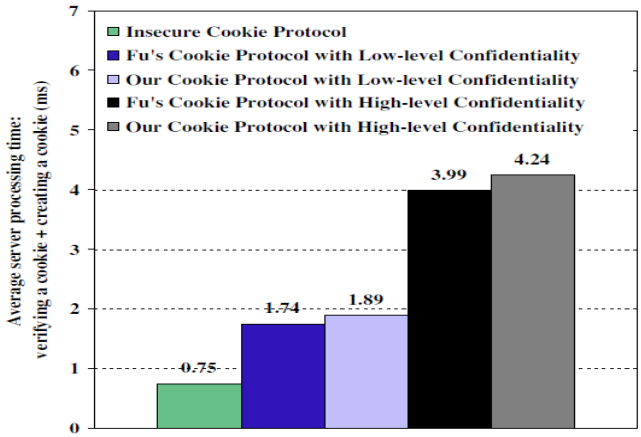

Figure 3. Server side performance comparison [2]

Second, our cookie scheme achieves high-level confidentiality. No one can obtain the key k for decrypting data without knowing the server key sk.

Third, our cookie scheme is secure against replaying attacks. Each SSL session ID is uniquely generated by a server; thus, the stolen cookie in one SSL session is invalid in another SSL session as the session IDs are different.

Fourth, for the user who receives a cookie from a server, from the hash HMAC (username, expiration time, data, session ID, k), they cannot infer any information about the data and the server key k because HMAC is a one-way collision resistant hash function. In other words, the user will not be able to choose a user name and even data that will allow them to infer the server key k. Note

that SSL session ID is sent in clear and scheme is secure against volume attacks because the data encryption key is used only in one SSL session.

IV.CONCLUSION

Cookies are the essential part for social media site to be more user friendly and user personalized. But the security of information residing in it is the questionable thing which should be analyse with appropriate solutions available. The time complexity and overhead are two concerns in which more evolution scope is exist which can be used as future work of research and analysis.

V. REFERENCES

[1] Noura Alomar, Mansour Alsaleh, Abdulrahman Alarifi, "Social Authentication Applications, Attacks, Defense Strategies and Future Research Direction : A systematic review": IEEE , 2016 DOI 10.1109/COMST.2017.2651741

[2] Amerah Alabrah, Mostafa Bassiouni "Robust and Fast Authentication of Session Cookies in Collaborative and Social Media Using Position-Indexed Hashing" IEEE, 2013

[3] Alex X. Liu, Jason M. Kovacs , Mohamed G. Gouda "A secure cookie scheme" elsevier, 2012 Department of Computer Science and Engineering, Michigan State University, East Lansing, MI 48824-1266, USA Exis Web Solutions Department of Computer Sciences, The University of Texas at Austin, Austin, TX 78712-0233, USA DOI: 10.1016/j.comment.2012.01.013

[4] Joon S. Park and Ravi Sandhu, George Mason University "Secure cookie on the web" IEEE, 2002

[5] Chuan Yue, Mengjun Xie, Haining Wang "An automatic HTTP cookie management system", ELSEVIER, 2010 Department of Computer Science, The College of William and Mary, Williamsburg, VA23187, United States DOI: 10.1016/j.comment.2010.03.006

[6] Paul Rabinovich "Secure cross-domain cookies for HTTP"
Springer,2016 Security Software Development, Exostar, Herndon,USA