Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2012 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-15-2012

Assessing Relative Weights of Authentication Components: An Expert Panel Approach

Herbert J. Mattord
Kennesaw State University, hmattord@kennesaw.edu

Yair Levy
Nova Southeastern University, levyy@nova.edu

Steven Furnell
Plymouth University

Assessing Relative Weights of Authentication Components: An Expert Panel Approach

Herbert J. Mattord[1]
Coles College of Business, Kennesaw State University,
Kennesaw, GA, USA

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

Steven Furnell
School of Computing and Mathematics, Plymouth University,
Plymouth, Devon, UK

ABSTRACT

Organizations rely on password-based authentication methods to control access to many Web-based systems. In a recent study, we developed a benchmarking instrument to assess the authentication methods used in these contexts. Our instrument developed included extensive literature foundation and an expert panel assessment. This paper reports on the development of the instrument and the expert panel assessment. The initial draft of the instrument was derived from literature to assess 1) password strength requirements, 2) password usage methods, and 3) password reset requirements. Following, the criteria within the index were evaluated by an expert panel and the same panel provided opinions on the relative weights of the criteria and the measures. The expert panel results were collected and analyzed using Multi-Criteria Decision Analysis (MCDA) techniques. We conclude with discussions on how the criteria were assembled, how the expert panel was conducted, and reporting the results from the panel. The results reported include the relative weights within te password usage and password reset measures as well as the relative weights of the three measures within the index.

[1] Corresponding author. hmattord@kennesaw.edu. +1 770 420 4741

Keywords: Authentication Methods, Password Authentication, Expert Panel Assessment, Multi-Criteria Decision Analysis (MCDA)

INTRODUCTION

Organizations continue to rely on password-based authentication methods to control access to many Web-based systems. In a recent study, we developed a benchmarking instrument to assess aspects of authentication methods used by Web-based information systems (ISs). We developed the Authentication Method System Index (AMSI) and collected data from representative samples of Web-based ISs in order to compare authentication methods measured and validate its effectiveness. The AMSI and its accompanying benchmarking instrument were developed from criteria drawn from academic literature, practitioner references, as well as industry standards. The AMSI measures 1) password strength requirements, 2) password usage methods, and 3) password reset requirements. Those measures were used to derive a single index value that represents an assessment of the quality of current authentication methods employed by Web-based systems. In this paper, we provide an overview of the expert panel work conducted as part of the AMSI development and validation, and summarize some literature on authentication methods. Then, we discuss the results of the expert panel work and conclude with some ideas about future research into this topic.

AUTHENTICATION METHODS

Access control includes those methods that are specified by systems to govern the identification, authentication, authorization, and accountability of systems users (Firesmith 2003). 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 et al. 2008; Sandhu and Samarati 1996). 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 et al. 1996). Accountability, sometimes called security auditing, is the means by which a system records its actions for later analysis (Firesmith 2003). For example, a firewall control, implemented in a hardware appliance, will often record all access attempts and the results of each of those attempts in a system log file.

An authentication method is a technique used by a system to perform authentication of potential users in order to confirm the identity of the user. Authentication methods include specifying 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 and Samarati 1996). 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 as widespread and growing (Acohido 2009; Ramim and Levy 2006). Moreover, Acohido 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" (Acohido 2009). Unfortunately, it is widely known that authentication methods that rely solely on passwords are easily compromised (Furnell and Zekri 2006). Such compromises may allow misuse of the ISs when they are protected by methods built on specifications of insufficient authentication methods (D'Arcy and Hovav 2007). The potential for misuse exists when insiders or outsiders exploit insufficient authentication methods or practices to gain unauthorized access to perform unauthorized actions (Furnell and Zekri 2006).

A variety of methods can be used to perform authentication (Benantar 2006; Clarke et al. 2008; Shimizu et al. 1998; Villarubia et al. 2006a; Weir et al. 2010; Wood 1977). Authentication

requires that the entity seeking access 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 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*) (Levy et al. 2011). These three factors of authentication are well defined and are "fundamentally different from one another" (Benantar 2006). 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).

Password Strength, Usage, and Reset Requirements

In this section, we provide a brief review of some relevant research published in the area of authentication using password-based techniques to identify some of the characteristics of this method that can later be assessed by the expert panel. Several scholars have indicated over the past several decades the continuing predominant use of passwords as an authentication method (Littman 1996; Furnell and Zekri 2006). We uncovered during the review of the authentication literature, repeated significant concerns with: 1) criteria regarding the strength of passwords used, 2) criteria regarding the usage of passwords, as well as 3) requirements regarding password initiation and resetting.

The topics of password strength and use have been included in the published research by several scholars (Campbell et al. 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 et al. 2007; Villaruba et al. 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 the edit distance of a password from a standardized set of dictionary words and the effective password length (Keith et al. 2007). Edit distance reflects the combination of ways in which the use of numbers, special characters, and case shifting can be use to make passwords less similar to the chosen set of dictionary words (Keith et al. 2007; Ma et al. 2007). PQI is similar to efforts by organizations and individuals to implement a variety of password strength measures (Ma et al. 2007; Palmer 2008). While PQI offers a sound theoretical approach, it has not been operationalized into an accessible mechanism to assess password strength. In order to provide a measurement that is more useful in the context of this research, an alternative that implements constructs drawn from PQI will be used.

Some Web–based systems utilize password strength measurement technologies to offer feedback to users (Vijaya et al. 2009). Different password strength tools each use varied approaches to implement lexical analysis to assess the quality of a password (Vijaya et al. 2009). If desired, a developer may choose to disallow selection of passwords that fall below specifications.

While the literature has explored the various facets of authentication, the work so far has been done in a piecemeal fashion where each topic is explored on its own. This research

proposes to synthesize some of the aspects of authentication previously explored into a benchmarking measure that adds value to the field. This might allow IS designers, quality assurance teams, and information security practitioners charged with validating ISs, a benchmarking tool they can use to measure the effectiveness of such authentication methods. This can enable continuous improvement of authentication methods employed in such Web-based systems.

Drawing from the literature, we chose the criteria for use in assessing password strength including: the number of subdivisions of characters in the choice set, the number of characters in the choice set from which passwords are assembled, and the fewest number of characters that make up a valid password (Campbell et al. 2007; Furnell 2007; Furnell 2011; ISO/IEC 2007; Ma et al. 2007; Villarrubia et al. 2006b). These criteria for password strength (PS) were assigned identifiers of PS_n.

The criteria chosen to assess password usage are: time and circumstances after an authentication is granted until re-authentication is required, how the client receives feedback, longest length of time that a password is valid, use of mutual authentication, guidance provided to users about selecting passwords, how the password is transmitted from the user to the server, and training requirements (De Angeli et al. 2005; Furnell 2007; ISO/IEC 2007; Palmer 2008; Ruffo and Bergadano 2005; Villarrubia et al. 2006b). The password usage (PU) criteria were assigned an identifier of PU_n.

The criteria used to assess password initialization and reset requirements are: maximum number of failed attempts allowed, whether users are notified of the date and time of the past use of their credentials, how an initial password is communicated, how passwords are assigned for a password reset, approach used for password reset by the authenticator, and number of prior

passwords blocked from reuse (Campbell et al. 2007; Furnell 2007; Scarfone and Souppaya 2009; Villarrubia et al. 2006b). The password initialization and reset (PR) criteria were assigned identifies of PR_n.

A composite index was created by selecting specific criteria used by some Web-based systems upon review of the literature. The validity and weighting of the various component elements making up the index were assessed using a panel of experts. An aggregation used the measurements to calculate a response using the weight values elicited from the same panel of experts.

Multiple-Criteria Decision Analysis (MCDA) and Composite Indices

Real-world decision making is often confronted with situations where a single criteria is not able to offer a solution to the problem being considered (Chen et al. 2008). Multiple-criteria decision analysis (MCDA), also called multi-criteria decision aid or multi-criteria decision making (MCDM), is an advanced field of Operations Research (OR) that offers theories and techniques that can be used to confront complex problems involving multiple criteria (Roy 2005). Researchers are sometimes faced with situations where it is useful to combine multiple and diverse criteria. One technique that has proven useful in some situations is to establish an aggregate measure known as a composite indicator (Srebotnjak 2007).

Within the realm of MCDA, one approach used to develop aggregated indices is multi-attribute utility theory (MAUT). MAUT is a structured approach that allows an overall evaluation based on the weighted addition (linearly or non-linearly) of multiple criteria (Belton and Stewart 2002). The modeling of decision maker's preferences is referred to as weight elicitation and can be accomplished in a number of ways including analytical hierarchical processing (AHP) using pair-wise comparison of each criteria, or some form of direct weighting

using either ratio between criteria or a method of allocating points among criteria (Bottomley et al. 2000).

APPROACH

The AMSI used three measures. These measure were: the password strength measure (PSM), the password usage measure (PUM) and the password initiation and reset measure (PIRM). The PSM was assessed using the PS criteria measured by observation and then used to derive a PSM indicator value. As it is a proven and reliable tool that produces assessments that are semantically compatible to this research, conforming passwords were assessed using The Password Meter (Vijaya et al. 2009). To derive the PSM, 10 passwords were generated such that the candidate passwords were each in conformance with the sample's password strength criteria (PS01 to PS06). Each unique candidate password was submitted to The Password Meter. The Password Meter text responses were recorded using an established numeric equivalent. The 10 responses were averaged and the resulting mean was used to assess the PSM.

The PUM was derived by first assessing each of the measured PU criteria using established criteria. That resulting value was then multiplied by an elicited preference weight from the expert panel for that criterion. Then, each of the criterion's intermediate weighted values was summed to arrive at a single composite indicator value for the PUM of the sampled organization. This was computed using the formula noted in Equation 1.

$$\mathrm{PUM} = \overrightarrow{\mathrm{PU}} \bullet \overrightarrow{\mathrm{W}}_{\mathrm{PU}} \qquad (1)$$

Where ● is defined as the dot product between vector PU that is the observed criteria and vector W_{PU} that is the elicited preference weight from the expert panel for password usage criteria.

The PIRM was derived by first assessing each of the measured PR criteria using established criteria. That resulting value was then be multiplied by an elicited preference weight from the expert panel for that criterion. Each individual weighted criterion value was summarized to arrive at a single composite indicator value for the PIRM of the sampled organization and was computed as:

$$\text{PIRM} = \overrightarrow{\text{PR}} \bullet \overrightarrow{\text{W}}_{\text{PR}} \quad (2)$$

Where ● is defined as the dot product between vector PR that is the observed criteria and vector W_{PR} that is the elicited preference weight from the expert panel for password usage criteria.

The AMSI combined the measures previously described (PSM, PUM, and PIRM). This was done using the following computation:

$$\text{AMSI} = \begin{bmatrix} \text{PSM} \\ \text{PUM} \\ \text{PIRM} \end{bmatrix} \bullet [\text{W}_{\text{PSM}} \quad \text{W}_{\text{PUM}} \quad \text{W}_{\text{PIRM}}] \quad (3)$$

The relationship amongst the elements of the AMSI is shown in Figure 1.

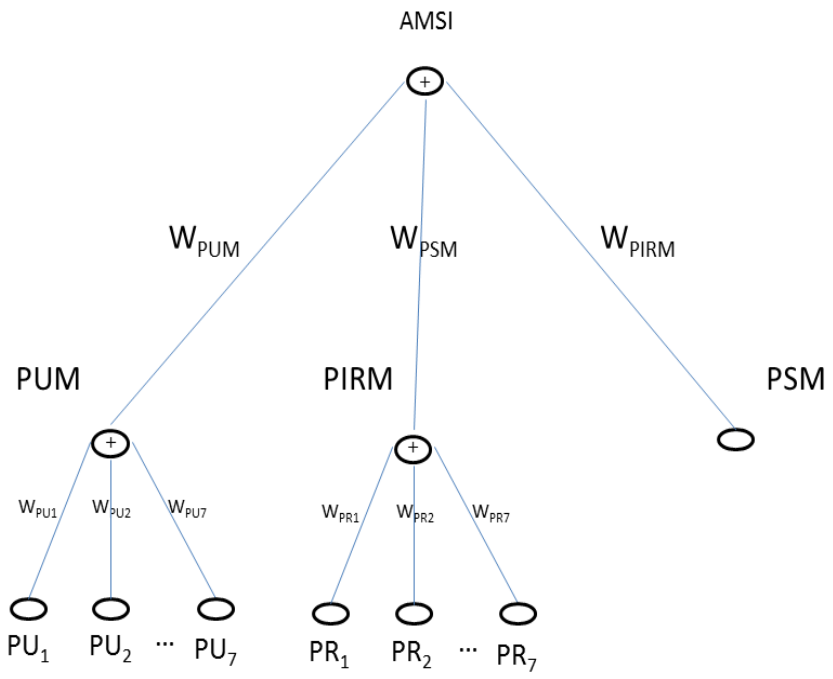

Figure 1. Hierarchical Ontology of the AMSI Index, Measures, and Criteria

Validity and Reliability

In order to assure that the approach had content validity, this research adopted the tactic of using an anonymous panel of knowledgeable subject matter experts to review elements of the proposed study including the hierarchical ontology of the AMSI Index, the AMSI measures, and the AMSI criteria. This expert review panel performed a subject matter review to assess the completeness and accuracy of the assessment criteria. Upon completion of their review, the proposed revisions were carefully considered, and the criteria for assessment were updated where indicated. The expert panel members were invited from a broad cross section of information security scholars and practitioners. In order to perform a valid expert panel decision making, the number of experts needed to be as large as possible and individual members should be sought based on demonstrated competencies related to the assessment of the decision making (Gabel and Shipan 2004). Gabel and Shipan wrote "to maximize the chance of an accurate

decision, panels should be made as large as possible" (Gabel and Shipan 2004). Thus, in this expert panel assessment, we have taken all possible avenues to obtain a large group of participants in the expert panel decision making phase.

RESULTS

The expert panel came from a pool of 35 individuals approached from academic and professional information security society mailing lists in addition to information security experts known to us. A Web-based survey tool engaged the expert-participants to record opinions and observations using the survey instrument. The survey was initiated by 28 expert-participants and five incomplete responses were omitted resulting in 23 completed expert survey responses. That represents a survey response rate of 80% and a survey completion rate of roughly 66%, which is considered high in these types of exploratory studies.

About the Expert Panel

In order to gauge the characteristics of the respondents, questions were asked about how respondents perceived their information security role as well as some measurements about professional activities and frequency and/or duration of various types of experience. The first of these questions asked the respondent to report about their perceived information security role - an academic and/or a practitioner. The aggregate responses to these questions are presented in Table 1.

Table 1. Experts' Self Perception of Information Security Role

Self-Identified Information Security Role	Number	Percentage
I consider myself to be an academic	1	4.3%
I am both an academic and a practitioner but am mostly focused on academics (teaching and scholarship)	8	34.7%
I consider myself to be evenly balanced as both a practitioner and an academic	2	8.6%
I am both a practitioner and an academic but I am mostly focused on the practice of information security	7	30.4%
I consider myself to be a practitioner	5	21.7%

Of interest in the results of the self-reported perception of the respondents is that a large majority of respondents view themselves as some combination of academic and practitioner information security experts, representing 17 of 23 responses or almost 74%. It is not known if this is simply a phenomenon based on who was invited or an aspect of the information security profession that majority of the academicians in this field consider themselves also as information security practitioner expert.

Elicited Weights for Criteria and Measures

In addition to reviewing the structure and questions of the AMSI, the expert-respondents were asked to allocate the relative weight for each of the criteria within two of the measures PUM and PRM, while no such elicitation was done for the third PIRM since it is based on actual system information. In addition, expert-respondents were asked to allocate the relative weight for each of the three measures within the AMSI. In the first request for point allocation, the expert panel was asked to allocate 100 points across the seven criteria within the PUM. The mean of the responses from the experts for that allocation is presented in Table 2.

Table 2. Password Usage (PU) Criteria Elicited Weights

Criterion	Weight
PU1 - How long does each authentication session retain validity?	21.0
PU2 - How is the users input of a password visualized to them by default?	9.4
PU3 - How long does a password remain valid?	15.7
PU4 - Is some form of mutual authentication in use?	12.0
PU5 - What password guidance/enforcement is used?	14.1
PU6 - How is the user credential transmitted from the user's browser to the Web server?	16.3
PU7 - What user training is readily available?	11.5

Next, the expert panel was asked to allocate 100 points across the six criteria within the PIRM. The mean of the responses from the experts for that allocation is presented in Table 3.

Table 3. Password Reset (PR) Criteria Elicited Weights

Criterion	Weight
PR1 - How many incorrect login attempts are allowed without recourse?	26.4
PR2 - Is information about the last use of the user ID made known to the user at next login?	11.1
PR3 - How is the initial password communicated to user?	14.4
PR4 - Is a prior password allowed to be reused?	12.2
PR5 - What password reset options are available?	21.1
PR6 - How many password changes until a prior password can be reused?	14.7

The single largest PR criteria was the number of logins allowed before recourse, confirming the expected results of some prior researchers (Furnell 2007).

As a final request for elicited weight using point allocation, the expert panel was asked to allocate 100 points between the PSM, PUM, and PIRM measures within the AMSI. The mean of the responses from the experts for that allocation is presented in Table 4.

Table 4. AMSI Measure Elicited Weights

Measure	Weight
Password Strength Measure - PSM	43.1
Password Usage Measure - PUM	27.7
Password Initialization and Reset Measure - PIRM	29.2

Password strength, represented by the PSM in this study, is the dominant factor in the aggregated perception of the panel of experts.

RECOMMENDATIONS AND FUTURE RESEARCH

The ability to measure the utility of the authentication methods use by Web-based systems may be advantageous to practitioners and owners of such systems. Understanding the components of such methods and the relative importance of each of the criteria would offer value to these audiences as they consider options to perform authentication. Given the relatively small sample size of the preliminary study undertaken in this paper (23 experts), while we understand the considerable efforts needed to expand expert panel sample size, future work should attempt

to broaden the size of the sample. That would enable improved validation of the criteria that have been proposed and more assurance that the weights of the criteria within the measures and the weights of the measures within the index are representative of the broader communities of scholars and practitioners. Additionally, some methodological choices used in the study may have limited the validity of the results. The use of only 10 randomly assigned passwords in assessing password strength may have resulted in imprecise outcomes and future research should implement a larger number of random assigned passwords.

Another aspect of future research could explore the self-reported perception of those involved in information security. As noted earlier, nearly 74% of the respondents to the expert panel survey in this paper considered themselves to be both information security scholars and practitioners. It is possible that this is a unique aspect of information security scholars as compared to other scholar groups or is a phenomenon on this sample group only. Further study into the self-perception of those employed in the information security field as compared to other fields might provide further insight.

REFERENCES

Belton, V., and Stewart, T. 2002. *Multiple Criteria Decision Analysis: An Integrated Approach*. Norwell, Massachusetts: Kluwer Academic Publishers.

Benantar, M. 2006. *Access Control Systems: Security, Identity Management and Trust Models.* New York: Springer Science.

Bottomley, P., Doyle, J., and Green, R. 2000. "Testing the Reliability of Weight Elicitation Methods: Direct Rating Versus Point Allocation," *Journal of Marketing Research* (37:4), November, pp. 508-513.

Campbell, J., Kleeman, D., and Ma, W. 2007. "The Good and Not So Good of Enforcing Password Composition Rules," *Information Systems Security* (16:1), January/February, pp. 2-8.

Chen, Y., Kilgour, D., and Hipel, K. 2008. "Using a Benchmark in Case-based Multiple-criteria Ranking," *IEEE Transactions on Systems, Man, and Cybernetics-Par A: Systems and Humans* (39:2), March, pp. 358-368.

Clarke, N., Dowland, P., and Furnell, S. 2008. "User Authentication Technologies," in *Securing information and communications systems: Principles, technologies, and applications,* S.

Furnell, S. Katsikas, J. Lopez, and A. Patel (Eds.), Norwood, MA: Artech House, pp. 5-20.

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), pp. 138-162.

D'Arcy, J., and Hovav, A. 2007. "Towards a Best Fit Between Organization Security Countermeasures and Information Systems Misuse Behaviors," *Journal of Information System Security* (3:2), pp. 4-30.

D'Arcy, J., and Hovav, A. 2009. "Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures," *Journal of Business Ethics* (89:1), pp. 59-71.

Firesmith, D. G. 2003. "Engineering Security Requirements," *Journal of Object Technology* (2), pp. 53-68.

Furnell, S. 2007. "An Assessment of Website Password Practices," *Computers & Security* (26:7-8), pp. 445-451.

Furnell, S. 2011. "Assessing Password Guidance and Enforcement on Leading Websites," *Computer Fraud & Security* (2011:12), pp. 10-18.

Furnell, S., and Zekri, L. 2006. "Replacing Passwords: In Search of the Secret Remedy," *Network Security* (2006:1), January, pp. 4-8.

Gabel, M., and Shipan, C. 2004. "A Social Choice Approach to Expert Consensus Panels," *Journal of Health Economics* (23), pp. 543-564.

ISO/IEC 2007. *ISO/IEC 27002: Information Technology: Security Techniques: Code of Practice for Information Security Management*, Winterhur, Switzerland: SNV Schweizerische Normen-Vereinigung.

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), pp. 17-28.

Levy, Y., Ramim, M., Furnell, S. and Clarke, N. 2011. "Comparing Intentions to Use University-provided vs. Vendor-provided Multibiometric Authentication in Online Exams," *Campus-Wide Information Systems* (28:2), pp, 1-10.

Littman, M. 1996. "Guidelines for Network Security in the Learning Environment," *Journal of Instruction Delivery Systems,* (10:1), January, pp. 35-40.

Palmer, A. 2008. "Criteria to Evaluate Automated Personal Identification Mechanisms," *Computers & Security* (27:7-8), pp. 260-284. doi:10.1016/j.cose.2008.07.007

Ramim, M. M., and Levy, Y. 2006. "Securing E-learning Systems: A Case of Insider Cyber-attacks and Novice IT Management in a Small University," *Journal of Cases on Information Technology* (8:4), pp. 24-34.

Roy, B. 2005. "Paradigms and Challenges," in *Multiple Criteria Decision Analysis: State of the Art Surveys. International Series in Operations Research and Management Science,* M. Ehrgott, J. Figueira and S. Greco (Eds.), Springer. pp. 3-24.

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*, Berlin, Germany, Springer-Verlag, pp. 75-82

Sandhu, R., and Samarati, P. 1996. "Authentication, Access Control, and Audit," *ACM Computing Surveys* (28:1), pp. 3.

Scarfone, K., and Souppaya, M. 2009. "Guide to Enterprise Password Management (Draft)," *NIST Special Publication 800-118*. National Institute of Standards and Technology, Washington DC.

Shimizu, A., Horioka, T., and Inagaki, H. 1998. "Password Authentication Method for Contents Communications on the Internet," *IEICE Transactions on Communications* (E81-B:8), pp. 1666-1673.

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)

The Password Meter 20110. *Password strength checker.* Retrieved November 21, 2011, from https:// http://www.passwordmeter.com/

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,* pp. 401-405.

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*, Berlin, Germany: Springer-Verlag, pp. 1013-1023

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.

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), pp. 153-164.

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.*