A Cognitive-Behavioral Framework of User Password Management Lifecycle[*]

Yee-Yin Choong

National Institute of Standards and Technology,
100 Bureau Drive, Gaithersburg, MD 20899, USA
yee-yin.choong@nist.gov

Abstract. Passwords are the most commonly used mechanism in controlling users' access to information systems. Little research has been established on the entire user password management lifecycle from the start of generating a password, maintaining the password, using the password to authenticate, then to the end of the lifespan of the password when it needs to be changed. We develop a cognitive-behavioral framework depicting the cognitive activities that users perform within each stage, and how the stages interact with the human information processor, i.e. memory and attention resources. Individual factors are also represented in the framework such as attitudes, motivations, and emotions that can affect users' behaviors during the password management lifecycle. The paper discusses cognitive and behavioral activities throughout the lifecycle as well as the associated economics. We show the importance of a holistic approach in understanding users' password behaviors and the framework provides guidance on future research directions.

Keywords: password, password management lifecycle, cyber security, password policy, usability, cognitive-behavioral framework, economics of passwords.

1 Introduction

Text-based passwords are the most commonly used mechanism in controlling users' access to information systems. Arguably, passwords are currently the best fit for many authentication needs as passwords allow access from anywhere assuming only a simple browser and revocation is as simple as changing passwords [1]. Users often possess multiple account-password pairs for work, school and private use. For example, it is reported that an average user has 25 web accounts requiring passwords [2], and employees of organizations have about 4 [3] to 9 passwords [4] at work.

Users are often viewed by IT security professionals as the weakest link of cyber security [5,6]. Users are also blamed for employing insecure behaviors such as selecting bad and simple-easy-to-guess passwords, reusing passwords, writing down or sharing their passwords, and, whenever possible, not changing their passwords on a

[*] The rights of this work are transferred to the extent transferable according to title 17 U.S.C. 105.

T. Tryfonas and I. Askoxylakis (Eds.): HAS 2014, LNCS 8533, pp. 127–137, 2014.

regular basis. For example, in a recent major security breach in which 150 million user accounts were compromised, “123456” was used the most as the password by over 2 million users, followed by a little more complicated password “123456789”, and the word “password” ranked 3rd used by 345,000 users [7].

On the other hand, for users, usability of passwords is their main concern. Users have to juggle multiple passwords for work, school or personal use and often are forced to comply with password policies that they view as burdensome [4,8]. Frustration with login problems such as forgetting or mistyping passwords increase greatly with the number of passwords that users must manage [1,4]. Users perceive that security measures hinder their productivity and sometimes use workarounds to break the security protocol [4,8].

Research focusing on human factors and usability of passwords has been challenging the view that users are the primary cause for cyber security issues and pointing out that security policies are often imposing unreasonable requirements and pushing users’ cognitive limits. For example, a typical enterprise password policy can require its employees create complicated passwords, not write down or store them, change passwords every 90 days, and not reuse the last 10 passwords. It is almost impossible for employees to comply with this stringent policy especially with multiple passwords as there are fundamental limitations on human memory (e.g. limited memory span, memory decay, recognition vs. recall, and memory interferences) as summarized by Sasse et al. [9]. Many studies have investigated the construct of users’ selection of “good” or “bad” passwords [10-12]. Researchers also challenge the necessity and true effectiveness of using aggressive password policies for security and sacrificing usability that forces users to adopt insecure practices and may eventually compromise security [13-15].

As shown, studies are abundant on password usability and its implications on cyber security. However, little research has been established on the cognitive and behavioral aspects of the entire user password management lifecycle, i.e. from the start of generating a password to the end of the lifespan of the password when it needs to be changed due to events such as forgetting, expiration, or compromise. While performing research on a particular stage of the lifecycle provides valuable insight on users’ experiences during that stage, it does not offer complete understanding of the entire process and could miss opportunities for identifying potential interactions and interdependencies among various stages during the password management lifecycle. This paper focuses on the holistic view of the end-to-end password management lifecycle and proposes a framework connecting the dots of users’ activities during the lifecycle. This framework serves as a foundation in guiding future research directions.

2 The Cognitive-Behavioral Framework

We develop a framework to represent the cognitive process and user behaviors in the end-to-end password management lifecycle and to guide our future research. The user password management lifecycle consists of three stages: *Generation*, *Maintenance*, and *Authentication*. The framework depicts the cognitive activities that users perform within each stage, and how the stages interact with the human information processor, i.e. memory and attention resources. In addition, individual factors such as attitudes, motivations, and emotions are also included that can affect users' decision-making and behaviors during the password management lifecycle. The framework is illustrated in Figure 1 and each stage in the user password management lifecycle is described in detail in the sections below.

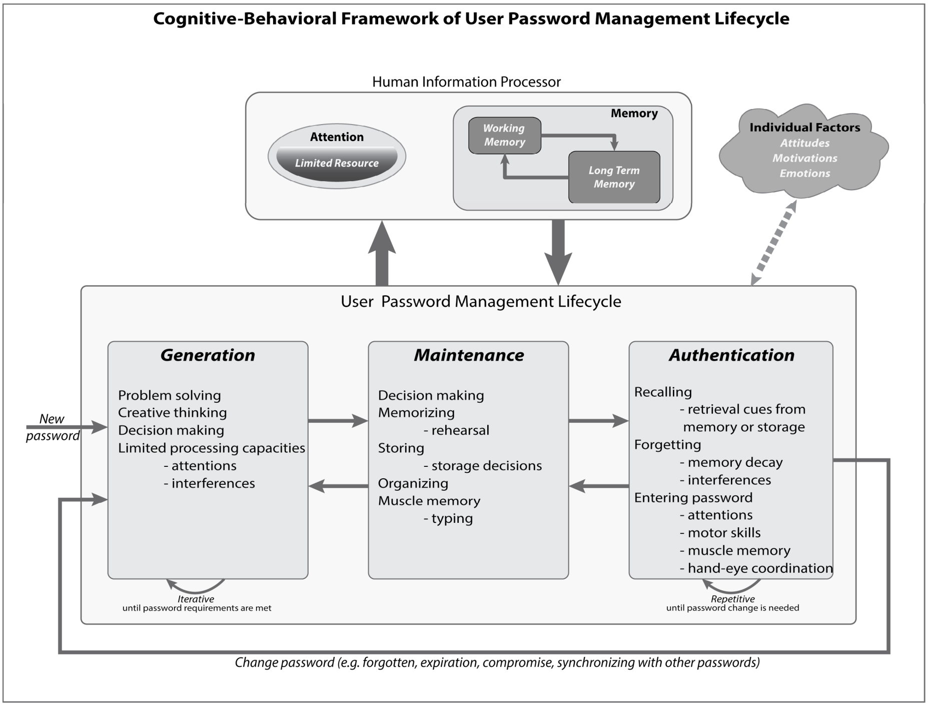

Fig. 1. A Cognitive-Behavioral Framework of User Password Management Lifecycle

2.1 Password Generation

In the first stage of the password management lifecycle, i.e. G*eneration*, users have to generate a plausible text string by combining various characters to satisfy the requirements for accessing the associated account or system. The requirements, known as composition rules, are a common organizational approach aimed at forcing users to select stronger passwords. The contents and wordings of those composition rules vary greatly from system to system, but they generally consist of rules on: password length (minimum and/or maximum), use (allowed or prohibited) of certain characters (uppercase or lowercase alphabets, numerical digits, special characters), use (allowed or prohibited) of common names, dictionary words, birthdays or other personal information. Composition rules can be presented as just password selection guidelines in some systems, whereas for other systems, the rules can be programmatically enforced such that users have to create compliant passwords in order to gain access to the systems.

This password generating and composing process is similar to a writing process that usually starts with the writer setting up the goals of the writing, understanding the constraints (e.g. grammar, target audience), generating ideas, selecting and arranging words, constructing text, and finally refining the written text [16]. This process, in essence, is a problem solving process that includes higher mental functions and creative thinking [17]. Password composition progresses in a similar way with the user first setting the goals of what account/system the password is for, understanding the constraints, choosing characters, then refining the text string to meet the password requirements. The constraints to the password generation problem can be categorized as: (1) *Environmental* – such as composition rules, platforms (e.g. desktop and/or laptop computers, and/or mobile devices), account/system type (e.g. web, application, or hardware access); (2) *Cognitive* – such as memory load and attention resources, rule comprehension ability; (3) *Individual* – such as attitudes, motivation, and perception of the criticality and sensitivity of the account and potential security threats.

This stage can be iterative as the user tries to find the best combination of characters that satisfies the password requirements while taking into account other environmental constraints, human-information process constraints (e.g. attention deficit, memory capacity) and individual factors (e.g. attitudes, motivations, and emotions).

This stage can also be a purely decision making stage without involving password composition or only involving composition partially. This happens when the user decides to reuse or make minor changes to an existing password as the best approach in the solution space while meeting the password requirements and the user's individual needs.

2.2 Password Maintenance

Once the user generates a satisfactory password for a specific account/system, the password moves into its second stage of the lifecycle, *Maintenance*. The user makes decisions on how he/she will keep track of the newly generated password, by memorizing or storing using some mechanism; and he/she also needs to decide how best to organize – mentally or physically – the newly generated password along with other existing and active passwords to minimize memory interferences at a later stage. If the user decides to memorize the password, he/she needs to employ some strategies (e.g. mnemonic device, rote rehearsing, or typing multiple times to establish muscle memory) to make sure the password has been encoded properly into the long-term memory. If the user decides to store the password, he/she needs to decide the storage mechanism, for example, writing down (in its entirety, partially, or disguised), recording electronically (file, devices, etc.), or utilizing some password management software. Sometimes, there may be an organizational policy on how passwords should be maintained by limiting maintenance options to users. For example, "Passwords should never be written down or stored on-line without encryption." is the most common policy set by many organizations.

It should be noted that there can be interactions and interdependencies between the *Generation* and *Maintenance* stages as the user may hold an *a priori* preference on whether to memorize or to store the password which can impact the user's password composing process with the thought that he/she has to memorize the text for later use. Also, the memorability of a text string can impact the user's decision on how to maintain the password.

2.3 Authentication

The last stage in the lifecycle is *Authentication* in which the password is used to gain access to the associated account/system. The authentication stage is repetitive as the password will be used multiple times for its entire lifespan until a change event occurs such as forgotten, expiration, password compromised, or user's desire to synchronize multiple passwords for different accounts. In each authentication instance, the user needs to retrieve the correct password either by recalling from memory or by looking up from stored media that matches the associated account/system for access, at the same time struggles with forgetting due to memory decay or interferences from other passwords, and needs to enter the password correctly which requires attentions, motor skills, muscle memory, and hand-eye coordination.

There are many factors that can affect a user's authentication experience with a password such as authentication frequency, how the password is maintained, memorability and type-ability of the account/password pair, or interferences from other passwords. The authentication experience (positive or negative) can then influence how the user creates new passwords when he/she moves out from the authentication stage and starts the next password management lifecycle.

3 Holistic Research Approach on User Password Behaviors Guided by the Framework

The framework serves as a constant reminder in research approaches to always consider users' password behaviors in a holistic manner that, at any point of time, the users are going through a stage in the password management lifecycle and their behaviors are a reflection of the interactions among stages in the lifecycle, the capabilities and limitations of the human information processor, and the individual factors.

In the following sections, we discuss the importance of employing a holistic approach and some misconceptions in the literature on user password behaviors research. We also review relevant research and point out areas for further research.

3.1 Password Generation – More than a Selection Task

The most common misconception of password generation in the literature is the notion of users' selecting passwords. It is often described that users *select* bad and insecure passwords [11,18,19]. However, generating passwords is more than a selection task in that the word "selection" implies choosing from a set of readily available password options. Users only *select* passwords when they decide to reuse existing passwords. In password generating tasks, users employ high-level cognitive, problem-solving tasks when they are faced with the task of composing text strings to satisfy password requirements of combining and arranging various characters with length limits while trying to make sense of the text strings and meeting their own personal needs.

3.2 Password Composition – Problem Solving

As noted earlier, password composition is in essence problem solving in that it involves goals defining, ideas searching/planning, and refining/finalizing. There have been few studies investigating password generation under restrictive composition rules [11,20,21]. However, those studies focused only on the outcomes of the password generation, i.e. the characteristics of the passwords generated, and the impacts of the restrictions, but did not investigate the entire generation process.

Password research has seldom recognized that composition is not a trivial task. There is a need for research on how users solve the "password generation" problem from the beginning when users first encounter and perceive the problem domain; comprehend the constraints (*Environmental*, *Cognitive*, and *Individual*); explore the solution space; verify solution feasibility; refine/narrow solution space; and make decisions on the best-fit solution. By researching password generation as a problem solving effort with the framework, it enables us to investigate topics such as the differences among the "problem solvers" (e.g. experts vs. novices); the impacts of password constraints on the solution space; the most important factor(s) leading to the best-fit solution; and the influences of the maintenance decision on password generation.

3.3 The Economics – Password Management Lifecycle

The cost of passwords appears low at a glance from the service providers' perspective as deploying a functional password system is relatively simple compared to other authentication alternatives such as biometrics or smart cards. From the users' perspective, it doesn't seem to cost much, either, since passwords allow instantaneous account setup and are readily understood [1]. However, there are significant costs associated with the password authentication mechanism for both the service providers and the end users. It is shown qualitatively [15] that an unusable password policy can degrade employees' productivity, and ultimately affect the organization's overall productivity. It is reported that more than 30% of IT support center calls were related to password resets [22]. On average, each call lasts about 5 minutes and the cost of support per incident is \$ 25[1] on average [23]. In addition to the support center cost, there are also costs associated with a user's time and productivity loss when making calls to the support center.

Of the three stages in the user password management lifecycle, *Generation* and *Authentication* are the most effort- and time-consuming stages for the users. It is imperative for researchers to start investigating the associated costs for these two stages from the users' perspective.

[1] All cost estimates in this paper are based on the United States dollar, i.e. USD or US$.

The Cost of Password Generation

Besides composition rules, organizations often include other requirements such as password expiration, password reuse limitations, and password uniqueness in their organizational policies. It will be difficult to quantify the direct impacts of the password policies on users' cognitive activities and behaviors and translate the impacts into associated costs. One way to estimate the costs is to look at the number of passwords generated and the time it takes to generate those passwords.

In the study performed by Choong et al. [4], it is reported that an employee has on average 9 work-related passwords. An organizational password policy commonly looks like:

- Password **must be**
  - Changed at least every 60 days
  - At least 12 characters long
  - Consistent with the complexity requirements (mixed-case characters, numbers, and special characters)
- Password **must not**
  - Be written down or stored on-line on non-organization systems
  - Reuse any password of the last 24 prior passwords
  - Use the same password on multiple systems, applications or websites

If a new employee acquires his/her 9 passwords in the first months on the job, by following the policy, it means that the new employee will have to generate 54 unique passwords within the first year of employment, which means that a unique and complex password is generated on average every week throughout the year. The constant password generation task puts a huge amount of burden on employees who only see managing passwords as a secondary task enabling access to their primary task [24]. This estimate does not take into account other password generation events outside of the regular changing cycle due to unplanned incidents such as forgotten passwords or password compromises.

It is also reported that the longest time it takes to generate passwords for work is, on average, 98.5 minutes for frequent passwords and 86.6 minutes for occasionally passwords [4]. The worst scenario: if every password takes the longest time to generate, an employee can spend 18.6 hours (or 2 ¼ business days) at a 60-day cycle each year generating passwords for their work. If the average annual wage of $81,704 (or $39.15/hour) of federal civilian workers is used [25], we can estimate an annual cost of $728.19 per employee being pulled away from work to generate passwords.

The Cost of Authentication

Users interact with authentication systems on a daily basis for work, school, or for personal use. As shown in Figure 1, each authentication instance involves retrieving the correct password (from memory or from stored media) and typing the password to gain access. This authentication instance can be iterative in itself if any step fails in the sequence, e.g. incorrect password retrieved – forgetting or interferences, typing errors, or system failure.

Research investigating real-life user authentication experience includes diary studies, e.g. [15,24,26,27], and longitudinal studies, e.g. [2,28]. The number of authentication instances varies greatly in those studies, ranging from typing 8.11 passwords per day [2], 75 password events in a two-week span [27], to 23 authentication events in a day with 46.9% (~11 times) being password logins [24]. Users expressed frustration and time wasted from various login problems such as mistyping passwords, forgetting passwords, mismatching account and password, and getting locked out [4]. When entering passwords from memory, it is reported that the most common error is incorrect capitalization (shifting), followed by missing character(s) [29].

While it is difficult to estimate the full costs of users' authentication experience with passwords, we can start with a simplified way to calculate the costs associated with password entry. In the diary study done at the National Institute of Standards and Technology (NIST) [24], employees entered passwords about 11 times in a day and the NIST's password policy requires passwords being 12 characters or longer. As reported in [21], it takes roughly14 seconds to type a password of 8 characters long. Estimating conservatively (as the NIST required passwords are longer than 8 characters), a typical full-time employee can spend 10.27 hours a year on typing passwords for authentication[2]. The estimate should be doubled, i.e. 20.54 hours, as a complete authentication often includes typing the user name besides the password. Using the same wage information (i.e. $39.15/hour) in [25], the annual cost per employee on entering user name and password pairs for authentication is roughly $804.14.

For an organization with 100 employees, a rough estimate of $153,000 annually can be spent on employees' basic password management activities (*Maintenance* not included), i.e. *Generation* ($728.19) and *Authentication* ($802.58), aside from productivity. For large organizations with 1,000 employees or more, this cost of basic password management can be more than $ 1,500,000 each year.

Hidden Costs

Beyond the two costs for basic password management demonstrated earlier, there are other hidden costs associated with the password management lifecycle. For example, it is not uncommon for organizations to enforce timeouts and screen locking to mitigate opportunistic misuse of an unattended computer [15,24]. It creates constant task interruptions and requires users to recover from interruptions that will also translate to productivity loss.

More and more users' computing experiences happen on mobile devices such as laptop computers, tablets, and smart phones. The cognitive and behavioral framework will provide us a foundation to explore the impacts on password entering experience with different keyboards and layouts. It will also allow us to investigate the potential interferences on users' muscle memory of a well-practiced password and the increase on recall errors or typing errors due to transitioning from one platform to another or having to switch back and forth between platforms. Research is needed to understand the associated costs of users' mobile authentication experience.

[2] Total of 240 workdays assuming 5 days a week, 52 weeks, and minus two vacation weeks and 10 federal holidays.

3.4 Positive Attitudes = Better Security Behaviors and Less Frustration?

In general, users are concerned with security, but they often are forced to develop less secure coping strategies (e.g. reuse passwords, or write down passwords) when they are unable to comply with password policies that are too restrictive and inflexible to match users' capabilities [15].

However, in a large-scale survey study [4], the researchers found that users' attitudes toward organizational password requirements are related to their password behaviors and experiences across all three stages in the password management lifecycle. Users holding positive attitudes toward password requirements value more in creating compliant and strong passwords, write down passwords less often, feel less frustration with authentication problems, better understand and respect the significance of security, as compared to users with negative attitudes.

The findings on attitudes lead us to more research questions on searching for plausible means to encourage positive user attitudes and to provide user support addressing the negative thoughts.

4 Conclusion

Are cyber security and usability two parallel lines that never meet? Or, are they cross roads where the intersection is yet to be reached? We believe that, though it may not be easily seen, the intersection does exist among the theoretical, technical, and usability aspects of cyber security. It requires collaboration from researchers and practitioners with multi-disciplinary backgrounds in finding the right balance to reach that intersection that will provide acceptable security and usability.

More research is needed on users' cognitive and behavioral activities regarding interrelationships among the three stages in the password management lifecycle. What can be done more on the technology side to ensure security and protect information assets, and alleviate the burden on users so they will think more positively about security measures? Future research should use a holistic approach with the goal of providing data to enable the policy makers to make informed decisions on security policies that are both secure and usable, and to provide guidance in user support and education to promote positive attitudes.

References

1. Herley, C., van Oorschot, P.: A Research Agenda Acknowledging the Persistence of Passwords. IEEE Security & Privacy 10(1), 28–36 (2012)
2. Florêncio, D., Herley, C.: A Large-Scale Study of Web Password Habits. In: Proceedings of the 16th International Conference on World Wide Web, pp. 657–666. ACM (2007)
3. Hoonakker, P., Bornoe, N., Carayon, P.: Password Authentication from a Human Factors Perspective: Results of a Survey among End-Users. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 53(6), pp. 459–463. SAGE Publications (2009)

4. Choong, Y.-Y.T.M., Liu, H.-K.: A Large-Scale Survey of Employees' Password Behaviors. Manuscript submitted for publication (2014)
5. Goverance, I.T.: Boardroom Cyber Watch 2013 – Report (2013), http://www.itgovernance.co.uk/what-is-cybersecurity/boardroom-cyber-watch.aspx
6. Haskins, W.: Network Security: Gullible Users Are the Weakest Link. TechNewsWorld (November 29, 2007), http://www.technewsworld.com/story/60520.html (retrieved)
7. Malenkovich, S.: 10 Worst Password Ideas (As Seen In the Adobe Hack). Kaspersky Lab Daily (November 21, 2013), http://blog.kaspersky.com/10-worst-password-ideas-as-seen-in-the-adobe-hack/ (retrieved)
8. MeriTalk.: Cyber Security Experience: Security Pros from Mars, Users from Mercury (2013), http://www.meritalk.com/cybersecurityexperience (retrieved)
9. Sasse, M.A., Brostoff, B., Weirich, D.: Transforming the 'weakest link' — a human/computer interaction approach to usable and effective security. BT Technology Journal 19(3), 122–131 (2001)
10. Brown, A.S., Bracken, E., Zoccoli, S., Douglas, K.: Generating and remembering passwords. Applied Cognitive Psychology 18(6), 641–651 (2004)
11. Campbell, J., Ma, W., Kleeman, D.: Impact of restrictive composition policy on user password choices. Behaviour & Information Technology 30(3), 379–388 (2011)
12. Yan, J., Blackwell, A., Anderson, R., Grant, A.: Password Memorability and Security: Empirical Results. IEEE Security & Privacy 2(5), 25–31 (2004)
13. Florêncio, D., Herley, C., Coskun, B.: Do Strong Web Passwords Accomplish Anything? In: Proceedings of the 2nd USENIX Workshop on Hot Topics in Security, pp. 1–6 (2007)
14. Herley, C.: So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In: NSPW 2009 Proceedings of the 2009 Workshop on New Security Paradigms Workshop, pp. 133–144 (2009)
15. Inglesant, P., Sasse, M.A.: The True Cost of Unusable Password Policies: Password Use in the Wild. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 383–392 (2010)
16. Flower, L.H., Hayes, J.R.: A Cognitive Process Theory of Writing. College Composition and Communication 32(4), 365–387 (1981)
17. Flower, L.H., Hayes, J.R.: Problem-solving strategies and the writing process. College English 39(4), 449–461 (1977)
18. Imerva Application Defense Center (ADC).: Consumer Password Worst Practices. Imperva White Paper (2009), http://www.imperva.com/docs/wp_consumer_password_worst_practices.pdf (retrieved)
19. Zhang, Y., Monrose, F., Reiter, M.K.: The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis. In: Proceedings of the 17th ACM Conference on Computer and Communications Security, pp. 176–186 (2010)
20. Proctor, R.W., Lien, M.-C., Vu, K.-P.L., Schultz, E.E., Salvendy, G.: Improving computer security for authentication of users: Influence of proactive password restrictions. Behavior Research Methods, Instruments, & Computers 34(2), 163–169 (2002)
21. Vu, K.-P.L., Bhargav, A., Proctor, R.W.: Imposing Password Restrictions for Multiple Accounts: Impact on Generation and Recall of Passwords. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 47(11), pp. 1331–1335. SAGE Publications (2003)

22. Pratt, M.K.: 5 Annonying Help Desk Calls - And How to Banish Them. PCWorld (April 3, 2012), http://www.pcworld.com/article/253073/5_annoying_help_desk_calls_and_how_to_banish_them.html (retrieved)
23. Abel, S.: Industry Average Help Desk Support Costs. The Content Wrangler (April 28, 2011), http://thecontentwrangler.com/2011/04/28/industry-average-help-desk-support-costs/ (retrieved)
24. Steves, M., Chisnell, D., Sasse, M.A., Krol, K., Theofanos, M., Wald, H.: Report: Authentication Diary Study. NISTIR 7983. National Institute of Standards and Technology, Gaithersburg, MD (2014)
25. U.S. Bureau of Economic Analysis: National Income and Product Accounts, Tables 6.6D, Wages and Salaries Per Full-Time Equivalent Employee by Industry (August 7, 2013), http://www.bea.gov/national/nipaweb (retrieved)
26. Grawemeyer, B., Johnson, H.: Using and managing multiple passwords: A week to a view. Interacting with Computers 23(3), 256–267 (2011)
27. Hayashi, E., Hong, J.I.: A Diary Study of Password Usage in Daily Life. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 2627–2630. ACM (2011)
28. Keith, M., Shao, B., Steinbart, P.: A Behavioral Analysis of Passphrase Design and Effectiveness. Journal of the Association for Information Systems 10(2), 63–89 (2009)
29. Stanton, B., Greene, K.K.: Character Strings, Memory and Passwords: What a Recall Study Can Tell Us. In: Proceedings of the 16th International Conference on Human-Computer Interaction (in press, 2014)