SASy Username and Password Management on the Cloud

CONFERENCE PAPER · MARCH 2012

READS
118

1 AUTHOR:

Majid Nasiri Nejad
Multimedia University
2 PUBLICATIONS **0** CITATIONS

SEE PROFILE

SASy Username and Password Management on the Cloud

Majid Nasiri Nejad
Jan 22, 1984
Majid.nasirinejad@gmail.com
A-18-09 Rhythm Avenue USJ 19
47620 – Subang Jaya – Selangor – Malaysia
Tel: +60143146426
Year: 2010 - Course Title: Computer Science
Faculty of Information Technology
Multimedia University

Cyberjaya, Selangor, Malaysia

***Abstract*— In this paper, we will discuss the user authentication problems and difficulties to managing user names and passwords. In many cases the lack of standard rules for choosing User name and Password has made it really challenging to remember login information. We continue to propose a model and a technique for this issue and discuss the implementation and utilizing of this service.**

***Keywords*— web service, gateway, authentication, cloud security**

I. INTRODUCTION

Along the technology improvements and moving towards globalization, communication tools have also been developed. One of the most accessible and simplest communication tools is web sites which can be implemented with a very low cost. The web sites owners always do their best to interact with their users and Web 2.0 provides the suitable environment for this. Using open source platforms and proper support and redevelopment was the reason for increasing the number of web users as the producers.

The variety of communication tools has also been increased along with the web and internet enhancement. While years ago connecting to the internet was only through using PCs or laptops but these days tablets smart phones, GPSs, console game, book readers, TVs and many other electronic devices can use the internet by utilizing their unique hardware and operating systems. It is not far reaching to imagine that one day all the electronic and electrical devices access the internet and being controlled through that platform.

By influence of the internet on different aspects of human life, there is always an issue which makes the services providers and users concern, and it is the safety of information and communication.

Creating users identity verification structure in each web site is a simple way which has been improved rapidly and can provide part of this security for a limited period of time. It is difficult to find a web site which does not ask for a username and password to provide a service. The same as a citizen in a country which needs an ID card to be verified to use different services, by rapidly increasing numbers of online web sites if a user needs to ask for a service from the host or participate in a discussion or make a comment about a subject he or she needs to be identified and the username and password is the minimum requirements for the identification purpose.

In this research the most common websites which are being used by the users has been categorized as:

1. Email Services
2. Financial Services (Banks, Insurances, Stock Markets, ...)
3. Job Services (Companies, Universities, Business, …)
4. News Agency
5. Social networks
6. Interests (Weblogs, Personal web sites, Restaurants, Shopping and entertainment centers, …)

The minimum requirement for a user to use these websites is having a username and password.

II. PROBLEM STATEMENT

Despite using a variety of platforms for websites, the lack of standard rules for choosing User name and Password is obvious. When a user wants to use a web services he or she should sign up for that. To choose a password there are compulsory rules such as mixing numbers and characters. There are also some websites which following their rules is a real challenge for the users. For instance to sign up and sign in to an email account on Multimedia University, users must select at least one uppercase letter, one lowercase letter, one digit and one common character, with minimum length of 8 characters for the password. In addition some of the websites have rules for choosing a User name.

So the challenge is how a user should remember and manage the user name and password for each website? Our observation shows that, Amateur users prefer to write user names and passwords on a clear piece of paper and keep it near the computer or in their bags. Passwords are vulnerable to dictionary attacks and can be easily phished using a spoofed

web site. For example, a recent breach at a large web site showed that close to 1% of users choose “123456" as their password [1]. This is risky since it can cause leaking information and user data abusing. Moreover, since users tend to use the same password at many sites, a single server compromise can result in account takeover at many other sites. Florencio and Herley found that a single password is typically used to access over five sites [2].

Some other users save their password as a text file and store in nested folders but they are not aware that it is not a big challenge for software robots which perform disk storages mining.

Another group of users mostly use password manager software for controlling their data which are not really safe. Professional users use their algorithm for choosing suitable password so they need to remember the algorithm that they choose.

Now that the problem is clarified; we will discuss the target of this paper and our solution will be introduced.

III. Objective and Significance of the Study

There is a large body of work on formally verifying security properties of network protocols, including model checking using a variety of tools [3]–[6], constraint-based methods [7], and formal and automated proof methods [8]–[11]. The purpose of this paper is proposing a method to easily access websites account without memorizing Username and Password by making minimum changes on web service authentication system. This method doesn’t need to keep user’s data on a local storage and/or using third party software. Advantages:

- Doesn’t need to reconstruct authentication structure
- Choosing a Username and Password following web portal service rules
- Easy access by internet browsers and electronic gadgets (Java base)
- No monopoly and restrictions
- No monopoly for keeping data while encrypted information will be shared between 3 and more companies
- The users trust provider companies

IV. Background Research

Using authentication plug-in is common these days. These plug-in let users to use their social networks accounts for signing in to new websites or synchronies their accounts together. For example, Yahoo users can sign in with Facebook or Google account. Whereas Facebook, Google, Twitter and some other social networks have proper support, using of these plug-in are increasing on the websites.

Some of the websites need the user’s information (basic or complete) to allow using this plug-in which is risky for leaking data. Another problem will be happened when a website attacking by hackers or steal the security certificates so accessing to all the websites that users allow them are easily. On the one side the social networks are very useful today’s in user life but on the other side they are risks for organizations, offices, universities and etc when they user spend more times during work. Following this issue some organizations implement restrictions to access social networks during working hours, which can cause problems if client use SN’s gateway.

We believe that since the security of our computer systems was provided by security companies such as antivirus producer from many years ago social networks should not be directly fully responsible for their user accounts security. Protection of users’ data in the cloud space should be the responsibility of the security companies. From another point of view it is obvious that users would like to be sure about their information safety and also provider companies doesn’t have access to the data.

V. Operation

In this paper first we will have a general overview about the proposed system, and theoretical parts will also be discussed. This applicable system can be implemented using a variety of web services programs such as Java, PHP, C# .Net and so on that we can discussing it at the implementation stage. This system will be called “SASy” that is the short form of Safe Authentication System

A. *Responsibility: SASy*

At the beginning of this project three well known companies, Alpha, Beta and Gamma are invited to accept responsibilities of user authentication. By joining more famous companies to this project, this system can attract more and more users who trust the computer security companies.

B. *Prototyping*

1) First Stage- Signup in SASy: At first, user should surf SASy website and register as a new user. Basic user information is compulsory and each user needs a minimum one cell phone number, one active email address, an image of IC (like passport, driving license, national card, student card, and so on) and finger print scan (if device is applicable).

This information is encrypted using special algorithm and divided in to three parts that each part is stored in one of the Alpha, Beta or Gamma servers. When a user requests to authenticate, the information are read back from each servers for concatenating together.

In case of technical problems or cyber attacks one of the servers maybe shuts down, backup information is kept on the previous server but its reachable only by the permit of the company that its server is suspended. Since the companies use different encryption and storage methods with their own standard rules, it is so rare that two servers being attacked at the same time.

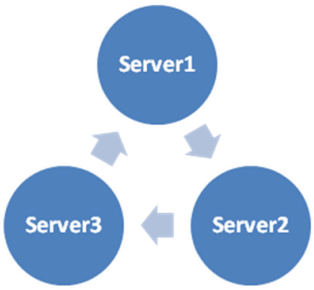

Fig. 1

2) Second Stage- First Entry: The first time entry and data entering process is shown in Fig. 2.

a. login page of web site.(for example Nasirinejad.ir)
b. Inserting Username and Password at the appropriate location.
c. Click on LOCK Icon.
d. In new page (Fig. 3), Input SASy Username and Password.
e. Click Add button.
f. In this level, SASy username and password is checked and if the process was successful, username and password of Nasirinejad.ir will be check.
g. If process "f" is passed website sends a packet to SASy to confirm that username and password are matched.

Fig. 2 Normal Login

Fig. 3 SASy Login

SASy store the encrypted Nasirinejad.ir account information without any rules on the storage table of SASy account.

3) Third Stage- Login: By special plug-in that provides a gateway, SASy accept authentication for other websites. When a user wants to use those websites services, can select one of the login methods.

a. Directly with username and password.
b. Or, Press Lock button for login and input SASy username and password then press Connect button. The entire ID's that user registered before on SASy's account shown to the user for choosing one of them.

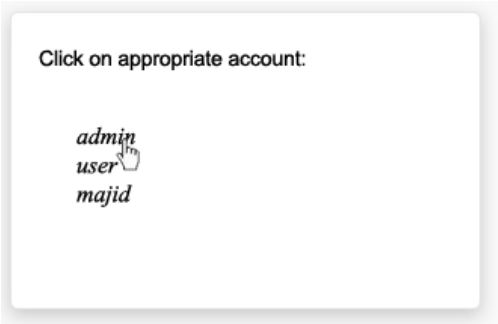

Fig. 4 Select an account

4) Fourth Stage- Username and Password review: If the user needs to change some parts of his or her profiles or maybe would like to change the password, should remembered the current password. If the user has forgotten the password can login to SASy website and recovers the password by using the private key that he or she has.

5) Fifth Stage- Forgetting SASy username and password: If the SASy user forgets the username or password, should follow two of three consecutive options:

a. Click reset password of one of the registered email addresses.
b. Upload an image of ID card that has been used for the first time registration.
c. Use fingerprint method

And finally should enter the PIN which is sent to the user's phone. RSA Mobile [12] is an SMS-based authentication system that requires the user to type a one-time password sent to their mobile phone into the computer's web browser in order to log in.

VI. Conclusion

To increase users' convenience and security, websites administrators can start providing a SASy gateway for sign-in and sign-up forms and notify their users to change their authentication method.

Since our technique is best implemented on Java, it can be used on many different electronic devices. Dividing encrypted data to 3 or more parts can increase the security compare to the methods used by common Password management software. Actually, more cooperation and interaction between computer security companies leads to attracting more users to this system.

Acknowledgment

In particular, I would like to thank Alireza Ahmadian Yazdi for discussing these ideas and reviewing earlier drafts of this paper.

References

[1] T. I. A. D. C. (ADC). Consumer password worst practices, 2009. www.imperva.com/download.asp?id=239.

[2] D. Florencio and C. Herley. A large scale study of web password habits. In *Proceedings of the 16th International Conference on World Wide Web*, pages 657-666, 2007.

[3] J. Mitchell, M. Mitchell, and U. Stern, "Automated analysis of cryptographic protocols using Muru," in Proc. IEEE Symp. Security and Privacy, 1997, pp. 141–151.

[4] J. C. Mitchell, V. Shmatikov, and U. Stern, "Finite-state analysis of ssl 3.0," in Proceedings of the Seventh USENIX Security Symposium, 1998, pp. 201–216.

[5] A. W. Roscoe, "Modelling and verifying key-exchange protocols using CSP and FDR," in 8th IEEE Computer Security Foundations Workshop. IEEE Computer Soc Press, 1995, pp. 98–107.

[6] D. X. Song, "Athena: a new efficient automatic checker for security protocol analysis," in Proceedings of the Twelfth IEEE Computer Security Foundations Workshop, June 1999, pp. 192–202.

[7] J. Millen and V. Shmatikov, "Constraint solving for boundedprocess cryptographic protocol analysis," in CCS '01: Proceedings of the 8th ACM conference on Computer and communications Security. New York, NY, USA: ACM, 2001, pp. 166–175.

[8] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," ACM Transactions on Computer Systems, vol. 8, no. 1, pp. 18–36, 1990.

[9] G. Bella and L. C. Paulson, "Kerberos version IV: Inductive analysis of the secrecy goals," in Proceedings of the 5th European Symposium on Research in Computer Security, J.-J. Quisquater, Ed. Louvain-la-Neuve, Belgium: Springer- Verlag LNCS 1485, 1998, pp. 361–375.

[10] A. Datta, A. Derek, J. C. Mitchell, and A. Roy, "Protocol Composition Logic (PCL)," Electronic Notes in Theoretical Computer Science, vol. 172, pp. 311–358, 2007.

[11] A. Datta, A. Derek, J. C. Mitchell, V. Shmatikov, and M. Turuani, "Probabilistic polynomial-time semantics for a protocol security logic." in Proceedings of the 32nd International Colloquium on Automata, Languages and Programming (ICALP' 05), ser. Lecture Notes in Computer Science. Springer-Verlag, 2005, pp. 16–29.

[12] "RSA Mobile: two-factor authentication for a mobile world" RSA Security, 2002.