Improving Online Account Security: Implementing Policy and Process Changes

Pankaj Goyal
MicroMega Inc.
Denver, USA
e-mail: Pgoyal@micro-mega.biz

***Abstract*— User authentication, a difficult problem, suffers from various shortcomings with the prevalent use of passwords as an authentication method. Requirements for password memorability and usability make them easy to break. Password reuse across sites, including insecure sites, phishing and spoofing attacks, requires that financial institutions examine security by analyzing end-to-end processes and identities involved. This paper presents an approach for intrusion tolerance, and the necessitated changes to processes and policies.**

Keywords - online security; transaction security; identity security; security policy; financial systems; intrusion tolerance

I. Introduction

User authentication is one of the most difficult problems in Internet security [19]. Passwords are ubiquitous in their use for authenticating users and pose the biggest security challenge. Users frequently forget passwords, necessitating expensive customer support calls or automated backup authentication schemes often involving challenge questions, that are even weaker forms of authentication. Users also can have their passwords stolen through phishing [5, 11], social engineering, man-in-the-middle (MITM) [13], and key-logging attacks, or they may share [32]. Most of the issues related to passwords have been well documented and numerous efforts to alleviate some of these issues have been proposed and implemented; a complete survey of the literature is beyond the scope of this paper but some of the methods are surveyed in Section II. Passwords because of their usability, ease of implementation, etc., are unlikely to be dislodged as the user authentication method of choice for online services; Herley et al. [19] lists a number of barriers to move away from passwords with a major obstacle being the diversity of requirements.

People today, are subscribers of an increasing assortment of online services: news, social networking, shopping, financial and medical. Unfortunately, users have a difficulty in creating unique, easily memorizable, secure passwords for all the services that they use. Thus, users tend to use something from their background (family, friends, pets, history, likes, dislikes, etc.) for creating passwords and overwhelmingly tend to reuse passwords across services; it should be noted that the security mechanisms of these service sites is as varied as their nature and content. Users password entropy is likely to remain constant, while the number of services that a user subscribes to increases and as does the adversary's computational power) and access to users personal information.

Attempts to address some of the weaknesses in password security include multi-factor authentication to increase security of a password-based system. Multi-factor authentication involves the use of more than one mode in the authentication processes, for example, two-factor authentication can be implemented by coupling the use of passwords with (1) a security-challenge or (ii) a code sent over another communication channel (example, mobile phone) that the user is then required to enter. These schemes still suffer from vulnerabilities, in particular, the real-time man in the middle attack. Password management, including password retrieval and resets, are major issues and areas of vulnerability. The efficacy of security-challenge questions, however, in the era of easy availability of personal data is in serious doubt.

In this paper, we present an approach for intrusion tolerance of a security system for a financial institution (FI). As part of the analysis, many best practices, their advantages and risks were examined and attempts made to find robust solutions to address these risks. In addition, the design attempted to protect victims of phishing or other attacks where the victim's password has been compromised. The analysis led to definition of policies and processes to ensure *authorization* of all sensitive actions – actions that can negatively impact the legitimate user and/or FI. Authorization is implemented using only an out-of-band communication channel, so that it is not susceptible to a real-time man in the middle attack over the primary interaction channel.

Section II presents an overview of the current approaches and their limitations. Passwords (or their predecessor watch-words) and associated vulnerabilities have existed for millennia. It is a given that attacks on authentication schemes will continue and get more sophisticated. It is, thus, not enough to attempt to secure passwords, use processes to manage password change and use of a separate channel for on-time passwords (OTP) or authorization codes. If a password change requires authentication but, say, the email address in the profile does not, then an attacker on gaining entry would first alter the email address thereby by blinding the actual owner of all changes to its account. In the natural world, a financial transaction involve multi-channel interactions and authentications. Thus, what is required, in the online world, are methods and processes that minimize damage in case of password compromise. In Section III, this paper presents a systems approach to identify at risk items and activities from a compromise of authentication systems, and methods and processes for intrusion tolerance so as to mitigate financial losses. The proposed schemes use bi-directional multi-channel interactions, use methods and processes to authenticate profile changes.

II. Background and Related Work

The increased use of computer systems is accompanied by an increased, and increasingly well-organized, attempts to breach their security. One of the most vulnerable elements of security is the *password*. This is also the most common method of user authentication. Once authenticates, the user is restricted to perform only authorized activities.

Authentication: is a means of verifying that a user is who they claim to be. In the process the user presents a *user-identifier*, representing the user's identity, and a set of *credentials* (e.g., password or certificates). The user is granted access to the service only on verification of the user-identifier and the credentials.

Authorization: determines whether the client is allowed to perform certain tasks or operations. Authorization enforces policies that controls access to activities, resources or services.

Identity management is concerned with users' credentials and their access to services. Identity management systems consist of an authentication part which is used to verify the correctness of an entity's claim to identity, and an access control part, authorization, which grants access to applications and resources. User-identifiers represent our digital identities, who we are, when engaging in online activities and transactions. Ideally, users should choose different user-identifiers (user-ids) for each service, however, this would require users to memorize user-id's in addition to passwords; this is not practical as analysis of passwords use has shown that users tend to reuse passwords [14]. Identity management is also a major issue of concern but is not the focus of this paper; for an introduction into issues related to usability and privacy, see [20].

A. *Password Management*

A big inconvenience in password based authentication is that ideally a user should memorize and use different passwords for different services and that these passwords should not be easily breakable. If a common password is used across all services then a service (or an attacker with knowledge of the common password) can impersonate a user to another service or a service can impersonate another service to the user. Password reuse across multiple services increases their vulnerability as compromising a single password allows an attacker access to multiple accounts. Gaw and Felton [14] conducted an experiment and found that password reuse rates increased over time because people subscribed to more services but did not create more passwords as reusing passwords made passwords easier to manage. Also sharing passwords among relatives and close friends has been found to be a sign of trust and intimacy [32].

Forcing people to choose and remember strong passwords - those that tend to be long character strings including both Roman letters and digits - is unworkable because such passwords are also unmemorable [12, 23]. Bellovin and Merritt [3, 4], Gong et al. [17], and Lomas et al. [25] have proposed authentication protocols that are resistant to password guessing attacks but with the added cost of additional messages; Gong [16] optimized the number of messages and cycles required.

Passwords are frequently deployed in an insecure manner. The large inconsistency of implementations between sites and the frequency of simple mistakes show an unanticipated level of insecurity and confusion [2]. While a site may not hold critical information and, thus, use simple security measures, a compromise of its security can allow the attacker to gain access to a compromised user's critical account on another site because of the reuse of user-id's and passwords. Given this threat of cross-domain password attacks, insecure sites collecting passwords have the potential to impose a costly externality on more careful sites.

Mobile phones and various other types of trusted mobile devices have been suggested as a means of achieving a two-factor authentication through devices that we routinely carry. Alternatives to passwords for authentication include Public-key infrastructure (PKI) but PKI security has been successfully compromised. Sotirov et al. [33] identified a vulnerability in the Internet Public Key Infrastructure (PKI) used to issue digital certificates for secure websites. They executed a practical attack scenario and successfully created a rogue Certification Authority (CA) certificate trusted by all common web browsers. This certificate would have allowed them to impersonate any website on the Internet, including banking and e-commerce sites secured using the HTTPS protocol; successfully used in a number of high profile cyber-attacks including compromise of Microsoft Update program (allowed 'Flame' malware to spread). It should be noted that the CA issuing authorities GlobalSign, Comode and DigiNotar have all been hacked. Biometrics suffer from deployment scaling, privacy and authentication from untrusted hardware.

Weir et al. [37] compared three different authentication processes, a 1-factor and two 2-factor methods. They found that convenience and personal ownership as some of the most important criterion in user preference of authentication methods and majority of the study participants perceived the 1-factor method as being the most secure and most convenient option. In their study experienced users gave higher usability scores to the 1-factor method they currently use.

Over the years, a variety of solutions have been proposed to the issue of password management. Bonneau and Preibusch [7] provide a broad overview of password history and management research. Anderson [2] provides a comprehensive overview of security engineering.

B. *Password Management Systems (PMS)*

Typical PMSs allow password resets online, including when a user runs out of the allowed number of retries, and some inform the user by email that a password change was made. In the era of email overload (and phishing attacks), by the time a user reacts to this informational message the damage might be done.

For example, certain sites that do not engage in any financial transactions may implement loose security policies and controls, such as, easy retrieval of passwords (clear text). But with the prevalence of passwords use across cross-sites this is a serious vulnerability. Some sites use security challenge questions to allow a user to reset their passwords; this is also allowed when a user runs out of password tries. These challenge questions, and their answers, are typically based on the user's background. With the increasing availability of online personal data, including through social networking sites of even such information as friends and pets, the efficacy of these security challenges is seriously in doubt. Secondly, they are vulnerable to real-time man in the middle attack.

FIs are starting to deploy dynamic challenge questions and two-factor authentication; the term FI includes online shopping, gaming, etc., as the issues faced by these online systems are similar. Challenge questions are commonly used to authenticate users who have lost their passwords. The PMSs that allow password resets on successful answer to a set of challenge questions suffer from the fact that increasing amounts of personal data is widely available online. Patterns have been found to exist in the security questions [21, 28]. An analysis of user-generated challenge questions found that 34% of user questions asked for a human name, 15% asked for a pet name and 20% asked for a place name [21]. Of the remainder, 22% asked for a user's favorite item amongst films, singers, car brands, etc., 5% asked for a time, date, or number, and the remainder were ambiguous. Thus, a few simple categories of proper names cover roughly 70% of real-world questions. While personal security questions may have had their use when there was scarce online or easy availability of personal information, however, with the ubiquitous availability of personal information online, the security provided by such questions is doubtful.

C. Password Managers

The objective of password managers is to be able to use complex, not easily breakable, unique passwords for user authentication by service providers while the user utilizes a simple easily memorizable password for password manager access.

One approach is to create centralized, trusted authentication services, such as Microsoft's Passport initiative [26] and its security has been analyzed [24]. Such centralized services require both users and service providers to place their trust onto a centralized service ("Big Brother") and every service that would use the centralized system for authentication would need to make changes to their systems.

Another proposal lets users choose their own passwords and then store them in a safe, for example, Password Safe application [31] stores the data in an encrypted database on the user's machine, secured with a user-chosen master password.

Another method assigns fixed passwords for each site or service that can be computed whenever they are needed. For example, the Lucent Personal Web Assistant [15] operates as an HTTP proxy server that users access with a master username and password. They can then tag web site password fields to be automatically filled in with values derived from a hash-based function of the user's master password and the domain name of the web site.

PwdHash [29], a user web browser plug-in, applies a similar hash-based technique. Password Multiplier [18], is also a user web browser plug-in, extend the approach of Kelsey et al. [22]. In Kelsey et al's method [22], the password is derived by repeatedly iterating a hash function on the original master password. Halderman et al. [18] compute the site-password in two steps. In the first step, an interim value is derived by applying the secure hash function is iterated k_1 times on the concatenation of the username and master password. In the second step, the site password is derived by applying the secure hash function is iterated k_2 times on the concatenation of the site name, master password and the interim value from step 1. Chiasson et al. [9] evaluate PwdHash and Password Multiplier suffer from major usability problems that cause security exposures – exposures that the users are unaware of. Also, password managers cannot prevent MITM attacks.

D. Single Sign On (SSO)

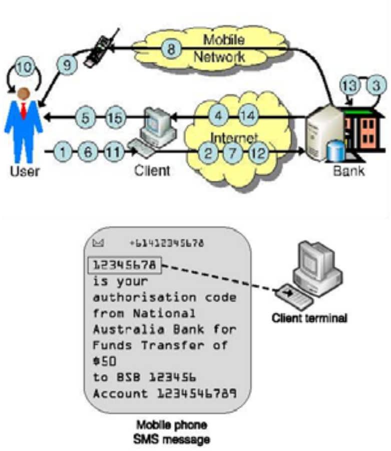
Fundamentally, Web single sign-on (SSO) systems shift the functions of identity collection and authentication from the content servive provider (CSP) to Identity Providers (IdP); in the process the CSP becomes a relying party (RP) of the IdP. An IdP issues identities or credentials to users, while an RP depends on the IdP(s) to assert the user credentials before allowing access to its services. This enables users to leverage one identity across multiple RPs.

An inherent risk of usingWeb SSO is that one compromised account on an IdP can result in breaches on all services that use this compromised identity for authentication. The SSO introduces a single point of failure or compromise -- the IdP systems and infrastructure [27]. An inherent characteristic of web applications is that some of the internal information flows are inevitably exposed on the network and encryption is insufficient to safeguard against information leaks [8]. Users may become accustomed to being redirected to identity provider web-sites for authentication. To prevent phishing attacks, users must verify the authenticity of an identity provider before entering their credentials.

Users and the RP have to trust the integrity of the IdP. In web SSO ecosystems, the issue of liability becomes highly complex as the integrity of the ecosystem depends upon the quality of the implementation of the IdP and all RP clients of the IdP; Wang et al [36] list the issue of implementation complexity as a major issue for SSO's. A number of researchers have investigated flaws in the protocols and implementations of such systems and surveyed [8, 27, 34, 36].

E. Man-In-the-Middle Attack (MITM)

It is possible for an attacker to intercept the communication between the customer and the FI server and impersonate them both [13]. The attacker tricks the customer into logging into the attacker's website, and masquerade as the real FI. This can for example happen through the attacks commonly known as *web spoofing* and *pharming* [5, 13].



12345678
is your
authorisation code
from National
Australia Bank for
Funds Transfer of
$50
to BSB 123456
Account 1234546789

Figure 1. Authorizing bank transactions via SMS (from AlZomai [1])

To counter MITM, some FIs use an OTP (One-Time-Password) to authorize each transaction (Fig. 1); also, referred to as the authorization code. It is common to send the authorization code through an out-of-band channel, for example, email or a mobile SMS; out-of-band channels are also referred to as authorization channels while the primary interaction channel is known as the in-band channel. The transaction authorization method based on SMS messages was introduced by FIs in response to phishing attacks. However, an investigation of the security and usability of SMS-based transaction authorization method and found that it is vulnerable to stealthy attacks, such as minor changes to account numbers [1]. The scheme also suffers from the fact that the user has to enter the authorization code using the in-band channel – potential for mistakes and still subject to a sophisticated MITM attack.

F. *Combining Text and Graphics*

In an attempt to counter password theft through phishing attacks and to differentiate real sites from spoofed sites, mix of text and graphic passwords have been proposed [10, 35]. Some online FIs employ site verification schemes; for example, SiteKey [6] displays a user selected image back to them at login. But, an empirical study [30] found that users will still enter their passwords when presented with fraudulent messages claiming that the image authentication server is down.

III. Financial Institution (FI) Situation and Analysis

The FI allows users to perform financial transactions online, including deposits, bill and recurring payments, and also sells certain financial and FI-related items (coin collections, piggy-banks, etc.) that are then shipped to the user specified address.

A. *Problem*

Based on analysis of available literature and experimental results (some of these are referenced in Section II), it was clear that (a) all identity credentialing and authentication schemes are vulnerable, and that these credentials can become known to attackers; and (b) passwords have to be used for user authentication. It was also clear that in the current environment challenge questions are ineffective and, while they would be implemented for psychological comfort, will not play any role in user authentication. The FI was interested in intrusion tolerance mechanisms that could minimize impact of, say, MITM attacks, and in using transaction authorizations.

B. *Challenges*

Let us consider the situation where the attacker has gained access to the users' identifier and password; the attacker takes control of the account and make changes to, say, the email address and mobile phone number, or add payees, etc.

It is not typical of online sites to inform users if, say, their email address or phone number have been changed. The email address change prevents the victim from receiving notices of password change, including links that allow password changes to be made; instead the attacker will receive them. The mobile phone number change allows the attacker to receive the transaction authorization SMSs.

TABLE I. Terms

(…)	tuple of items
{…}	set of items
A_i	Attribute name
a_i	value for attribute A_i
Account	(Account-Type, Account-Identifier, {(Account-Actions, Limit), …})
Address	mailing, shipping, billing, primary/secondary email, SMS
Authorization Action Channels (AAC)	are associated with a ROC and user action
Channels	postal mail, email, Fax, Voice call, browser, smart phone app
Identity	{ (Identity-Attribute, value), ….. }
Identity-Attribute	Name, Address, Phone, Account, Identity-Category
Identity-Category	Self, Payee, Beneficiary
Name	User/Account Holder, Payee, Beneficiary [e.g., Family-Friends]
Phone	Home, Work, Mobile, Other, Fax
Request Originating Channel (ROC)	channel through which any user action is requested (for example, logging in)
User Actions	login, delete/add/change any profile information

A number of other challenges were analyzed. During the analysis a number of terms were identified (Table 1; not all terms identified) and it became clear that users needed to be informed of any identity changes. A more stringent and secure criterion is that any identity change needed to be authorized through an authorization channel distinct from the request originating channel; this is different from the currently used methods where the authorization is performed on the request originating channel. The primary purpose of the analysis and the formalization of terms was to identify at risk items – items that can contribute to circumvent security.

C. *Interaction Channels*

At the FI, the following channels can be used to originate requests, including changes to user profiles and accounts:

- Paper, typically signed forms and letters
- Telephone (only from registered phones)
- Web site
- *In person*

For each of these requesting originating channels, alternate authorization channels are specified (Table 2); it is possible for users to choose a preferred authorization channel. Emails are used as a notification method and contain instructions on how to perform the requested authorization. Originating requests in person allows the FI personnel to physically authenticate the user and the user authorizations the actions by signing documents (may be online).

TABLE II. AUTHORIZATION CHANNELS FOR REQUEST ORIGINATING CHANNELS

Request Originating Channel	Authorization Channels
Paper	Email, Paper (signature), SMS, Telephone
Telephone - Landline	Email, Paper (signature), SMS
Telephone - Mobile	Email, Paper (signature)
Web site	Email, Telephone, SMS
In Person (face to face)	At service/interaction point; receipts may be transmitted by Email

D. *Policy Changes*

- All changes, including add/delete, to identity require explicit user authorization
- New financial transactions require explicit user authorization
- On users' initiation of a change to identity or a new financial activity, the change/activity will be put in pending status and, thus, are effectively inactive.
- All authorizations must be made through a channel distinct from the request originating channel.
- Both authorization requests and user responses to these requests must be made on the authorization channel.
- A change in pending status is made active or inactive based on the user authorization response.
- Challenge questions shall play no role in making decisions about a users' identity
- In person (physical presence) on the presentation of valid photo-id shall allow the user to request immediate changes with authorization received in the form of users' signature.

E. *Process Changes*

Every process that deals with users (interactions), user profiles, and user accounts is affected. Some of the major process changes were to call center processes as the policy changes impacted a number of processes. For example, customer service representatives could no longer reset passwords on the phone, or make changes to emails – any change to identity; they should mark the requested changes to be pending status and await authorization through an alternate channel.

F. *Impact of these Changes*

1) *Password compromise*

The affect of these changes is that even with the attacker logged into the victims' account, the attacker is prevented from making changes to the victims' identity. Thus, for example, the attacker cannot make a change to the victims' registered email address or mobile number; any changes will need to be authorized by the victim before they can take effect and such authorization will occur through a different channel. Similarly, the attacker cannot add a new beneficiary or payee or make changes to their addresses or account details. Thus, the attacker is effectively prevented from causing any harm to the victim.

2) *Man-in-the-Middle (MITM) Attack*

Similar to the password compromise scenario (above), the attacker is unable to authorize its illegal gain activities, as all authorization will occur on a channel different from the channel that the attacker has spoofed.

It should be noted that there is no defense against an attacker who has total control over the victim, viz., the attacker has control over all possible communication channels.

G. *Other Design Options*

It is possible to construct channel use charts where for each request originating channel a set of approved authorization action channels are defined. During the design phase it was decided against including this extra level of complexity as the potential benefits were not clear.

There was considerable debate on whether authorization should be required for any transactions above a certain minimum amount. Since, any beneficiary or payee identity would be created only on explicit authorization any benefits of a transaction would accrue to members of the account holder's circle and that any benefit would be subject to the upper limit for that identity. The problem with creating exceptions is that there is a cost of implementation and ongoing costs as changes to exceptions are made. Secondly, any activity not initiated by the account holder is still a major inconvenience both to the account holder and the FI.

H. *Usability*

Users have the option to opt out of out-of-band authorization for certain profile changes and low-value financial transactions; users can not opt-out of financial transactions above a FI defined threshold, nor can they opt out of authorizing changes to their passwords, email address and authorization channel information. Given that an attacker would be unable to gain financially it is expected that attackers would concentrate their attention elsewhere.

Authorizations utilize automated systems, similar to those utilized to automatically activate credit and debit cards. Thus, there is no extra burden on call center representatives.

ISBN: 978-1-61208-209-7

IV. Conclusions

Passwords are likely to retain their predominant position in user authentication. With the increase in the sophistication of phishing and man-in-the-middle attacks, cross site use of passwords by users, sharing of passwords and the wide availability of personal information, requires that FIs assume password compromise, including knowledge, and devise intrusion tolerant processes and policies to minimize adverse effect on their customers and themselves. Most of the methods proposed by researchers address one or two shortcomings of passwords, for example, password breakability. Security implementations at online sites do not consider end-to-end impacts of password compromise. This paper has presented some of the outcomes of a comprehensive analysis and methods incorporated in the design of an FIs security system tolerant to malicious intrusions. One of the characteristics of the design requires that any change to an identity/profile requires user authorization, say, using mobile networks as an authorization channel. With near ubiquitous use of mobile devices these methods are not onerous.

Identity credentialing and authentication methods, other than passwords, are also not immune from compromise. The complexity of some implementations [36] may introduce vulnerabilities that require new methods and tools to detect. In the absence of faultless systems and processes, it is incumbent on organizations to analyze intrusion impacts, and introduce intrusion tolerant systems, processes and policies. These intrusion tolerant schemes have to be designed by each organization based on their risk exposure.

References

[1] M. AlZomai, B. AlFayyadh, A. Jøsang, and A. McCullagh, “An Experimental Investigation of the Usability of Transaction Authorization in Online Bank Security Systems,” Sixth Australasian Conference on Information Security, pp. 65-73, 2008.

[2] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, Second Edition, Wiley Publishing, 2008.

[3] S.M. Bellovin and M. Merritt, “Augmented Encrypted Key Exchange: A Password-Based Protocol Secure Against Dictionary Attacks and Password File Compromise,” 1st ACM Conference on Computer and Communications Security, pp. 244-250, 1993.

[4] S.M. Bellovin and M. Merritt, “Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks,” IEEE Symposium on Security and Privacy, pp. 72-84, 1992.

[5] H. Berghel, ‘Phishing mongers and posers’, Communications of the ACM, 49(4), pp. 21–25, 2006.

[6] Bank of America SiteKey. http://www.bankofamerica.com/privacy/sitekey/ [retrieved: March 2012].

[7] J. Bonneau and S. Preibusch, “The password thicket: technical and market failures in Human authentication on the web,” The Ninth Workshop on the Economics of Information Security (WEIS 2010), 2010.

[8] S. Chen, R. Wang, X. F. Wang, and K. Zhang "Side-Channel Leaks in Web Applications: a Reality Today, a Challenge Tomorrow," IEEE Symposium on Security and Privacy, pp. 191-206, 2010.

[9] S. Chiasson, P.C. van Oorschot, and R, Biddle, “A Usability Study and Critique of Two Password Managers.” 15th USENIX Security Symposium, 2006.

[10] S. Chiasson, Usable Authentication and Click-Based Graphical Passwords. PhD thesis, Carleton University, Ottawa, Canada, January 2009.

[11] R. Dhamija, J. Tygar, and M. Hearst, “Why Phishing Works,” SIGCHI conference on Human Factors in Computing Systems, pp. 581-590, 2006

[12] D.C. Feldmeier and P.R. Karn. UNIX Password Security - Ten Years Later. Crypt0 ‘89, volume 435, Lecture Notes in Computer Science, Springer-Verlag, pp. 44-63. 1989.

[13] E. Felton, D. Balfanz, D. Dean, and D. Wallach. Web Spoofing: An Internet Con Game. 20th National Information Systems Security Conference, also Technical report 540-96, Princeton University, 1997, http://www.princeton.edu/sip/pub/**spoofing**.html [retrieved: February 2012]

[14] S. Gaw and E.W. Felton, “Password management strategies for online accounts,” SOUPS '06 Proceedings of the second symposium on Usable privacy and security, pp. 44-55, 2006.

[15] E. Gabber, P.B. Gibbons, Y. Matias, and A.J. Mayer, “How to make personalized web browsing simple, secure, and anonymous” Financial Cryptography, pp. 17–32, 1997.

[16] L. Gong, “Optimal Authentication Protocols Resistant to Password Guessing Attacks,” Eighth IEEE Computer Security Foundations Workshop (CSFW '95), pp. 24-29, 1995.

[17] L. Gong, T.M.A. Lomas, R.M. Needham, and J.H. Saltzer, “Protecting Poorly Chosen Secrets from Guessing Attacks,” IEEE Journal on Selected Areas in Communications, 11(5).pp. 648-656, 1993.

[18] J.A. Halderman, B. Waters, and E.W. Felten, “A Convenient Method for Securely Managing Passwords,” 14th Intl Conf on World Wide Web (WWW’05), pp. 471-479, 2005.

[19] C. Herley, P.C. van Oorschot, and A.S. Patrick “Passwords: If We're So Smart, Why Are We Still Using Them?” Financial Cryptography and Security, pp. 230-237, 2009.

[20] M. Josang, S. AlZomai, and S. Suriadi, “Usability and Privacy in Identity Management Architectures,” Fifth Australasian Information Security Workshop: Privacy Enhancing Technologies (AISW 2007), pp. 143-152, 2007.

[21] M. Just and D. Aspinall, “Personal Choice and Challenge Questions: A Security and Usability Assessment,” 5th Symposium on Usable Privacy and Security (SOUPS’09), 2009.

[22] J. Kelsey, B. Schneier, C. Hall, and D. Wagner, “Secure applications of low-entropy keys” *Lecture Notes in Computer Science*, 1396, pp. 121–134, 1998.

[23] D.V. Klein, “Foiling the Cracker: A Survey of, and Improvements to Password Security,” 2nd USENIX Unix Security Workshop, pp. 5-14, 1990.

[24] D.P. Kormann and A.D. Rubin, “Risks of the Passport single signon protocol” 9th International World Wide Web Conference on Computer Networks, North-Holland Publishing Co., pp. 51–58. 2000.

[25] T.M.A. Lomas, L. Gong, J.H. Saltzer, and R.M. Needham, “Reducing Risks from Poorly Chosen Keys” 12th ACM Symposium on Operating System Principles, ACM Operating Systems Review, 23(5), pp. 14-18, 1989.

[26] Microsoft Passport service. http://www.passport.net [retrieved: July 2011].

[27] D. Pham and A. K. Sood, "An Intrusion Tolerance Approach to Enhance Single Sign on Server Protection," 2010 Third International Conference on Dependability, pp. 98-103, 2010.

[28] A. Rabkin, “Personal Knowledge Questions for Fallback Authentication: security questions in the era of Facebook,” 4th symposium on Usable privacy and security (SOUPS 2008), pp. 13-23, 2008.

[29] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J.C. Mitchell, “A browser plug-in solution to the unique password problem,” 2005. Technical report, Stanford-SecLab-TR-2005-1.

[30] S.E. Schechter, R. Dhamija, A. Ozment, and I. Fischer, “The Emperor's New Security Indicators,” IEEE Symposium on Security and Privacy, pp. 51-65, 2007.

[31] B. Schneier et al. Password Safe application. http://www.schneier.com/passsafe.html [retrieved: July 2011].

[32] S. Singh and A. Cabraal, C. Demosthenous, G. Astbrink, M. Furlong, “Password Sharing: Implications for Security Design Based on Social Practice,” SIGCHI conference on Human factors in computing systems (CHI ’07), pp. 895–904, 2007.

[33] A. Sotirov, M. Stevens, J. Applebaum, A. Lenstra, D. Molnar, D.A, Osvik, and B. de Weger, “Creating a Rogue CA certificate," 25th Chaos Communication Congress in Berlin 2008. Also: http://www.phreedom.org/research/rogue-ca/ [retrieved: July 2011].

[34] S. T. Sun, Y. Boshmaf, K. Hawkey, and K. Beznosov, "A billion keys, but few locks: the crisis of web single sign-on," 2010 Workshop on New Security Paradigms (NSPW'10), pp. 61-72, 2010.

[35] P.C. van Oorschot and T. Wan, “TwoStep: An Authentication Method Combining Text and Graphical Passwords,” 4th MCETECH Conference on eTechnologies, Lecture Notes in Business Information Processing, E-Technologies: Innovation in an Open World, pp. 233-239, 2009.

[36] R. Wang, S. Chen, and X. F. Wang, "Signing Me onto Your Accounts through Facebook and Google: a Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services," IEEE Symposium on Security and Privacy, pp. 365-379, 2012.

[37] C.S. Weir, G. Douglas, T. Richardson, and M. Jack, “Usable security: User preferences for authentication methods in eBanking and the effects of experience,” Interacting with Computers, 22 (3), pp. 153-164, 2010.