Is Buying and Transacting Online Easier and Safer than Down Town? : An Emerging Economy Perspective

Edna Martim[1], Moses Dlamini[1], Darelle van Greunen[2], Jan Eloff [3] Marlien Herselman [4]
SAP Research CEC Pretoria[1], Nelson Mandela Metropolitan University[2], University of Pretoria[3], Tshwane University of Technology[4], Pretoria, South Africa
[1]edna.martim@sap.com
[1]moses.dlamini@sap.com
[2]Darelle.vanGreunen@nmmu.ac.za
[3]eloff@cs.up.ac.za
[4]HerselmanME@tut.ac.za

Abstract: Security and usability are crucial factors for the successful of any e-commerce system. However, they have traditionally been considered a design trade-off. In an effort to align them, this paper highlights the design principles and guidelines for usable and secure systems. These principles and guidelines are used to evaluate and demonstrate several real-life cases of effective and less effective security and usability implementations in an emerging economy (South African) context.

Keywords: security, usability, e-commerce, retail, banking, emerging economy.

1. Introduction

E-commerce has the potential to reach global markets without limits, reduce marketing and advertising costs, expand customer bases, build reliable customer intelligence and increase profits (Vatanasombut, Stylianou & Igbaria, 2004). These are but a few of its benefits that can be leveraged to improve firms' competitiveness. By now most customers and firms in emerging economies are expected to be diving head first into e-commerce. Yet, a significant number is still reluctant and not comfortable to do their shopping and transactions online. Is e-commerce failing to achieve its full potential or people are just not aware or transacting and shopping down town is still considered much easier and safer than online?

There are several barriers that contribute to less acceptance and adoption of e-commerce. Schaaper (2008) highlights the following "no need to buy online", "security concerns", "trust concerns", "privacy concerns", "lack of skills", "no payment cards" and "online shopping and transacting is too expensive". Schaaper (2008) also argues that news headlines about credit and debit card fraud constitute another serious barrier.

In emerging economies, specifically in the South African (SA) context, these obstructing factors include aspects such as cultural impediments (Macagnano & Greeff 2007), people's resistance to change, technical difficulties, post-apartheid effects, illiteracy (Wesson, 2000; Hugo, 2002), lack of customer trust (Barnard & Wesson, 2003), lack of technical skills to design good user interfaces (Wesson, 2000), security and usability (Yee, 2004).

This paper considers security and usability in the application domain of e-commerce. The rationale behind this choice emanates from the fact that consumers do not fully understand e-commerce security and usability issues. In any case, what would you expect when security mechanisms are designed by security experts who would rather have 100% secure e-commerce software that is completely unusable than to have 99% secure e-commerce software that is usable (Gedda, 2006)?

A lack of usability could easily render a secure e-commerce system insecure as users circumvent or disable security systems (Balfanz *et al*., 2004). E-commerce security mechanisms are also useless if they cannot be used, and usable e-commerce systems are useless if the systems are insecure.

When users cannot find what they are looking for, they simply cannot transact (Schaffer & Sorflaten 1999; Bias & Mayhew 2005; Lauesen, 2005). Moreover, unless users know for sure that their personal and payment card details are safe they will not transact online. Based on the above, usability and security are no longer a luxury, but rather a basic requirement of e-commerce systems (Nielsen & Norman, 2000; Barnard & Wesson, 2003).

The next section begins with a discussion of related work. Next is a section on the outline of design principles and guidelines for usable and secure systems. These design principles and guidelines are used to evaluate and demonstrate several cases of effective and less effective security and usability implementations in an emerging economy (SA context). The last section concludes the paper.

2. Related Work

2.1 E-commerce Definition and Statistics

Several definitions have been proposed for e-commerce (McLaren & McLaren, 2000; Barnard & Wesson, 2003). However, for the purpose of this paper, e-commerce is defined as allowing customers to purchase items and conduct financial transactions over the Internet with ease of use, securely and effectively.

E-commerce has substantially increased in SA over the past few years. ICT World (2007) reported about R243 million spent on online between November and December in 2006, compared with just R26 million in 2004 over the same period. The number of transactions over the Christmas period increased from 38 902 in 2004 to 241 438 in 2006. This may seem a huge increase, but it is almost insignificant when compared to the overall expenditure in conventional shopping over the Christmas period.

2.2 Security and Human/Computer Interactions

Security and human/computer interaction (HCI) have traditionally been considered a design trade-off (Yee, 2004; Rozinov, 2004; Payne & Edwards, 2008; Hafiz *et al*., 2008). Several researchers (Zurko & Simon, 1997; Yee, 2002; Smith, 2003; Balfanz *et al*., 2004; Whitten, 2004; Reeder & Arshad, 2005; Gutmann & Grigg, 2005; Furnell, 2007; Camp, 2007; Cranor, 2008; Payne & Edwards, 2008) have done significant work in trying to merge and align these fields. However, there is still no work (at least according to the authors) that addresses both security and usability in e-commerce application domain.

The available literature shows that existing HCI criteria can be used to analyse and enhance security features of an interface to make it usable (Johnston, Eloff & Labuschagne, 2003). The argument is that a good interface can promote users' understanding of a specific technology. However, Balfanz *et al*. (2004) refute this with the claim that adding explanatory dialog boxes to a complex, confusing and unusable security system is not an answer. Even the best interface cannot solve usability issues if applied as an after-thought.

Falk, Prakash and Borders (2008) analysed websites of financial institutions for security design flaws. This paper analyses web sites in both the retail sector and banking sector. Furthermore, unlike (Falk, Prakash and Borders, 2008), this paper analyses the web sites for both usability and security design flaws. The choice of banking and retail sector is chosen to eliminate any biases that might be introduced by an individual sector since the goal is to get generic results that will reflect on more than just one sector. Each of the four chosen web sites is evaluated against usability and security design principles and guidelines.

2.3 Usable Security

Passwords provide a helpful example of the conflict between security and ease of use and, thereby, of the need for a concept of usable security (e.g. Morris & Thompson, 1979). While passwords such as person names are relatively easy for a user to remember, they are weak from a security point of view because they are vulnerable to dictionary attacks. Strong passwords (e.g. y3j%t#C2) are less vulnerable to attack but at the same time more difficult to remember. Hence, Payne and Edwards (2008) argues that password selection guidelines focus more on security than usability. Moreover, people are increasingly getting more accounts. How then can we resolve such conflict?

The term 'ease of use' is used in this paper in the sense of learnability and understandability of user interfaces. The ISO 9241-11 (1998) definition of usability is widely accepted. This standard defines usability as the *"extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use."* This broad definition equates usability to the quality of a system in use and thereby addresses the entire issue of whether the system meets the needs of actual users. Specifically, effectiveness includes whether a system enables users to achieve their goals at an appropriate level of security, and likewise, ease of use is contained within the ISO 9241-11 definition of usability.

The usable security aspect of such systems appears not to be fully understood. Several studies suggest that security measures that are inconvenient for users may weaken security, due to lack of user acceptance or outright resistance. Dourish and Redmiles (2002) propose a distinction between theoretical and effective security. Theoretical security concerns the level of security that is technically possible. For example, digital signatures provide strong authentication on the assumption that various difficult computational problems related to prime numbers will not be solved within some time frame. Effective security concerns the level of security achieved in practice and is typically lower than theoretical security, due to weaknesses with respect to (among other things) algorithm implementations, protocol design – and ease of use.

Whitten and Tygar (1999) suggest that security-related software is usable if the people who are expected to use it

- are reliably made aware of the security tasks they need to perform;
- are able to figure out how to successfully perform those tasks;
- don't make dangerous errors;
- are sufficiently comfortable with the interface to continue using it.

This definition addresses the effectiveness, efficiency and satisfaction of security-related software, and so agrees with ISO 9241-11 (1998).

3. Principles for Designing a Usable and Secure e-commerce System

Several security and usability design principles and guidelines are available in literature (e.g. Yee, 2002; Stoneburner, Hayden & Feringa, 2004; Information Systems Security Association (ISSA), 2004) and (e.g. Norman, 1990; Neilsen, 1993; Shneiderman, 1998) respectively. With regard to security, the study considers some of the key design principles of achieving a baseline security as stated in the National Institute of Standards and Technology NIST Special Publication 800-27 Rev A (Stoneburner, Hayden & Feringa, 2004). These have been combined with some of the Generally Accepted Information Security Principles (GAISP v.3) as stated by ISSA (2004) in the context of e-commerce system design. Put together, these principles form a baseline e-commerce security. On the other hand, the study considers a set of guidelines based on Nielsen's heuristics (1993). Table 1 and Table 2; outline these design principles and guidelines.

Table 1: Nielsen's design principles for designing a usable e-commerce system

	Design principle	Description
1	Visibility of system status	Improving the visibility of the state of usability will allow online users to make informed choices.
2	Match between system and the real world	It is necessary to use language, phrases and concepts known to the user.
3	User control and freedom	The e-commerce site should support user control and freedom. Users need to feel they are in control at all times. Web sites should clearly mark exits for the user to leave the unwanted state with ease.
4	Consistency and standards	The wording, icons and command buttons should be used consistently.
5	Error prevention	Error-prone conditions should be eliminated. Errors should be checked for, and users be presented with a confirmation option before they commit to the action.
6	Recognition rather than recall	Objects, actions and options should be made visible to minimise memory load. Users should recognise where they are all the time.
7	Flexibility and efficiency of use	The e-commerce system should be effective and flexible to use.
8	Aesthetic and minimalist design	Dialogues should not contain information that is irrelevant or rarely needed. Such information must be short and precise.
9	Help user recognise, diagnose and recover from errors	Error messages should be expressed in plain language, the problem should be precisely indicated, and a constructive solution be suggested.
10	Help and documentation	Even though it is better if the e-commerce system can be used without documentation, it may be necessary to provide help and documentation.

(**Adapted from:** Nielsen, 1993)

Table 2: Information security design principles and guidelines for designing a secure e-commerce system

	Design Principle	Description
1	Make security an integral part of system design	Security must be considered at system design and should not be "bolted-on" as an afterthought to an already fully developed system.
2	Protect information (confidentiality, integrity and availability) with the proportionality principle in all forms	The system and their information assets must be protected at all mediums. Moreover, their value, sensitivity and criticality must be considered along with the risk
3	Minimise critical resources and implement least privileges	Critical or sensitive information must be kept in isolation and access to such resources must be done on a need-to-know basis.
4	Design, implement and monitor audit mechanisms	Through a unique user ID, each and every user record can be monitored for malicious activities and unauthorised access.
5	Use open standards for portability and interoperability	The system must be technology independent and able to work with different systems.
6	Use common language	The system must use what is being generally acceptable and must not deviate from the norm.
7	Strive for operational ease of use	The system must not be complex and complicated, but it must be easy to use in practice – even for a novice user.
8	Design an e-commerce system that is resilient in the face of expected threats	Fail-safe options should be provided, rather than to allow the whole system to go down. In the case of a threat, some part of the system must remain available.
9	Isolate public access resources from mission critical resources	Publicly available information on products must not be stored together with sensitive and critical information. Critical information must be stored in an encrypted form on a different network segment that is well protected.

10	Prevent common errors	The rule of thumb is to prevent errors, but should prevention fail, the system must fail safely without serious consequences.

(**Adapted from** ISSA, 2004 and Stoneburner, Hayden & Feringa NIST, 2004)

4. Case Studies

A heuristic evaluation of four SA e-commerce systems was conducted to uncover both usability and security design flaws only on the front end (client interface); from the retail and banking sector. The heuristic evaluation was done using the combined principles and guidelines described in the above tables 1 and 2. Moreover, they were also conducted on several tasks that are involved when a user is buying and transacting online on the front end. For the retail sector, the evaluated tasks included the analysis of the homepage, registration process, login, item selection, shopping cart, entering the payment details and logout. For the banking sector the tasks included the analysis of the homepage, registration, login and logout processes. The analysis and evaluation did not go into the actual buying and transacting process. As mentioned earlier, the choice of banking and retail sectors was made in order to eliminate any biases that might be introduced by an individual sector since the goal is to get generic results that will reflect on more than just one sector. The results seek to illustrate the cases of effective and less effective security and usability implementation on South African e-commerce systems. E-commerce systems from the retail sector are referred to as EC 1 and EC 2 and those from the banking sector are referred to as EC 3 and EC 4.

5. Results

Table 3 highlights the heuristic evaluation results of both table 1 and table 2. Where (3) indicates that the principle is fully implemented, (2) indicates that the principle is partly implemented but requires more work, (1) indicates that it could not be ascertained whether the principle has been implemented or not, and (0) indicates that the principle was not implemented.

Table 3: Heuristic evaluation results for four e-commerce systems

	Principles	**Retail**		**Banking**	
	Principles for designing a usable e-commerce system	**EC 1**	**EC 2**	**EC 3**	**EC 4**
1	Visibility of system status	3	3	3	3
2	Match between system and the real world	2	3	3	3
3	User control and freedom	2	2	0	0
4	Consistency and standards	2	3	3	3
5	Error prevention	0	3	2	3
6	Recognition rather than recall	2	3	0	3
7	Flexibility and efficiency of use	3	3	0	3
8	Aesthetic and minimalist design	1	1	0	3
9	Help user recognise, diagnose and recover from errors	1	2	3	3
10	Help and documentation	3	3	3	3
	Principles for designing a secure e-commerce system	**EC 1**	**EC 2**	**EC 3**	**EC 4**
11	Make security an integral part of design	0	0	3	3
12	Protect information with the proportionality principle in all forms – in transit, storage and at processing	0	0	2	3
13	Minimise critical resources and implement least privileges	1	1	3	3
14	Design, implement and monitor audit mechanisms	1	1	3	3
15	Use of open standards for portability and interoperability	3	3	3	3
16	Use common language	0	3	3	3
17	Strive for operational ease of use	2	2	3	3
18	Design an e-commerce system that is resilient in the face of expected threats	2	2	2	2
19	Isolate public access resources from mission critical resources	3	3	3	3
20	Prevent common errors	0	3	3	3

6. Discussion of the Results

The following section discuses the results depicted on table 3 and provide some of the issues which were uncovered during the heuristic evaluation.

6.1 Retail E-commerce Systems

Both EC 1 and EC 2 implement principle 1, while the systems perform tasks they also display their status to inform the user of what is happening. EC 1 shows inconsistencies it uses both “terms of use” and “terms and conditions” links to the same target, thus violating the usability principle 4. EC 1 in some cases violates the principle 2, since some of the terms that are confusing and uncommon terms for example to refer to the type of accommodation i.e. house, flat. EC 1 uses the term “Dwelling Type”.

In both systems, the principle 3 is partly implemented. EC 1 does not eliminate error prone conditions for example it accepts character in a field that requires numeric data (e.g. the telephone and credit card number fields) and does not inform the user immediately. EC 2 however, prevents this kind of error. If a number is entered instead of a character, the system immediately generates an appropriate and actionable error message. EC 1 partly implements the principle 7, whereas EC 2 implements it in full. Although both systems implement principle 7, principle 8 needs to be considered in both systems. EC 1 also partially implements principle 9 the error messages generated were not guiding the user to easily recover form the errors, the same applies for EC 2. Both systems implement principle 10.

In both cases the privacy and security policies are not shown directly and clearly on the registration form. The user has to click a link (“Terms and conditions” in EC 1 and “Our policy” in EC 2) to view them. Moreover, nothing is said about confidentiality, availability and integrity of the user’s information. This is not even to mention that neither system emphasises the use of strong passwords. We may therefore, have to assume that they are non-existent and therefore, that security is not an integral part of these systems.

None of the retail EC systems implements principle 11, but both mentioned that forgotten passwords can be sent to the user. The assumption is that the information is sent in clear text – thus not encrypted. It could not be ascertained whether both systems in fact implement principles 13 and 14. However, their privacy policies clearly state that they reserve the right to send the user information on offers and promotions of their organisation (this is spam put nicely). To a certain extent and without much conviction, we may conclude that both systems implement principle 15, because they work with at least two browsers (Mozilla and Internet explorer). The openness for the back-end could however not be ascertained. EC 1 violates principle 16, because instead of using “security”, “privacy policy” or “policy” in isolation, it uses “terms of use” and “terms and conditions”. EC 2 fares much better on this principle because reference is made to “our policy”. Both systems need to improve on principle 17 and, more especially, on principle 18, namely to reduce system down time. Principle 19 is implemented by both EC systems, since browsing the contents of the systems is separated from the shopping cart. As mentioned above, principle 20 is violated by EC 1 but it is implemented in EC 2.

6.2 Banking E-commerce System

EC 3 and EC 4 both implement the principles 1 and 2, as they inform the user of the status of the system while processing. Similar to what was found with regard to the retail sector; both of the banking EC systems do not implement principle 3. In fact, they dictate to the user what ought to be done. Both systems implement principle 4 regarding consistency and standards. Principle 5 should receive some more attention from EC 3 which partly implements it, as compared to EC 4 that implements it in full.

Principles 6, 7 and 8 are not implemented in EC 3 but they are implemented in EC 4. In the two-factor authentication, EC 3 compelled the user to memorise the password and also the sequence of the password characters, despite this not being memorable at all. EC 4 only requires the user to remember the password, otherwise a one-time password (OTP) is either sent to the user’s e-mail address or cell phone. EC 3 suffers from information overload. This is clear from the system's error messages, which cause it to violate principle 8. Both systems fully implement principle 9 and 10.

In both EC 3 and EC 4 security constitutes an integral part of their system design. This is reflected in the two-factor authentication and once again the strength of user passwords is not mentioned – probably for usability issues. EC 3 violates principle 12 because it does not protect the identity information of the user. Once the user logs in, access to this kind of information is guaranteed. In EC 4, on the other hand, the user is required to enter an OTP to access such information. Unlike EC 3, we can therefore conclude that EC 4 has taken an initiative to protect the user against identity theft.

Principles 13, 14, 15, 16, 17, 19 and 20 are all implemented in both systems of the banking sector. In the case of principle 18, we could not ascertain whether both the systems are resilient in the face of expected errors or threats. The next section concludes the paper.

7. Conclusion

From the above results we can deduce that e-commerce is still at its infancy stage in SA (as an emerging economy) and especially so in the retail sector. There are still a lot of security and usability issues that needs to be addressed in the retail sector to increase the acceptance and adoption of e-commerce systems. The banking sector appears to be at an advanced stage when considering both usability and security. Hence, we can conclude that the retail sector illustrates a case of less effective e-commerce implementation and the banking sector illustrates a case to a certain extent of effective implementation in the context of SA an emerging economy. Even though the banking sector seems to be on the right direction, the conclusion is that buying down town is still considered easier and safer than buying on line.

This work is mainly focused on the front-end and future work is still required to look at the back-end issues of security and usability of e-commerce system in both sectors.

8. References

Balfanz, D., Durfee, G., Ametters, D.K., & Grinter, R.E. (2004). In Search of Usable Security: Five Lessons from the Field*, IEEE Computer Society, IEEE Security and Privacy*.

Barnard, L., & Wesson, J. (2003). Usability Issues of E-commerce in South Africa: An Empirical Investigation, *The Proceedings of SAICSIT 2003*, ACM, pp. 258 - 267.

Bias, R.G., & Mayhew, D.J. (2005). *Cost-Justifying Usability: An update for the Internet Age.* USA. Elsevier.

Camp, L.J. (2007). Security and Usability*, IEEE Technology and Society Magazine*, Spring 2007, pp. 23 - 24.

Cronar, L.F. (2008). A Framework for Reasoning About the Human in the Loop, *Symposium On Usable Privacy & Security (SOUPS 2008),* July 23 – 25, 2008, Pittsburgh, PA, USA

Dourish, P., & Redmiles, D. (2002). An Approach to Usable Security Based on Event Monitoring and Visualization, *Proceedings of the New Security Paradigms Workshop 2002.* Virginia Beach, VA.

Falk, L., Prakash, A., & Borders, K. (2008). Analysing Websites for User-Visible Design Flaws, *Symposium On Usable Privacy & Security (SOUPS 2008),* July 23 – 25, 2008, Pittsburgh, PA, USA.

Furnell, S. (2007). Making Security Usable*, Computers & Security,* Vol. 26, pp 434 - 443.

Gedda, R. (2006). Security vs Usability: No one's Winning*, ComputerWorld Australia*, available at www.computerworld.com/news/index.jsp, visited 07 March 2008.

Gutmann, P., & Grigg, I. (2005). Security Usability*, IEEE Security and Privacy,* Vol. 3, Issue No.4, pp. 56 - 58.

Hafiz, M.D., Abdullah, A.H., Ithnin, N., & Mammi, H.K. (2008). Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique, *IEEE Computer Society, 2nd Asia International Conference on Modelling & Simulation,* pp 396 – 403.

Hugo, J. (2002). *HCI and Multiculturalism in Southern Africa*, CHI2002 Development Consortium.

ICT World, (2007). Online Christmas Shopping up by 800% in Two Years, *ICT World Magazine,* [Online], January 22, available at http://www.ictworld.co.za/EditorialEdit.asp?EditorialID=27991, visited 05 March 2007.

Information Systems Security Association (2004). *Generally Accepted Information Security Principles version 3.0 (GAISP V.3),* available at http://all.net/books/standards/GAISP-v30.pdf, visited 19 April 2008.

ISO 9241-11 (1998). *Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs) - Part 11: Guidance on Usability*, International Organization for Standardization, Geneva.

Johnston, J., Eloff, J.H.P. and Labuschagne, L. (2003). *Security and Human Computer Interfaces,* Computers & Security, Vol. 22, Issue No. 8, pp. 675 - 684.

Lauesen, S. (2005). *User Interface Design: A Software Engineering Perspective,* UK. Addison Wesley.

Macagnano, E.V., & Greeff, M. (2007). Universal Design for HCI in a developmental context: myth or reality? The South African example, *HCI International 2007*, Beijing, China, 22-27 July 2007, p. 6.

McLaren, C.H., & McLaren, B.J. (2000). *E-commerce: Business on the Internet.* Cincinnati: South-Western Educational Publishing.

Morris, R., & Thompson, K. (1979). Password security: a case history, *Communications of the ACM*, 22(11), 594-597.

Nielsen, J. (1993). *Usability Engineering,* Orlando, Florida: Academic Press.

Neilsen, J., & Norman, D.A. (2000). *Web-Site Usability: Usability On The Web Isn't A Luxury,* available at http://www.informationweek.com/773/web.htm, visited 15 April 2008.

Norman, D. (1990). *The design of everyday things*. Doubleday, New York.

Payne, B.D., & Edwards, W.K. (2008). A Brief Introduction to Usable Security, *IEEE Computer Society,* Vol.12, Issue No.3, pp 13 -21.

Reeder, R.W., & Arshad, F. (2005). *Conference Reports, SOUPS 2005*, Carnegie Mellon University, IEEE Security and Privacy, pp 47 - 50.

Rozinov, K. (2004). *Are Usability and Security Two Opposite Directions in Computer Systems*? available at http://rozinov.sfs.poly.edu/papers/security_vs_usability.pdf, visited 4 April 2008.

Schaaper, M. (2008). Measuring Security and Trust in the Online Environment: A View Using Official Data, Directorate for Science, Technology and Industry (DSTI), Committee for Information, Computer and Communications Policy (ICCP). Working party on Indicators for the Information Society (IIS), DSTI/ICCP/ISS (2007) 4/Final, Organisation for Economic Co-operation and Development (OECD), available at: www.oecd.org/dataoecd/47/18/40009578.pdf, visited 15 April 2008.

Schaffer, E., & Sorflaten, J. (1999). Web usability illustrated: breathing easier with your usable E-Commerce site, *Journal of Economic Commerce*, Vol. 11, Issue 4.

Shneiderman, B. (1998). *Designing the User Interface: Strategies for Effective Human-Computer Interaction*, Third Edition, Addison Wesley, Reading, MA.

Smith, S.W. (2003). Humans in the Loop: Human-Computer Interaction and Security*, IEEE Computer Society, IEEE Security and Privacy*, pp 75 - 79.

Stoneburner, G., Hayden, C. & Feringa, A. (2004). Engineering Principles for Information Technology Security (A Baseline for Achieving Security), National Institute of Standards and Technology, available at http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf, visited 4 April 2008.

Vatanasombut, B., Stylianou, A.C., & Igbaria, M. (2004). How to Retain Online Customers*, The Communications of the ACM,* Vol. 47, Issue No. 6, pp. 64 - 69.

Wesson, J. (2000). The Role of HCI Design Patterns in Software Development in South Africa. *CHI-SA'2000*, 8-10 May 2000, University of Pretoria, South Africa.

Whitten, A. (2004). *Making Security Usable,* Ph.D. thesis, School of Computer Science, Carnegie Mellon University.

Whitten, A., & Tygar, J.D. (1999). “Why Johnny can’t encrypt: a usability evaluation of PGP 5.0”, *Proceedings of the 8th USENIX Security Symposium*, USENIX, Berkeley, CA.

Yee, K. (2002). User Interaction Design for Secure Systems*, Proceedings of the 4th International Conference*, ICICS 2002.

Yee, K. (2004). Aligning Security and Usability*, IEEE Computer Society, Security and Privacy*, pp. 48 - 55.

Zurko, M.E., & Simon, R.T. (1997). User-Centered Security*, New Security Paradigm Workshop*, ACM, pp. 27 - 33.