ChaMAILeon: Usable email sharing like never before!

Prateek Dewan, Niharika Sachdeva, Ponnurangam Kumaraguru
Indraprastha Institute of Information Technology - Delhi
{prateekd,niharikas,pk}@iiitd.ac.in

ABSTRACT

While passwords, by definition, are meant to be secret, recent trends in the Internet usage have witnessed an increasing number of people sharing their email passwords for both personal and professional purposes. As sharing passwords increases the chances of your passwords being compromised, leading websites like Google strongly advise their users not to share their passwords with anyone. We conducted an online survey with 228 participants to study users' general password sharing trends, and found that 62.72% participants felt a need to share their email passwords. Further, about 77% participants said that, if given the opportunity, they would want to use a system which could provide them with certain access control features in their email. To address the concerns of users who need to share passwords, we introduce ChaMAILeon, a system which allows users to share their email while maintaining their privacy and not compromising their security. We present a novel approach of sharing emails, by allowing users to create multiple passwords for a single email address, with customizable access control rules. Each password gives a different view of the email account, thus allowing, say, a supervisor, to allow her assistant to read only her official emails, and hide your personal emails from her. We are presently conducting controlled experiments to determine the usability of the system.

1. INTRODUCTION

The main aspect associated with a password is its secrecy. Leading Internet giants like Google, Yahoo etc. highly recommend that their users do not share their passwords with anyone. [1] [2] However, it has been observed and studied worldwide, that users come across a wide variety of scenarios in their day-to-day lives, where they share their password with other users. A study of banking and security in Australia unveiled the practice of sharing passwords [7]. In the real world, leading executives have expressed the need to share their email accounts with their assistants, in order to be more productive [5]. Sharing passwords amongst teenagers has also become a trend in the recent times. Pew Internet research [3] recently found that 1 in 3 teens surveyed share passwords with a friend, boyfriend or girlfriend [6]. Pew reported that while passwords may be guarded closely by some youth, password sharing among peers can be a sign of trust and intimacy. Some of the downsides to this include obsessive scouring of a significant other's account for signs of infidelity and using the access for sabotage when a relationship goes sour; as reported by a New York Times article.

Most of the existing work undertaken to solve the problem of password sharing, like [1, 2, 3], indicates that there is a need for email management systems where emails can be shared with other human delegates / users, while maintaining the owner's privacy and without compromising on security. However, the current state of the art does not completely fill this gap. While [2, 4] do not cater to the need of the owner's privacy, [1, 3], are yet to find deployment as working systems. To the best of our knowledge, there exist no systems for sharing email accounts (or passwords), which successfully address a common user's need to share, and her desire to maintain her privacy simultaneously.

To cater to this problem of password sharing, we introduce ChaMAILeon, a system and approach which allows users to share their email while maintaining their privacy and not compromising their security. We present a novel approach of sharing emails, by allowing users to create multiple passwords for a single email address. Access control rules are customizable, and are mapped to the different passwords associated with an email account.

2. METHODOLOGY

To explore users' password sharing practices and expectations, we conducted an online survey with 228 participants. Based on the insights from the survey, we designed ChaMAILeon. We tried to build a generic framework to incorporate as many features as possible, from the users' requirements and concerns, as found in the survey.

2.1 Online Survey

We first conducted an online survey to study users' general password sharing trends and practices. The motivation behind conducting this survey was to discover users' intent towards sharing their email passwords and see how comfortable they were in doing so. In addition, we also captured if users were willing to use a system which provided them with various access control features on their emails during 3 example scenarios. In all, 228 respondents from various ethnic backgrounds participated in the survey. The survey was open to everyone, and was publicized on Facebook and through word of mouth. As an incentive, participants were also given the option to participate in a lucky draw by submitting their contact information (email ID).

3. SURVEY RESULTS

3.1 Current user behavior and expectations

Participants showed contradictory behavior to what was recommended by the email services they were using. We asked participants in the survey, if they share or feel the need for password sharing of the email accounts, and found that 62.72% participants mentioned a need for sharing email passwords. To support our findings, we visited their security policies and found that both of these services highly recommended their users not to share passwords.

[1] https://accounts.google.com/PasswordHelp
[2] http://help.yahoo.com/kb/index?page=content&y=PROD_ACCT&locale=en_US&id=SLN3012&impressions=true
[3] http://pewinternet.org/

Most participants (74.56%) were not comfortable sharing passwords. Further, upon asking, 88.59% participants mentioned that they thought password sharing may lead to unwanted consequences. We found that 96.92% users felt the need to change their passwords after sharing. These results indicated to user worries and uneasiness when they share the passwords and formed reasonable need for a systems which could help users with easy and fearless email sharing.

3.2 Need for a system

To better understand the exact system utilities, features and requirements, we gave users a scenario, in which a system allows them to control the accessibility of their emails / settings / features, when they share their password.

Share emails with spouse: Here, we asked the users to consider a situation, where they wanted to share their email with their spouse, but did not want him / her to see emails from a particular friend, or did not want him / her to be able to reply to any emails. We then asked them if they were willing to use a system which could provide them with this functionality, and found that 64.91% users were willing to use such a system.

Share emails with assistants: We asked users to consider a scenario where they were an official at a big post in a company, and received a lot of emails every day. They wished to allow their assistant to be able to log into their account and reply to emails on their behalf. However, they would want the assistant to be able to see emails sent from only specific people, and not all of them. We found that users felt the need for such a system more in a professional environment, as compared to the previous scenario, with 84.21% agreeing to use of such a system in the current scenario.

Accessing emails in insecure environment: We asked, if users were in a cyber cafe where they were not sure if the network was secure, and they needed to check their email. In such a setting, users would be afraid that their password and email content might get compromised over the insecure network. Under such a scenario, they were given an option to log into their account with a different password, such that, logging in with this password would give them very limited access to their account. In addition, their important emails would be filtered at the server level, and would not be transmitted to them over this insecure network. Almost 83% participants mentioned that they would use such a system.

4. SYSTEM DESIGN

In response to the results of the online survey, we developed ChaMAILeon, an email application which provides users with the features described in the survey scenarios. ChaMAILeon is a modified version of SquirrelMail, [4] an open source email package built using PHP. SquirrelMail was altered to support a "Configure Account" option to enable users to get control over their email accounts. We configured ChaMAILeon to work with Gmail. Figure 1 represents how ChaMAILeon communicates between a user and Gmail, and the tasks it performs.

Technically, ChaMAILeon adds two new features to the existing web mail technology, which alters the way the conventional email works. First, it allows the owner of the email account to create "sub-users" for their email account. A

[4] `http://squirrelmail.org`

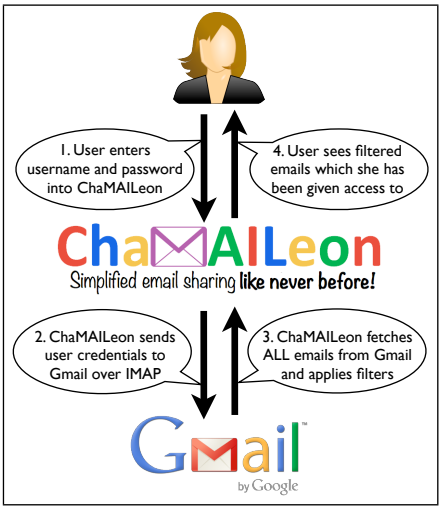

Figure 1: Flow diagram depicting how ChaMAILeon works as a middleware between a user and Gmail's mail server.

"sub-user" essentially corresponds to a new password which can be used to access this email account. ChaMAILeon thus allows to log into one email account using one email ID and multiple passwords. Each password (or sub-user) can be configured by the "owner" of the email account, to provide different views of the email account and grant different permissions. Secondly, ChaMAILeon provides the owner of the account, with an option to create "lists". Each list is simply a collection of email addresses clubbed together under one name; the name of the list. The advantages of creating such lists are realized through configuring the sub-users. Each list can act as a black-list or a white-list for a sub-user. i.e. a sub-user can be allowed / restricted to "send to" and "read emails" from a "list" of email addresses specified in the list. A combination of sub-users and lists form a powerful and robust mechanism to generate and implement fine-grained access control rules on emails.

5. REFERENCES

[1] S. Best, J. Girouard, and T. Snow. Handling email communications having human delegate prepared summaries, Nov. 9 2010. US Patent App. 12/942,216.

[2] Google. Set up mail delegation. 2012.

[3] M. Hudecek. Auto-forwarding and auto-delegating email folder control, Jan. 7 2005. US Patent App. 11/030,818.

[4] T. Hunt. Mifrenz: Safe email for children. *New Zealand Journal of Applied Computing and Information Technology. Volume*, 12(1), 2008.

[5] M. Hyatt. Managing email with an assistant. *Michael Hyatt Intentional Leadership*, 2010.

[6] A. Lenhart, M. Madden, A. Smith, K. Purcell, K. Zickuhr, and L. Rainie. Teens, kindness and cruelty on social network sites. *Washington, DC, Pew Research Center*, 2011.

[7] S. Singh, A. Cabraal, C. Demosthenous, G. Astbrink, and M. Furlong. Password sharing: implications for security design based on social practice. In *SIGCHI Conference on Human Factors in Computing Systems*, CHI '07, pages 895–904, New York, NY, USA, 2007.