Factors of Password-based Authentication

Research-in-Progress

Herbert Mattord
Coles College of Business, Kennesaw State University, Kennesaw, GA, USA
hmattord@kennesaw.edu

Yair Levy
Graduate School of Computer and Information Sciences, Nova Southeastern University,
Ft. Lauderdale, FL, USA
levyy@nova.edu

Steven Furnell
School of Computing and Mathematics, Plymouth University, Plymouth, Devon, UK
s.furnell@plymouth.ac.uk

ABSTRACT

Organizations continue to rely on password-based authentication methods to control access to many Web-based systems. This research study developed a benchmarking instrument intended to assess authentication methods used in Web-based information systems (IS. This approach explored how authentication practices can be measured in three component areas: 1) password strength requirements, 2) password usage methods, and 3) password reset requirements. This report explores the criteria that are required to define these component areas.

Keywords (Required)

Authentication Methods, Password Authentication.

INTRODUCTION

The broader research area of which this is an initial part, seeks to develop a benchmarking instrument that assesses certain aspects of authentication methods employed by Web-based information systems (IS). The anticipated benchmarking instrument is intended to be developed from criteria drawn from academic literature, practitioner references, as well as industry standards. The planned benchmark will measure 1) password strength requirements, 2) password usage methods, and 3) password reset requirements. Those measures will be used to derive a single index value that represents an assessment of the quality of current authentication methods employed by a Web-based system.

LITERATURE REVIEW

The research problem addressed in this project is the widespread use of insufficient authentication methods allowing misuse of Web-based ISs (Furnell, 2007; Furnell, 2011). Authentication was defined by Sandhu and Samarati (1996) as a process that "establishes the identity of one party to another [within the context of] information and systems security" (p. 241). An authentication method is a way that a system performs the process of authentication. Authentication methods include the specification of which and how many authentication factors are used, what values are allowable, and which associated access control procedures are used to control the actions taken by authenticated users (Sandhu & Samarati, 1996). Authentication practices are behaviors that system users employ to access systems that have identified authentication methods (Rhee, Kim and Ryu, 2009). The difference in how users react to specified authentication methods with manifested authentication practices may enable attacks on the system (Furnell, 2007).

Attacks against Web-based ISs have been showcased in media reports which indicated such cyber attacks are widespread and growing (Acohido, 2009). Acohido (2009) illustrated a significant number of instances where cyber attacks were made possible by the Web-based systems' lack of sufficient authentication controls. Moreover, Acohido (2009) noted that the "the vast majority of organizations routinely fail to take simple defensive measures, such as shoring up common Website weaknesses or uniformly enforcing the use of strong passwords" (p. B1). The ease and rapidity of cyber attacks against networked ISs have also been documented previously by Littman (1996). She observed that "security breaches can take place when authorized users select poor passwords" (p. 35). Thus, poor passwords allow unauthorized users to gain access. Additionally, Littman (1996) indicated that the current authentication methods specified by the majority of Web-based ISs are to rely only on password-based authentication mechanisms. However, authentication methods that rely solely on passwords are easily compromised (Furnell & Zekri, 2006). Furnell and Zekri (2006) stated that such compromises may allow misuse of the ISs when they are protected by methods built on specifications of insufficient authentication methods. Systems misuse, in this context, was defined by Magklaras and Furnell (2002) as the use of an IS for a purpose that is unacceptable or unapproved by the system owner. Since shortcomings in authentication methods used in Web-based system can fail to perform adequate authentication of users, additional investigation is needed to enable assessment of these methods.

Access control includes those methods that are specified by systems to govern the identification, authentication, authorization, and accountability of systems users (Firesmith, 2003). Of particular interest to this research, an authentication method is one that validates a proposed user's identity so as to allow a system to discriminate between valid and invalid identities (Clarke, Dowland and Furnell, 2008; Sandhu & Samarati, 1996). Identification methods are the mechanisms used by a system to identify external actors before interacting with them (Firesmith, 2003). Authorization is the process used by a system to grant specific permissions to use system features based on the authenticated identity of a user (Sandhu, Coyne and Feinstein, 1996).

A variety of methods can be used to perform authentication (Benantar, 2006; Clarke et al., 2008; Shimizu, Horioka and Inagaki, 1998; Weir, Douglas, Richardson and Jack, 2010; Wood, 1977). As previously noted, authentication requires that the entity seeking access, hereafter called the supplicant, propose an identity (Benantar, 2006; Clarke et al., 2008). That proposed identity is then validated by an element of the system being accessed called the authenticator (Shimizu et al., 1998). The identity proposed by the supplicant is validated by the authenticator using one or more of three main approaches (Weir et al., 2010; Wood, 1977). These approaches are 1) use of a fact that is known to the supplicant and the authenticator (known as secret knowledge), 2) use of a characteristic of an object that is possessed by or is assigned to the supplicant and can be proven to be in the possession of the supplicant (known as a token), or 3) use of a measurement of some physical characteristic of the supplicant or a measurement of some action the supplicant can perform that can be provable shown to be unique to the supplicant (known as a biometric factor) (Clarke et al., 2008; Weir et al., 2010; Wood, 1977). These three factors of authentication are well defined and are "fundamentally different from one another" (Benantar, 2006, p. 11). Authentication may be done by using one factor or by choosing to combine the use of two or more factors from different categories to achieve multiple-factor authentication (Benantar, 2006).

The literature has provided useful guidance about the individual criteria that might use to derive measures of the authentication process. The intent is to develop a single index value that can represent of the overall process of performing the authentication process. After identifying these criteria, they have been analyzed and assigned into three measures, the password strength measure (PSM), the password usage measure (PUM), and the password initialization and reset measure (PIRM). The detailed focus is on the predominant use of passwords as a single-factor authentication method. Of specific concern are: 1) criteria regarding the strength of passwords in methods implemented by Web-based systems that determine the strength of passwords (elements of the PSM), 2) criteria regarding the usage of passwords established in methods implemented by Web-based systems that contribute to the quality of the authentication process (elements of the PUM), and 3) requirements regarding password initiation and resetting established in methods implemented by Web-based systems that regulate how passwords are initiated and reset (elements of the PIRM). Figure 1 shows how an index value might be structured using the three measures and the relevant criteria for each measure.

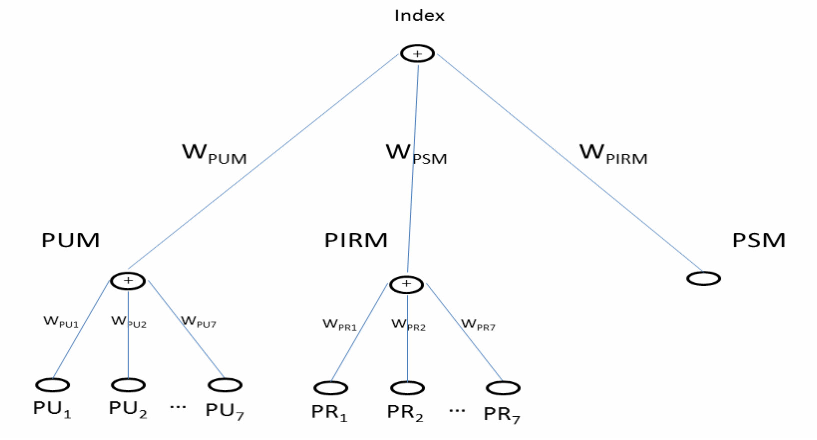

Figure 1. Index, Measures, and Criteria

The detailed focus is on the predominant use of passwords as a single-factor authentication method. Of specific concern are: 1) criteria regarding the strength of passwords in methods implemented by Web-based systems that determine the strength of passwords (elements of the PSM), 2) criteria regarding the usage of passwords established in methods implemented by Web-based systems that contribute to the quality of the authentication process (elements of the PUM), and 3) requirements regarding password initiation and resetting established in methods implemented by Web-based systems that regulate how passwords are initiated and reset (elements of the PIRM).

PASSWORD STRENGTH

The topics of password strength and use have been included in the published research of several scholars (Campbell, Kleeman and Ma, 2007; Furnell, 2007; Villarrubia et al., 2006a). Some researchers have reported on theoretical approaches, such as the development of conceptual frameworks for assessing password quality (Ma, Campbell, Tran and Kleeman, 2007; Villaruba, Fernandez-Medina and Piattini, 2006a). Other researchers have worked to apply these and other theories about passwords to measure the quality of password-based controls used in IS (Campbell et al., 2007; Furnell, 2011). One theoretical treatment proposed a construct called the Password Quality Indicator (PQI) (Ma et al., 2007). PQI was derived from two empirical dimensions of the password allowed for use by systems policy. The first of these dimensions was the edit distance of a password from a standardized set of dictionary words using a computed value (Keith, Shao and Steinbart, 2007). The second dimension was the effective password length. Edit distance is a computed value that reflects the combination of ways in which the use of numbers, special characters and case shifting can be used to make passwords less similar to the chosen set of dictionary words (Keith et al., 2007; Ma et al., 2007). The mechanisms employed by PQI are similar to some efforts by various organizations and individuals to implement a variety of password strength measures (Ma et al., 2007; Palmer, 2008). For example, where PQI documented the fundamental aspects of password strength measurement, it does not offer an easily comparable value such as that used for the PSM in this research. In order to provide a measurement that is more useful in the context of this research, an alternative that uses constructs drawn from PQI will be used.

Some Web–based systems utilize password strength measurement technologies for password checking or to offer feedback to users creating their own passwords (Vijaya, Jamuna and Karpagavalli, 2009). Different password strength tools, such as The Password Meter, Google Password Strength Measure, and Microsoft Password checker each use different approaches to implement lexical analysis to dynamically assess the quality of a password (Vijaya et al., 2009). These tools offer users who propose self-generated passwords a visualization or a verbal assessment of the strength of the password using a lexical analysis of that proposed password. Several tools are available to Web developers under open-source license that allows varying levels of customization. This variant provides a detailed verbal assessment of the characteristics of the proposed password. As each character of the proposed password is entered the user can see the lexical analysis as well as both a verbal and color-coded graph. The Password Meter reports to the user on the length of the password, the character sets being used as well as characteristics often not specified in authentication policy requirements such as repeating characters as well as consecutive use of characters or numbers in sequence. The key element of the feedback from The Password Meter is the verbal assessment of “Too Short”, “Very Weak”, “Weak”, “Good”, “Strong”, or “Very Strong”. The intent is to allow the user to make an informed decision about the strength of the password. If desired, the developer may choose to disallow selection of passwords that fall below specifications required by that systems authentication method.

Another password strength tool that is available to Web developers as an open-source option is the Google Password Strength Meter (Google, 2011). This tool allows Web developers to let users propose passwords to be evaluated. While less information is provided that with The Password Meter, it offers a clean and simple interface to the user to see a verbal strength assessment as well as a colored graph. This tool offers strength assessments based on the lexical functions noted by Vijaya et al. (2009) and offers feedback to the user as verbal assessment of "Too Short", "Fair", "Good", or "Strong" (Google,2011). As with other such tools, the intent is to offer users feedback on the computed password strength.

While other forms of assessment of password have been proposed to estimate password strength, the use of lexical functions capable of dynamic assessment is deemed appropriate as a function assessment (Ruffo & Bergadano, 2005). The output values provided from The Password Meter (2011) are simple, effective and semantically useful.

The criteria selected for inclusion in the PSM were drawn from literature as noted and the criteria are explained following and are summarized in Table 1.

Alphabet Classes – the number of subdivisions of characters in the choice set. For example, if some number of characters in the password must be chosen from the 94 printable ASCII characters, and some number of characters in the password must be chosen from the digits 0-9, and some number of characters in the password must be chosen from the set of special characters, then the password would have three alphabet classes (Campbell et al., 2007; Furnell, 2007; Ma et al., 2007; Villarrubia, Fernandez-Medina and Piattini , 2006b). This criterion is called "number of different classes demanded" (Villarrubia et al., 2006b, p. 545). It is also called "character sets" (Ma et al., 2007). In data collection, this criterion will be noted as PS1.

Alphabet Size – the number of characters in the choice set from which passwords are assembled. For example, if only roman-alphabet, capital letters are allowed the alphabet size is 26 (A-Z). If only decimal digits can be chosen, the alphabet size is 10 (0-9). If all printable ASCII characters are allowed, the alphabet size is 93 (Ma et al., 2007; Villarrubia et al., 2006b). Alphabet size has a direct impact on the password keyspace, the "total number of possible different values that a key, such as a password can have" (Scarfone & Souppaya, 2009, p. 3). In data collection, this criterion will be noted as PS2.

Minimum Length – the fewest number of characters that make up a valid password (Furnell, 2007; Furnell, 2011; ISO/IEC, 2007; Ma et al., 2007; Villarrubia et al., 2006b). The choices are a) 4 characters or less, b) 4 to 8 characters, c) 9 to 12 characters, d) 13 to 16 characters, or e) over 16 characters (Villarrubia et al., 2006b). Minimum length also has a direct impact on the password keyspace (Scarfone & Souppaya, 2009). In data collection, this criterion will be noted as PS3.

No.	Criterion	Categorization	Supporting Literature
PS1	Alphabet classes	1, 2, 3, or 4	Campbell et al., 2007; Furnell. 2007; Ma et al., 2007; Villarrubia et al., 2006b
PS2	Alphabet size	1 - 10 characters or less 2 - 11 to 25 characters 3 - 26 to 50 characters 4 - 51 to 75 characters 5 - 76 characters or more	Ma et al., 2007; Villarrubia et al., 2006b
PS3	Minimum length	1 - 4 characters or less 2 - 4 to 8 characters 3 - 9 to 12 characters 4 - 13-16 characters 5 - 17 characters or more	Furnell, 2007; Scarfone & Souppaya, 2009

Table 1. Password Strength Measurement Criteria

PASSWORD USAGE

The criteria that will be used in the AMSI benchmarking instrument to compute the PUM, describing how systems use, store and transmit passwords have been drawn from the literature as summarized in Table 5. The criteria are discussed here and are summarized in Table 2.

Authentication Period – the time and circumstances after an authentication is granted until re-authentication is required. The choices are multiple sessions, one session, intra-session with a 15 minutes maximum of inactivity, five minutes maximum of inactivity (Villarrubia et al., 2006b). Also called "session time-out" (ISO/IEC, 2007, p. 86). In data collection, this criterion will be noted as PU1.

Input Visualization – documents how the client receives feedback from the systems for the characteristics of the password chosen. The options are plain text, replacement characters (often "*" is used), no visualization, or the display of a password strength assessment (Ruffo & Bergadano, 2005; Villarrubia et al., 2006b). In data collection, this criterion will be noted as PU2.

Maximum Lifetime – the longest length of time that an issued password is intended to remain valid (Furnell, 2007; ISO/IEC, 2007; Villarrubia et al., 2006b). The possible values are over 12 months, six to 12 months, three to five months, or under three months. This is also called "credential lifetime" (Palmer, 2008, p. 276). In data collection, this criterion will be noted as PU3.

Mutual Authentication – is the use of a mutual authentication process to confirm the validity of the authenticator to the supplicant prior to use of the password (De Angeli, Coventry, Johnson and Renaud, 2005; Furnell, 2007). This includes a number of techniques including use of images to allow users to confirm the validity of the server requesting credentials. This criterion is measured as a binary response (Yes or No). In data collection, this criterion will be noted as PU4.

Password Guidance – documents how much guidance is provided to users about selecting passwords. The options are none, defines minimum strength, offers selection tips, or both defines minimum strength, shows a password strength meter, and/or offers selection tips (Furnell, 2007). In data collection, this criterion will be labeled PU5.

Password Transmission – documents how the password is transmitted from the users browser to the Web server. The options are none, user identifier as unprotected text and password as encrypted text, or fully encrypted session (Villarrubia et al., 2006b). In data collection, this criterion will be labeled PU6.

User Training – whether or not training is required for all system users before credentials are issued (Palmer, 2008; Villarrubia et al., 2006b). This criterion is measured as a binary response (Yes or No). In data collection, this criterion will be labeled PU7.

No.	Criterion	Categorization	Supporting Literature
PU1	Authentication period	1 – Multiple sessions 2 – Session 3 – Intra-session 15 minute max 4 – Intra-session 5 minute maximum	Villarrubia et al., 2006b; ISO/IEC (2007)
PU2	Input visualization	1 – Plain text 2 – Replacement characters 3 – No visualization 4 – No visualization and password strength or other validity assessment is given	Ruffo & Bergadano, 2005; Villarrubia et al., 2006b
PU3	Maximum lifetime	1 – Over 12 months 2 – 6 to 12 months 3 – 3 to 5 months 4 – Under 3 months	Furnell, 2007; ISO/IEC (2007); Palmer, 2008; Villarrubia et al., 2006b
PU4	Mutual Authentication	Y or N	De Angeli et al., 2005; Furnell, 2007
PU5	Password Guidance	1 – none 2 – defines minimum strength 3 – offers selection tips 4 – displays a password strength	Furnell, 2007

		meter 5 – enforces minimum strength	
PU6	Password Transmission	1 – none 2 – user identifier as unprotected text and password as encrypted text 3 – fully encrypted session 4 – out-of-band transmission	Villarrubia et al., 2006b; ISO/IEC, 2007
PU7	User Training	1 – none 2 – at time of registration 3 – compulsory online prior 4 – periodic courses	Palmer, 2008; Villarrubia et al., 2006b

Table 2. PUM Criteria

PASSWORD INITIALIZATION AND RESET

Password initialization and reset requirements are those policies that organizations establish to govern why, when, and how passwords are reset for and by users (Furnell, 2011). This aspect of authentication is complementary to password strength requirements since "indeed, if the recovery process is simple and secure enough, it provides a basis for users to select strong passwords without the need to remember them" (Furnell, 2007, p.449). A compilation of password initialization and reset requirements has been assembled from the work of researchers (Furnell, 2007; Campbell et al., 2007). The password reset PIRM criteria are discussed in the following paragraphs and summarized in Table 3.

Error Attempts – documents the maximum number of failed attempts allowed by a user before the system takes action against the user as a possible attacker. The ranges for response are no limit, 11 to 50 tries, four to 10 tries, less than four tries. This criterion is also called "maximum number of erroneous attempts" (Villarrubia et al., 2006b, p.545). In data collection, this criterion will be noted as PR1.

Information About Use – defines whether users are notified of the date and time of the past use of their credentials (Villarrubia et al., 2006b). This criterion is measured as a binary response (Yes or No). In data collection, this criterion will be noted as PR2.

Initial Communication – describes how an initial password is communicated to the user, or if a pre-defined value is used as a shared secret. The options are non-secure, use of a single-use password sent non-secure, sent via a secure channel, or use of a shared secret (Villarrubia et al., 2006b). In data collection, this criterion will be noted as PR3.

Password Reassigning – determines how passwords are assigned for a password reset. The options are the prior password reactivated or a new password is created (Villarrubia et al., 2006b). "When a user forgets a password, generally there are two options: regain access to the old password—password recovery—or set a new password—a password reset" (Scarfone & Souppaya, 2009, p. 3). In data collection, this criterion will be noted as PR4.

Password Reset Method – the basic approach used for password reset by the authenticator. When a user fails authentication, they identify themselves by user ID or email address and then the options (multiple options can apply) include: a) authenticator will email link to registered address that initiates the reset process to be completed in another Web session, b) authenticator will allow reset immediately if user can prove identity using secret knowledge, c) user must enter a verification code (such as a captcha) to continue reset process, d) sends a new, assigned password to the registered email address (Furnell, 2007). In data collection, this criterion will be noted as PR5.

Reuse Counter – the number of prior passwords that each user is blocked from reusing (Campbell et al., 2007; Villarrubia et al., 2006b). The possible values are none (reuse of last allowed), two to three, four to 10, 11 to 25, 26 and over. This criterion is also called "record length" (Villarrubia et al., 2006b, p. 546). In data collection, this criterion will be noted as PR6.

No.	Criterion	Categorization	Supporting Literature
PR1	Error attempts	1 - No limit 2 - 11 to 50 tries 3 - 4 to 10 tries 4 - Less than 4 tries	Villarrubia et al., 2006b
PR2	Information about use	Y or N	Villarrubia et al., 2006b
PR3	Initial communication	1 - Non-secure 2 - Send single-use 3 - Secure channel 4 – Shared secret	Villarrubia et al., 2006b
PR4	Is existing password allowed for reuse	Y or N	Scarfone & Souppaya, 2009; Villarrubia et al., 2006b
PR5	Password reset method	1 – No reset is available 2 – Email link 3 – Immediate reset 4 – Verification code 5 – New password	Furnell, 2007
PR6	Reuse counter	1 – None (reuse of last allowed) 2 – 2 to 3 3 – 4 to 10 4 – 11 to 25 5 – 26 and over	Campbell et al., 2007; Villarrubia et al., 2006b

Table 3. PIRM Criteria

NEXT STEPS

The next steps for this area of research are to first identify a method to assemble the criteria and measures into an index. Then validate the proposed criteria and measures. Finally, data collection and statistical processes will be used to assess the reliability of the derived Index.

Creating a Composite Index

Researchers are sometimes faced with situations where it is useful to combine multiple and diverse criteria. One technique that may proven useful in some situations such as this is to establish an aggregate measure known as a composite indicator (Srebotnjak, 2007). Srebotnjak (2007) wrote "Composite indicators are designed to measure a state, trend, or process that is the scope of policy decisions" (p. 14). The degree of usefulness of a composite indicator has been described as the degree to which it applies to the content of what is being measured and a perception of legitimacy (Hezri & Dovers, 2006). The utility of a composite index derives from having it provide more value to its users than the cost of collecting the data and computing the composite index value (Rose, 1972). A composite index is structured following a four step process: selection of the indicator's components, standardization of the components, weighting of the components, and development of an aggregation mechanism (Nardo, Saisana, Saltelli and Tarantola, 2005). In this research a composite index, might created by using the specific observed criteria about authentication methods from the review of the literature and then validated by a panel of experts. The weighting of the various component elements making up the index can be based on weighing responses from the same panel of experts. The index could then be a computed value using an aggregation mechanism based on the response values elicited from the same panel of experts.

Validity

In order to assure that the future research has content validity, future work might adopt the tactic of using an anonymous panel of knowledgeable subject matter experts to review the criteria and measures proposed here. As noted by Sekaran

(2003), "a panel of judges can attest to the content validity of the instrument "(p. 206). The expert review panel can be asked to perform subject matter review to assess the completeness and accuracy of the assessment criteria proposed. Research into the use of expert panels to perform group decision making observed that the number of experts needs to be as large as practical and individual members should be sought based on demonstrated competency (Gabel & Shipan, 2004). Such a panel could be invited from a broad cross section of scholars and practitioners with the intention of drawing together a well-qualified group from categories of individuals.

Testing Index Reliability

A later phase of this research effort will be to use the index, built from the validated measures and criteria, to assess authentication methods use in one or more samples of existing systems. Given sufficient large sample sizes, it should then be possible to use statistical techniques to measure the reliability of the construct.

CONCLUSION

Prior efforts to explore authentication methods and how Web-based systems implement password controls have been accomplished using either a descriptive approach (Furnell, 2007; Furnell, 2011) or a theoretical approach (Ma et al., 2007; Villaruba et al., 2006a). It seems that limited attention has been paid to development of a tool to serve as a benchmarking instrument. Such a tool could be used to assist in assessing password strength, password usage and password initialization and reset practices used by Web-based IS. By combining a tightly focused and practical approach from Furnell (2007) with the theory-driven approaches from others as identified earlier, this research may enable Web-based systems owners and operators to assess current methods used within the systems they control in order to identify opportunities for improvement in the security of those systems. This may assist them in understanding whether or not their current methods are deficient. Further, they may then be able to determine which additional or alternate authentication methods might be considered for use in improving the authentication methods of the systems for which they are responsible.

REFERENCES

1. Acohido, B. (2009, October 9). Cyberthieves find workplace networks are easy pickings: Simple hacking techniques have potential to collect data from any entity using a digital network. *USA Today*, p. B1.
2. Benantar, M. (2006). Access control systems: Security, identity management and trust models. New York : Springer Science.
3. Campbell, J., Kleeman, D. and Ma, W. (2007). The good and not so good of enforcing password composition rules. *Information Systems Security, 16*(1), 2-8.
4. Clarke, N., Dowland, P. and Furnell, S. (2008). User authentication technologies. In S. Furnell, S. Katsikas, J. Lopez and A. Patel (Eds.), *Securing information and communications systems: Principles, technologies, and applications* (pp. 5-20). Norwood, MA: Artech House.
5. De Angeli, A., Coventry, L., Johnson, G. and Renaud, K. (2005). Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies, 63,* 138-162.
6. Firesmith, D. G. (2003). Engineering security requirements. *Journal of Object Technology, 2*, 53-68.
7. Furnell, S. (2007). An assessment of website password practices. *Computers & Security, 26*(7-8), 445-451.
8. Furnell, S. (2011). Assessing password guidance and enforcement on leading websites. *Computer Fraud & Security, 2011*(12), 10-18.
9. Furnell, S. and Zekri, L. (2006, January). Replacing passwords: In search of the secret remedy. *Network Security,* 4-8.
10. Gabel, M. and Shipan, C. (2004). A social choice approach to expert consensus panels. *Journal of Health Economics, 23*, 543-564.
11. Google (2011a). *Google accounts.* Retrieved November 21, 2011, from https://www.google.com/accounts/EditPasswd
12. Hezri, A. and Dovers, S. (2006). Sustainability indicators, policy and governance: Issues for ecological economics. *Ecological Economics, 60*, 86-99.
13. ISO/IEC. (2005). ISO/IEC 27001: Information technology: Security techniques: Information security management systems: Requirements. Geneva, Switzerland: ISO/IEC.
14. ISO/IEC. (2007). ISO/IEC 27002: Information technology: Security techniques: Code of practice for information security management. Winterhur, Switzerland: SNV Schweizerische Normen-Vereinigung.

15. Keith, M., Shao, B. and Steinbart, P. (2007). The usability of passphrases for authentication: An empirical field study. *International Journal of Human-Computer Studies, 65*(1), 17-28. doi:10.1016/j.ijhcs.2006.08.005
16. Littman, M. (1996). Guidelines for network security in the learning environment. *Journal of Instruction Delivery Systems, 10*(1), 35-40.
17. Ma, W., Campbell, J., Tran, D. and Kleeman, D. (2007). A conceptual framework for assessing password quality. *International Journal of Computer Science and Network Security, 7*(1), 179-185.
18. Magklaras, G. and Furnell, S. (2001). Insider threat prediction tool: Evaluating the probability of IT misuse. *Computers & Security, 21*(1), 62-73.
19. Nardo, M., Saisana, M., Saltelli, A. and Tarantola, S. (2005). *Handbook on Constructing Composite Indicators: Methodology and User Guide*, volume STD/DOC(200G):1 of OECD Statistics Working Paper Series. Organization for Economic Development and Co-operation (OECD), Paris.
20. Palmer, A. (2008). Criteria to evaluate automated personal identification mechanisms. *Computers & Security, 27*(7-8), 260-284. doi:10.1016/j.cose.2008.07.007
21. Rhee, H., Kim, C. and Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816-826. doi:10.1016/j.cose.2009.05.008
22. Rose, R. (1972). The market for policy indicators. In Andrew Shonfield and S. Shaw (Eds.), *Social Indicators and Social Policy* (119-141). London: Heinemann.
23. Ruffo, G. and Bergadano, F. (2005). EnFilter: A Password Enforcement and Filter Tool Based on Pattern Recognition Techniques. In Lecture Notes in Computer Science: Volume 3617.Image Analysis and Processing (pp. 75-82). Berlin, Germany: Springer-Verlag. doi:10.1007/11553595_9
24. Sandhu, R. and Samarati, P. (1996). Authentication, access control, and audit. *ACM Computing Surveys, 28*(1), 3.
25. Sandhu, R., Coyne, E., Feinstein, H. and Youman, C. (1996). Role-based access control models. *IEEE Computer, 29*(2), 10.
26. Scarfone, K. and Souppaya, M. (2009). Guide to enterprise password management (Draft) (NIST Special Publication 800-118). Retrieved from National Institute of Standards and Technology Website: http://csrc.nist..gov/publications/drafts/800-118/draft-sp800-118.pdf
27. Sekaran, U. (2003). Research methods for business - A skill building approach. Hoboken, NJ: John Wiley & Sons.
28. Shimizu, A., Horioka, T. and Inagaki, H. (1998). Password authentication method for contents communications on the internet. *IEICE Transactions on Communications, E81-B*(8), 1666-1673.
29. Srebotnjak, T. (2007). The development of composite indicators for environmental policy: Statistical solutions and policy aspects. Available from ProQuest Dissertations and Theses database. (UMI No. 3293388)
30. The Password Meter (2011). *Password Strength Checker.* Retrieved November 21, 2011, from https:// http://www.passwordmeter.com/
31. Vijaya, M., Jamuna, K. and Karpagavalli, S. (2009). Password strength prediction using supervised machine learning techniques. Proceedings of the 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies, Trivandrum, Kerala, Indi, 401-405. doi:10.1109/ACT.2009.105
32. Villarrubia, C., Fernandez-Medina, E. and Piattini, M. (2006a). Metrics of password management policy. In Lecture Notes in Computer Science: Vol. 3982. Computational Science and its Applications (pp. 1013-1023). Berlin, Germany: Springer-Verlag. doi:10.1007/11751595
33. Villarrubia, C., Fernandez-Medina, E. and Piattini, M. (2006b). Quality of password management policy. *Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06)*, Vienna, Austria.
34. Weir, C., Douglas, G., Richardson, T. and Jack, M. (2010). Usable security: User preferences for authentication methods in eBanking and the effects of experience. *Interacting with Computers, 22*(3), 153-164. doi:10.1016/j.intcom.2009.10.001
35. Wood, H. (1977). The use of passwords for controlling access to remote computer systems and services. *AFIPS '77: Proceedings of the June 13-16, 1977, National Computer Conference* (pp. 27-33).