BEHAVIOUR & INFORMATION TECHNOLOGY, 2017
VOL. 36, NO. 5, 493–516
http://dx.doi.org/10.1080/0144929X.2016.1262897

Taylor & Francis
Taylor & Francis Group

Trading off usability and security in user interface design through mental models

Mona A. Mohamed[a], Joyram Chakraborty[b] and Josh Dehlinger[b]

[a]Department of eBusiness and Technology Management, Towson University, Towson, MD, USA; [b]Department of Computer and Information Sciences, Towson University, Towson, MD, USA

ABSTRACT

The aim of this paper is to establish the foundations for developing a mental model that bridges the gap between usability and security in user-centred designs. To this purpose, a meta-model has been developed to align design features with the users' requirements through *tacit knowledge* elicitation. The meta-model describes the combinatorial relationships of Security, Usability and Mental (SUM) and how these components can be used to design a usable and secure system. The SUM meta-model led to the conclusion that there is no antagonism between usability and security. However, the degree of usable security depends on the ability of the designer to capture and implement the user's tacit knowledge. In fact, the SUM meta-model seeks the dilution of the trading-off effects between security and usability through compensating synergism of the tacit knowledge. A usability security *cognitive map* has been developed for the major constituents of usability and security to clarify the interactions and their influences on the meta-model stipulations. The three intersecting areas of the three components' relationships are manipulated to expand the *Optimal Equilibrium Solution* (OES) (δ) expanse. To put the SUM meta-model into practice, knowledge management principles have been proposed for implementing user-centred security and user-centred design. This is accomplished by using collaborative brainpower from various knowledge constellations to design a system within the user's current and future perception boundaries. Therefore, different knowledge groups, processes, techniques, tactics and practices have been proposed for knowledge transfer and transformation during the mental model development.

ARTICLE HISTORY
Received 26 October 2015
Accepted 16 November 2016

KEYWORDS
Usability; security; tacit knowledge; synergism; mental model; knowledge management

1. Introduction

Presently, there is no universal formula for minimising the apparent paradox between usability and security. Therefore, software designers and security architects (SAs) continue to face the dilemma of these two seemingly conflicting goals in developing a system that is both usable and secure. This entails making the system easy to use and efficient for the users to accomplish their tasks, while at the same time making it difficult for the intruders to compromise. The relationship between usability design and security architecture, as manoeuvred by the mental model of the user and the designer, is vital for building usable and secure systems. However, the main challenge remains in how to elicit the users' tacit knowledge and translate it into the interface design without compromising system security or underestimating system usability.

Striking the balance between usability and security through narrowing the gap between mental models is critical for minimising the effects of their trade-off. However, most of the research to date has been dealing with each area of Security, Usability and Mental (SUM) models separately. The literature on the interaction between usability and security has recently shown only moderate growth as reported by Jøsang et al. (2007), Talhi et al. (2002), González et al. (2009), Mihajlov, Blažič, and Josimovski (2011), Ben-Asher et al. (2009), Mihajlov, Josimovski, and Jerman-Blazič (2011), Flechais, Mascolo, and Sasse (2007), Schultz et al. (2001), Schreuders, McGill, and Payne (2012) and Bo et al. (2014).

Indeed, the importance of usability in security rests in the fact that most of security functionality and controls are embedded in the user interface (UI) and a good interface design results in more effective security functionality (DeWitt and Kuljis 2006; Rukšènas, Curzon, and Blandford 2008; Yee 2002). There has been a considerable amount of research on the effects of mental models on usability parameters, as documented in the works of Graham, Zheng, and Gonzalez (2006), McDougall, Curry, and de Bruijn (2001), Lei, Yang, and Zhang (2006), Law, Blazic, and Pipan (2007) and Langan-Fox, Platania-Phung, and Waycott (2006). Surprisingly, little attention has been devoted to topics that combine security and mental models (Bravo-Lillo et al. 2011; Camp

CONTACT Mona A. Mohamed mmohamed@towson.edu

2009; Forget et al. 2008; Ka-Ping 2004). Yet, the research that interrelates the effects between all three domains remains sparse.

So far, most of the research conducted is limited to specific parts of the relationship between usability and mental model. McDougall, Curry, and de Bruijn (2001) examined the role of content of graphical user interfaces (GUIs) on the user's knowledge structure. The authors found that users' knowledge structures rely on the nature of the graphical information presented through the interface, but does not depend on the use of the visual metaphor. In a detailed study Olaverri-Monreal and Goncalves (2014) mapped the user's mental model and expectations to a UI design with no security involved. However, Nielsen (1989) observed that users view usability from various features of the system as they may not do things the way designers feel they ought to do them. Drawing on a review of literature concerning mental models, significant inconsistencies between the user and the designer's mental models were observed by Langan-Fox, Platania-Phung, and Waycott (2006) and Gillan et al. (1995), while Bravo-Lillo et al. (2011) limited the use of mental models to design security warnings. On the contrary, Camp (2009) and Raja et al. (2011) found no evidence of using mental models in security research; while previous work by Forget et al. (2008) attributed that to the complexity of security systems. All these variations are related to the intrinsic differences between the user and the designer's personal mastery levels as described by Senge (1990), Gillan et al. (1995) and Wells and Fuerst (2000).

Human-computer interaction (HCI) concepts have been applied to significantly improve information security posture. Based on earlier works of Sasse, Brostoff, and Weirich (2001), Peltier (2006), Lineberry (2007), Schultz et al. (2001), Tri and Dang (2009), Tam, Glassmana, and Vandenwauverb (2010), Schreuders, McGill, and Payne (2012) and Bulgurcu, Cavusoglu, and Benbasat (2010), this paper hypothesises that the user is the weakest link in the information security chain. Furthermore, Jøsang et al. (2000) it considers usability itself to be the weakest link in the security chain in many enterprise applications. Consequently, the user's acceptance of any information system security feature largely depends on the degree of usability of the system (Crespo 2013; Dinev and Hu 2007). This acceptance depends on many intermingling factors. For instance, Jonas and Norman (2011) found that a student's acceptance of technology in a voluntary usage behaviour is governed by the modified and extended Technology Acceptance Model (TAM2) with factors such as perceptions of usefulness and the ability to explain the benefits of the system. Further, Van Schaik et al. (2004) used the original TAM framework to evaluate the acceptance of the decision-support system and concluded that besides the TAM factors, disadvantages or cost of the system play a significant role in system acceptance. However, Zhang and Xu (2011) enhanced TAM with mental models building in maintenance features to understand how users cognitively accept replacement systems.

This multidimensional relationship necessitates a thoughtful exploration of the user's mental model development and the user's potential engagement in the system design process. Accordingly, this paper attempts to build a holistic SUM meta-model and to put the model into practice by applying knowledge nurturing, mobilisation and sharing concepts in meta-model development.

The remainder of this paper consists of and discusses four main sections, namely, the meta-model components, the meta-model construct, the implementation of the meta-model, mental model acquisition and finally concludes with a bottom line statement.

2. The model components

2.1. Components' definition

Usability rules have been defined in different standards using different software quality characteristics that affect the user's interaction with systems. ISO (1998) defined 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'. Likewise, Theofanos (2007) reported that ISO 13407 defines stages of user-centred design as an activity in an iterative process of the requirements specification. The same is emphasised by its successor, ISO 9241-210:2010. It is described by Santos and Boticario (2015) that ISO 9241-210:2010 offers the directions on human-centred design steps throughout the life cycle of four iterative activities, namely: (1) understanding and specifying the context of use; (2) specifying the user requirements; (3) producing design solutions to meet user requirements and (4) evaluating designs. Furthermore, the software life cycle processes and requirements of medical device software development is defined in IEC 62304 (ISO/IEC 2006), while the description of the UI features is detailed in ISO/IEC 9126-1 (Theofanos 2007). However, Kahraman and Bilgen (2015) noted that the 25010:2011 standard revised ISO/IEC 9126:2001 and introduced a multilevel hierarchy model for the quality of software systems with well-defined quality characteristics of software products. Nevertheless, Nielsen (1990) cautioned that applying the interface design rules for consistency could not be the only consideration where the user and task differences

are of extreme importance to the design. This is confirmed by Thovtrup and Nielsen (1991) who observed that UI standards and formal specifications can be difficult for the developers to apply and are likely to be violated. In fact, the authors believe to have found that standards restrict the creativity of the system designers. But, they considered this behaviour necessary as long as the developer provides explanation for such deviations.

The final appraisal of usability is solely at the mercy of the user. Generally, this appraisal depends on the most popular characteristics of usability listed in the literature, namely, efficiency, effectiveness, user satisfaction, learnability and memorability (Bevan 2001; Bushma 2010; Doddrell 1995; Hashim and Sultan 2009; Ma, Johnston, and Pearson 2008; Wilke et al. 2007; Yeratziotis, Pottas, and Greunen 2012). As a matter of fact, three of these characteristics of usability are well represented in ISO 9241-11, which focuses on 'learnability' (Khelifi and Suryn 2003). Nielsen and Phillips (1993) stated that 'learnability is more important for the success of many user interfaces'. Ziefle (2002) reports that 'learnability is concerned with features of the man-machine interaction that allow users to understand easily how to handle a specific device and how to improve the performance level quickly'.

Information security, on the other hand, has been defined by many institutions as being based on many traits, such as functionality, properties, policy, etc. Davidson, McCredie, and Vikelis (1994), who authored the *IBM Dictionary of Computing*, defined security as: 'The concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or advertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use'. Nevertheless, information security aims to satisfy the principles of Availability, Integrity and Confidentiality (AIC) (Costas 2000; Fitzgerald 1995; Hyun, Wang, and Ullrich 2012; Khansa and Liginlal 2009; Ma, Johnston, and Pearson 2008; Mitrakas 2006; Skovira 2007). Joshi et al. (2001) state that the goal of confidentiality is to ensure that information access is restricted to authorised personnel only, while the intent of integrity is to protect information from unauthorised modifications. Further, the aim of availability is to make the information available when needed by legitimate users. Vance, Lowry, and Eggett (2013), Ma, Johnston, and Pearson (2008), Mylonakis and Malioukis (2010), White (2010) and Joshi et al. (2001) added the accountability principle, which ensures that every action can be tracked back to its origin. Moreover, Ting and Comings (2010), Chan and Kwok (2001), Liddy and Sturgeon (1999), Ma, Johnston, and Pearson (2008) and Walle et al. (2004) put emphasis on assurance as a security principle, which it reflects the degree of confidence in the system security.

The usability model developed in this research is in harmony with the description of Winter, Wagner, and Deissenboeck (2008) in which the usability model is characterised as a 'central knowledge base for usability-related relationships in the product and process. It documents, in a structured manner, how the properties of the system, team and organization influence different usage activities'. In an attempt to improve the ISO usability model. Hashim and Sultan (2009) and Khelifi and Suryn (2003) defined the usability model which includes security, in addition to effectiveness, efficiency, learnability and satisfaction. Moraga et al. (2007) developed a comprehensive usability model for portlets with different attributes based on the ISO/IEC 9126, quality models and web applications. The authors found the results to be confining in scope as they can only be applied to specific portlets. In general, a security model is a formal representation of security requirements and specifications that provide the desired protection of an organisation's information system. There are many security models adopted by different organisations such as access control matrix, Brewer and Nash, information flow, lattice, state machine, etc. However, as stated by Wang (2005) there is no one security model that fits all. Nevertheless, Kwok (1997) recommended that information security models should be prepared with a macro-level view of the risk within the current security situation of the organisation. Hence, the model must look at all aspects of the information-processing environment, including the system, users and the information.

The relationship amongst the SUM meta-model components is very complex. The following three sub-sections explain the aspects of this relationship.

2.2. Mental model

The mental models of the user and the designer are of great significance to their decisions and their interactions with any UI and/or security control. More often, the mental model is a result of the internalisation of tacit knowledge that affects the user's rationale about how the system works. However, Wilke et al. (2007) observed that the user's mental model may not be consistent with the system's conceptual model because of many exogenous factors that lead to the formation of the users' mental model. Factors may include previous experience with the system, experience using other similar systems, information obtained from system publications and knowledge of how the system technology works. Mental models allow individuals to make predictions about the

outcomes of their actions in real life, including when the individual makes security decisions (Zhang-Kennedy, Chiasson, and Biddle 2013). Based on the Mental Model Theory (MMT), Van der Henst (2002) and Zhang and Xu (2011) attribute human reasoning to the building, maintenance and manipulation of the mental model. The same logic was pursued by Zhang-Kennedy, Chiasson, and Biddle (2013) who described the mental model as 'a simplified internal concept of how something works in reality'. Therefore, people depend on the reasoning of their mental models to predict outcomes in real life. Equally, Senge (1990) clearly characterised the mental model as 'deeply held internal images of how the world works'. More specifically, Uther and Haley (2008) defined the mental model as 'a cognitive representation of a situation or system that constitutes the users understanding of that situation or system'. In more detail, David (2000) described the mental model as 'a schema (knowledge structures) plus cognitive processes (mental operations) for manipulating and modifying the knowledge stored in a schema'. The author differentiates between knowledge structure and the mental model, whereby the former is a form of schema the learners use to represent knowledge in memory, and the latter is the schema plus cognitive processes for manipulating and transforming knowledge that is contained in that schema. With regard to mental model development, Zhang-Kennedy, Chiasson, and Biddle (2013) recognised only two types of mental models, namely, complementary mental models which consist of knowledge structures related to team creative processes and held by team members with specific roles (focus group); and Shared Mental Models (SMMs) represented by a knowledge structure possessed by team members that contains analogous content. Xiang, Lu, and Gupta (2013) pointedly defined SMM as 'a common thinking style developed when individuals perform similar tasks in a cohesive manner'. The authors found that SMM was highly related to knowledge sharing and team performance.

With respect to HCI, Rook and Donnell (1993) empirically evaluated agents that drive user/expert system interaction and found that good mental models lead to increased user/computer interaction and optimal performance. Ruggles (1998) claimed that 'The mental model is the root of usability of user interfaces'. More pointedly, Westerink, Majoor, and Rama (2000) and Uther and Haley (2008) found that navigation behaviour depends on the user's mental model experience and previous navigation paths. On the other hand, Stibel (2005) stated that incorrect mental models can lead to fateful outcomes. This observation corresponds with the proposal of Kim, Sekiyama, and Fukuda (2009) for an information retrieval method based on mental models, which eventually reduces the navigation paths in the system. To align the interface design with the mental model, Vicente (1990) distinguished between two categories of work domains, namely, correspondence and coherence-driven work which are used in making the interface representation compatible with the user's mental models. Olaverri-Monreal and Goncalves (2014) report that user-centred design entails the knowledge of the future user's requirements trends during the design phase. Therefore, Damondaran (1998) recommended close communications between the user and the designer to accurately identify the 'desired future state'. The consideration of the user's mental model in the design phase is crucial to the ultimate success of the system. Hence, the user's mental and conceptual models should line up to yield a UI that is consistent with the user's expectations, and with representation of how the system should function. In fact, the symmetry between the conceptual and mental models smooth out the operations in a predictable manner and promotes mastering of the functionality that leads to user satisfaction. However, Raja et al. (2011) noted that experts' mental models, as expressed in the conceptual model, are not good representative models for typical users.

2.3. Coupling of security and usability

The most widely known and earliest published research in the area of security usability has been conducted by Saltzer and Schroeder (1975). The authors investigated the dynamics of how protection systems handle security controls at all levels of functional capability and found that the human interface must be designed in a way that the user can intuitively or routinely protect the system with no difficulty. In many overly protected systems, users see security mechanisms as roadblocks (Aldridge, White, and Forcht 1997; Grobauer, Walloschek, and Stöcker 2011; Zurko 2005). In fact, the actual focus of usability is described by ISO 9241-11 where the product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use. On the other hand, the emphasis on information security is to provide AIC.

The characteristics of an appropriate security interface have been an intriguing subject of research. Yee (2002) describes the design principles of the security interface that lead to expressiveness, clarity, visibility, least resistance and trusted path. More importantly, this interface must be in agreement with the user's mental image of the protection goals. The design of the interface is critical for the proper implementation of security controls. In many cases, the design of the interface is a

determining factor in security controls effectiveness. For example, Bravo-Lillo et al. (2011) found that users 'had very inaccurate mental models of phishing', because of their lack of understanding of how emails spoofed websites. The authors attributed this misconception to the poor design of the warning dialogs that neither carry an explanation of the risk, nor contain information about how the user can avoid the risk. Likewise, Li et al. (2014) found that blacklist-based and whitelist-based anti-phishing toolbars in phishing-detection applications caused no significant performance difference among users in detecting phishing attempts and potentially harmful pages. But, the authors observed the lack of information explaining security certificates in the sites tested. On the other hand, Imgraben, Engelbrecht, and Choo (2014) and Jansson and von Solms (2013) claimed that training contributes to users' phishing resistance, because it minimises the probability of users becoming a victim to any future phishing attempts. To comprehensively address these multifaceted problems, Cranor (2008) proposed a framework, called human-in-the-loop security, for systems designers and system operators to secure systems design problems and analyse the root cause of security failures that have been attributed to 'human error'.

In minimalist designs, the UI is intuitive and easy to learn. Yet, this ease of use can also provide an opportunity for an attacker to compromise that system. Conversely, high usability should reduce the likelihood of insiders committing inadvertent errors or intended attacks to compromise data. A well-designed UI should minimise the memorability errors of security authentication and authorisation and, consequently, information security controls. The implementation of information security controls should not limit authenticated users from performing their duties. Nevertheless, security controls may cause unwarranted inconvenience to the user. Therefore, it has been stated by many investigators that factors affecting usability and security mechanisms are antagonistic (Braz, Seffah, and M'Raihi 2007; González et al. 2009; Ka-Ping 2004; Lei, Yang, and Zhang 2006; Potter 2012; Sahar 2013).

Many solutions for minimising the effects of conflicts between usability and security goals have been proposed. Potter (2012) claimed that the conflicts between security and usability goals can be avoided by dealing with goals conjointly through an iterative process of the design. However, Ka-Ping (2004) stated that the conflict between security and usability can be avoided through different approaches of security management such as including both goals in the design phase and maintaining agreement between the system's security state and the user's mental model.

Yet, other investigators contested the conflict argument in the first place and considered it as being no more than erroneous conceptions. For instance, Khelifi and Suryn (2003) considered security as one of many usability model characteristics.

Indeed, some security functionality will not exist without acceptable usability. For instance, availability, as one of the security principles, will be incomplete without accessibility to the application. Braz, Seffah, and M'Raihi (2007) report that there is a common mistaken belief that security is associated with software functionality and not with software usability. This opinion is noticeable in a vast number of authentication and authorisation mechanisms. For instance, without attentive usability the HCI proof of CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) in the websites will be utterly dysfunctional. By definition, CAPTCHA is a simple challenge-response verification using optical characters' recognition to grant more confidence that the authentication credentials are provided by humans and not by automated software. More interestingly, Olalere et al. (2014) and Banday and Shah (2009) used the SoundsRight Audio to add usable and secure audio CAPTCHA for visually impaired people with background noise instead of text.

Paivio (1991) developed a theory on the influence of graphic aids in the development of mental models as they are often constructed from metaphors. Similarly, Raja et al. (2011) found that metaphors of physical security are appropriate for risk communication to users in computer security. Therefore, metaphoric representation in the form of CAPTCHAs should have positive effects on the user understanding the technique. However, in many cases CAPTCHA has no meaningful metaphorical references that help the user's understanding of its intention. Accordingly, it provides a GUI-based challenge where the user provides a username and password combination plus the optical characters. In fact, CAPTCHA, which is founded on securing a system using the Human-Interaction Proof (HIP) technique, is designed to exclude automated software or script attacks from computer robots (bots). Reza, Beheshti, and Liatsis (2015) report that one of the most important challenges of CAPTCHA is to design it in a way that makes it difficult for the computer to break its test, but fairly easy for the human to solve it. In general, CAPTCHA is annoying to many users either due to its ill-defined GUI, distorted wavelike characters or due to the fact that it does not make sense to the user to perform such a challenging task just to access the system. Nonetheless, if the user clearly understands its components and the rationale behind it, she might be less disturbed by the technique.

Ahn et al. (2008) concluded that 'although CAPTCHAs are effective at preventing large scale abuse of online services, the mental effort each person spends solving them is otherwise wasted'. Banday and Shah (2009) added that adaptive CAPTCHA has been exploited by dictionary and brute-force attacks. Accordingly, the authors introduced special type of CAPTCHA called reCAPTCHA, which is used by Google, Facebook, YouTube, LinkedIn and Twitter. The displayed challenge in reCAPTCHA is a word copied from very old printed books that are not previously digitised. The words are photographically scanned in bitmap images, then transformed into text files for indexing and searching by Optical Character Recognition (OCR). The authors proved that these texts cannot be deciphered by programs, but can easily be read by human with 99% accuracy. In fact, Reza, Beheshti, and Liatsis (2015) claimed that it is almost impossible for the computer to solve it, while Hsieh and Wu (2013) reported that it is just too difficult for the computer to answer the reCAPTCHA challenge. Nevertheless, Gao et al. (2016) claimed that they were able to launch a successful attack on text reCAPTCHA. The original reCAPTCHA design has been modified to fit various purposes. For instance, Kiziloz and Bicakci (2015) designed an effective audio reCAPTCHA to be easily used by visually impaired users, but difficult for bots. Furthermore, Hillena and Höfleb (2015) enhanced reCAPTCHA to adapt it to geographic information domains. However, Abubaker et al. (2015) presented a cloud-based design and architecture for an Arabic reCAPTCHA. More advances have recently been reported on reCAPTCHA. Sivakorn, Polakis, and Keromytis (2016) stated that the 'no CAPTCHA reCAPTCHA' introduced by Google uses advanced risk analysis procedures which depend on the confidence scores that reflect the confidence of the system. Users with high confidence scores are only required to click a checkbox. This allows user verification without providing difficult challenge and with a simple user-friendly interface. Abubaker et al. (2015) gave an example of no CAPTCHA reCAPTCHA as checking a box next to the statement: 'I'm not a robot'.

The authentication process is a rich subject of study where the UI can align with and improve the security posture, when used in accordance with usability principles. The authentication in its entirety consists of two steps: (1) identification, where the active subject (user or process) or passive subject (system) claims a particular identity; and, (2) if approved by the system, then authorisation is granted to access the object, that is, file or folder. This same idea was expressed earlier by Saltzer and Schroeder (1975) who differentiated between the two access steps and simply stated the very first rule in the relationship between security and UI as 'most real systems contain both kinds of sharing implementations – a list-oriented system at the human interface and a ticket-oriented system in the underlying hardware implementation'.

Similarly, Whitten and Tygar (2003) introduced a technique of safe staging based on conventional UI staging to satisfy computer security requirements in software design. The authors claimed that while the technique provides continuous protection, it minimises the complexity of security concepts for users. The design of the UI for access controls such as password protection must be expressive and intuitive to the user; however, the security functionalities associated with the password must be kept in mind. These functionalities may be facilitated by password policy such as password masking. This is important in protecting user Personal Identification Information (PII) data such as a Social Security Number (SSN). In most cases, SSN is concealed by substituting the numbers with stars for privacy, or masking data to be revealed only when a certain code is entered.

The effectiveness of security measures, in many cases, depends on the efficacy of the UI. Zhang-Kennedy, Chiasson, and Biddle (2013) found that visual aids and metaphorical references such as keys, locks and walls icons used in security software always help alleviate the problem for novice home-users. To make use of such association, the development of the security interfaces must follow user-centred design approaches, which, ultimately, lessen the effects of conflicting requirements of software usability and information security on the UI. This combined approach for understanding both security and usability at early stages of system development is necessary. Hence, it is crucial that usability designers must thoughtfully envision the usability specifications and security functionality with the involvement of the SA. Ironically, the communications between the software designers and information security professionals is always postponed until the later stages of the system development life cycle (SDLC) (Ka-Ping 2004).

In general, security specifications are used in the SDLC at two phases: product design and detailed design. However, DeWitt and Kuljis (2006) recommend the inclusion of security and usability at the beginning of the design. Yet, this may introduce impediments that originate from the SA with poor usability experiences as summarised by Houmb et al. (2010) who stated the main challenges are brought about by poor information security expertise in development teams and a shortfall of current techniques to assist developers with security expertise. In actuality, developers think about fulfilling functional requirements and satisfying users' expectations, before they think about any security

specifications during the SDLC. On the contrary, the security professional's objective is to protect the system from unauthorised access, with minimal or no consideration of system usability.

In an investigation about the relationship between mental models and inference, Rook and Donnell (1993) concluded that graphical interfaces would result in a higher performance than textual explanations. Graphical interfaces can play an important role in authentication with both forms and factors, that is, factors that the 'user knows' (password) and factors that the 'user is' (biometrics). By using the Theory of Planned Behaviour (TPB) as a reference framework, Seyal and Turner (2013) suggested that 'people attitudes towards biometrics is a predictor of behavioral intention, whereas, subjective norms are predictors of attitude, perceived behavioral control, behavioral intention and behavior'. With biometric access control systems, the UI is critical in understanding what is needed from the user to avoid the system falsely rejecting the authentication process (Type I error), or falsely accepting unauthorised users (Type II error).

2.4. Mental model of usability and security

The main challenge in designing usable security is to cautiously strike a balance between protecting the system from unauthorised disclosure and cognitively design the system to conform to the user's expectations and satisfaction. Achieving such balance is not a trivial task. Saltzer and Schroeder (1975) observed that most modern systems are characterised by complex security interfaces to the extent that the user faces a problem of identifying the security requirements. Therefore, the authors recommended that the UI closely match the users' mental models for ensuring a safe behaviour. Otherwise, poor usability may result in low productivity and/or compels the users to circumvent security controls. Rukšènas, Curzon, and Blandford (2008) developed a framework to identify confidentiality leaks because of inappropriate design and to determine designs that are prone to attacks due to mental aptitude of the intruders. Additionally, the authors concluded that users breach security due to mismatches between the computer system and the users' mental model settings. For this match to materialise, the authors proposed the implementation of a user-centred security, which provides a security model with software usability as the primary goal.

The consideration of mental models in UI can play a major role in minimising risks and improving the manipulation of embedded controls and unforeseen security practices of novice users. Camp (2009) investigated the role of mental models on security and privacy and found one critical method of risk communication was to utilise the existence of human risk heuristics and communicate the intended information using a simple mental model of risk. Despite its importance in reducing risks, the author found that there is no evidence of using mental models in security research and literature. This is in an agreement with Raja et al. (2011) who stated that the mental model approach has been effectively applied in many areas such medical, environmental and risk communications, but not in information system development for secure systems.

Generally, mental models can be employed in system design to mitigate risks. For instance, the mental model's effect on embedded controls and implicit security mechanisms can be seen in security practices such as steganography and various attacks such as data aggregation and Trojan horses. Steganography is an object-oriented solution where one object encapsulates another to hide its details. The data aggregation, on the other hand, is a process of stitching low-sensitivity datasets to yield high-sensitivity datasets. Karat, Brondie, and Karat (2006) noted that in isolation, a single data item might not identify a person, but through data aggregation, the PII may be disclosed. Therefore, GUIs should be designed in ways which discourage aggregation attempts that lead to easy inference.

Users behave according to their mental models, which can be reflected in a design of a *cognitive map*. The cognitive map is a graphical representation of entity schemata in real life. Spicer (1998) studied the effects of mental models and the cognitive mapping on organisational learning which describes the cognitive map as a unique technique in which an individual views a particular domain. In general, the closer the illustration to reality in the design and security requirements, the higher the security and usability of the system will be. Moody, Blanton, and Augustine (1996) state that the conforming mental model of a system is based on whether the conceptual model, one which captures the basic synopsis of the components that constitutes the system, or the procedural model, one that outlines the 'how to' commands, was utilised during the design. The ability to understand the user's mental model will help in designing specific products. Olaverri-Monreal and Goncalves (2014) state that mapping between the user's mental model and the product's conceptual model guarantees a smooth operation across the design which eventually leads to user satisfaction. In fact, Nielsen and Levy (1994) found that there is strong positive correlation between users' task performance and their subjective satisfaction.

Warning interface design is critical for systems to draw attention to system vulnerabilities. In fact, Molich

and Nielsen (1990) advise that systems should always keep the user informed in a reasonable time. Bravo-Lillo et al. (2011) examined the implementation of a mental model approach to bridge the gaps in computer security warnings. The authors used mental models to highlight effective ways to convey security information to the average user and to improve warning interface design in several ways. This improvement in the design of complete dialogs is important for communication with the user. Cranor (2008) stated that system designers may easily overlook the failure of communications delivery through incomplete dialogs and considered it as an underlying cause of human security failure. Conceptually, information security controls must have insignificant influence on the ability of authorised users to interface with the system to perform their duties. However, obstructive UI may be an alluring ticket for the user to bypass security controls. In an attempt to determine the difficulties of designing privacy through understanding and action, Lederer et al. (2004) defined five pitfalls of design; among them is the design of the UI to inhibit people's ability to understand privacy implications and to conduct meaningful actions on them.

The UIs can facilitate various security functionalities that stretch from visible icons to indecipherable password dialogs. Schultz et al. (2001) suggest that usability of security should address two important goals: (1) increase the willingness of the user to use the method and (2) ensure the user can use it with ease, in less time, with fewer errors and higher satisfaction. Interfaces should be self-evident and intuitive; otherwise, violations and incidents may occur from the users themselves. However, users should not be blamed for security violations that result from poor usability, which exhibits discrepancies between the user's mental model and the UI. Vance and Paik (2005) suggest that the UI can be used to make users feel more accountable for their actions and less likely to misuse their access rights.

3. The meta-model construct

The meta-model construct demonstrates the potential consequence of relationships and interactions of SUM components. This meta-model, as depicted in Figure 1 (a,b), presumes that the proportionality of each of the three domains is expressed by the size of the optimal intersection areas between them and it is a reflection of the degree of security and a level of usability as shaped by the effectual mental models. The intersection areas are represented in Figure 1(a,b) as α, β, γ and their convergence is shown as δ. In general, the expanse of this area is elastic and determined by the continually changing business requirements and the resiliency of the infrastructure. Then, the effectiveness of both the usability design and the security architecture is governed by the homogeneity of the designer and the user's mental model. It is unlikely to achieve a perfect congruency between the mental model of the user and that of the designer. This is due to the inherited inconsistency between the usability designer and the user's mental models as described by Langan-Fox, Platania-Phung, and Waycott (2006) and Gillan et al. (1995). The meta-model with its three major domains at the user and designer's level is shown in Figure 1(a,b), respectively. Further clarification of the meta-model relationships and intersection areas are shown in Tables 1 and 2 and Figure 2.

Aside from the intersection areas depicted in Figure 1 (a,b) and explained in Tables 1 and 2 there are other composite conditions that arise as a result of the relationships within δ and γ that merit additional clarification. These relationships are described next.

The interaction between individual elements of security and usability is shown in Figure 2 and detailed in Table 2.

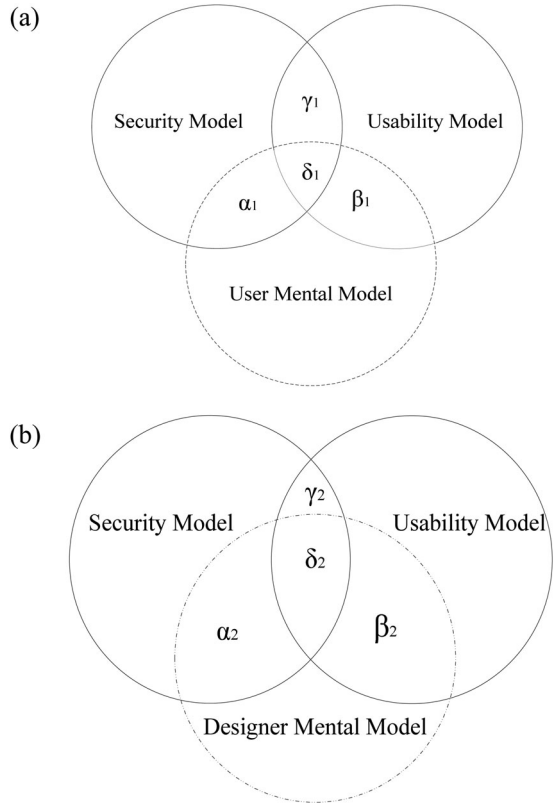

Figure 1. (a) The conceptual representation of the relationships between the meta-model domains, that is, usability, security and the user's mental model's intersection areas. (b) The conceptual representation and relationships between the meta-model domains, that is, usability, security and the usability designer's mental model intersection areas.

Table 1. The description of the intersection and the convergence areas between the usability, security and mental models.

Intersection area	System characteristics	Interaction semantics
α	*Low* α: Secured, but not understandable or cognisable *High* α: Secured and understandable	Measures how well the security model is within the realm of the designer/user mental models, along with the understandability of the security system purpose and function
β	*Low* β: Usable, but not understood *High* β: Usable and well understood	Measures the degree to which the system behaviour is in agreement with the designer/user's mental models, along with the understandability of the system and why it behaves in certain ways
γ	Low γ: Usable and secured, but operates as two separate functions with minimal effectiveness *High* γ: Usable and secured, operates seamlessly with high degrees of security and operational effectiveness	Measures the degree to which the system is both secure and usable
δ	*Low* δ: secure and usable but only with strenuous effort on the part of the user *High* δ: Optimal Equilibrium State (OES): secure, usable and understandable	Measures the degree to which the system is secure, usable and understandable in a unified way; the larger this convergence area, the higher the alignment between the three models, and the higher the likelihood of achieving an optimal solution using the three domains. In other words, this is where the trade-off effect is minimised

- *The difference between* δ_2 *and* δ_1: This divergence expresses the designer/user's Mental Model Gap (MMG) that establishes the sphere for the designer's creative insight to improve usability and security within the boundaries of the user's conceptualisation; it is achieved through experience and familiarity with the system and the environment. In the main, its value reflects the degree of the designer's ability to minimise the paradox between conflicting actions such as protecting against malicious intruders and the authentic user convenience. The MMG can be mitigated by different mechanisms including nontechnical

Table 2. Possible relationships between usability and security components, where the numbers in the first column indicate the number of the unidirectional or bidirectional relationships shown at the arrows depicted in Figure 2.

No.	Relationship description and findings	Sources
1	Secure UI with less authentication error and less encryption failure will increase confidentiality. But the complexity of the encryption interface such as security certificates and as many security provisions CAPTCHA may decrease efficiency at the user level	Hanmer, McBride, and Mendiratta (2007), Crespo (2013), Braz, Seffah, and M'Raihi (2007), Li, Raghunathan, and Jha (2010), Jain and Sivaselvan (2012), Ajjana et al. (2014), Carroll and Mcelellan (1971)
2	Effective usage of secured (encrypted) UI increases confidentiality, while failed commands and information leaks due to confidentiality errors decrease effectiveness	Rukšènas, Curzon, and Blandford (2008), Li, Raghunathan, and Jha (2010), Chang and Lin (2007), Chen (2009), Baker and Wallace (2007)
3	Encrypted data and biometric authentication improve user's satisfaction through feeling of protection and privacy	Hanmer, McBride, and Mendiratta (2007), Sae-Bae et al. (2014), Chowdhury, Poet, and Mackenzie (2014), Aljahdali and Poet (2014), Hyun, Wang, and Ullrich (2012), Braz, Seffah, and M'Raihi (2007)
4	Learnability improves confidentiality through reducing errors. Complex authentication takes longer time to learn, but CAPTCHA and password metaphoric representation improves learnability	Crespo (2013), Jain and Sivaselvan (2012)
5	Many complex authentication methods create memorability problems, but improving memorability through graphical password provides better authenticity and confidentiality	Crespo (2013), Renaud and De Angeli (2004), Braz, Seffah, and M'Raihi (2007), Kainda, Flechais, and Roscoe (2010), Renaud (2003)
6	Data consistency improves data efficiency and data integrity. Using links is more efficient and effective than folio	Coursaris and Kim (2011), Liu and Li (2011)
7	Effectiveness increased due to integrity controls that result in reliability, more accuracy, less time spent on error and less repetition of the task	Willer et al. (1999), Ratnasingham and Swatman (1997), Chang and Lin (2007)
8	User satisfaction is attained due to reliable, accurate and complete data. Integrity reduces the number of times the users get frustrated and increases user's trust and feeling of protection	Zhang and Shen (2006), Fisher and Chu (2009)
9	Learnability increases due to accuracy; easy learning helps data integrity; learnability promotes protection of sensitive information	Coursaris and Kim (2011), Braz, Seffah, and M'Raihi (2007)
10	Availability always increases user satisfaction and reduces number of user complaints	Scott and Keyworth (1998), Fikre and Mostefaoui (2012)
11	Availability encourages learnability; learnability of a system is directly dependent on immediacy in response to user actions and feedback	Ashley, Brandon, and Cates (2014), Jain and Sivaselvan (2012)
12	System availability has a direct effect on effectiveness	Sun et al. (2012), Willer et al. (1999)
13	Assured system brings satisfaction, enjoyment and less frustration due to loss of data. But, highly assured system may fail due to lack of user acceptability	Winter, Wagner, and Deissenboeck (2008), Doll et al. (2004), Irvine et al. (2002)
14	Confidence and assurance increase learnability	Jain and Sivaselvan (2012)
15	Increase in system availability reduces user waiting time, improves system task success rate	Sun et al. (2012)
16	Effectiveness largely depends on assurance	Fisher and Chu (2009)
17	Effectiveness of UI fosters accountability	Chang and Lin (2007), Vance, Lowry, and Eggett (2013)

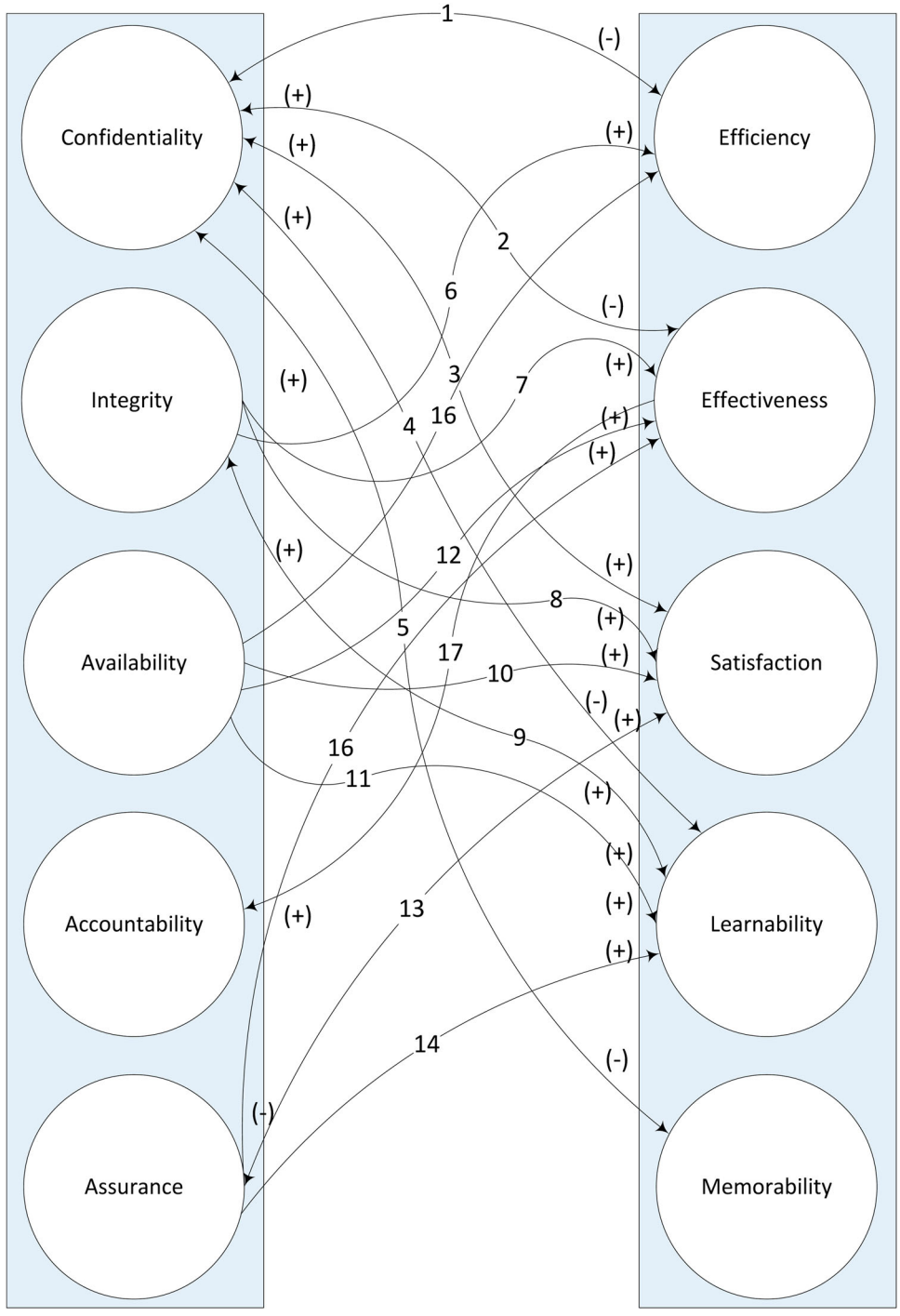

Figure 2. The *cognitive map* of the components' Cartesian relationship between usability and security divided into constituent relationships of security principles (block on the left) and usability features (block on the right). A (+) indicates a positive relationship, while a (−) indicates a negative relationship that affects the meta-model and the size of its Optimal Equilibrium State (OES) δ.

solutions such as launching a Knowledge Management (KM) initiative. KM facilitates the elicitation of the user's tacit knowledge for the designer to apply it into the design. Other methods such as development of elicitation techniques for specific purposes can be employed. For instance, Chao, Salvendy, and Lightner (1999) developed a conceptual framework and an operational methodology to extract knowledge from experts for diagnosis, debugging and interpretation of applications. Similarly, Ahrama, Karwowskia, and Amaba (2011) proposed the use of collaborative social networking and system engineering processes to share and integrate knowledge for the design and development of better products.

- *The equivalence of δ_2 and δ_1*: This equilibrium status is materialised only when the usability designers' mental model equalises the users' mental model. This condition cannot be fully satisfied because of the intrinsic differences between the two personal mastery levels as stated by Senge (1990) and described by Gillan et al. (1995) and Wells and Fuerst (2000). The conjoint cognitive space between δ_1 and δ_2 is a Cartesian product of the SMM. The SMM can be dealt with at two distinct levels: one as the shared beliefs at the designers' team level (SMM_1) and the other among team members of the users' community (SMM_2). Attaining the potential maximum alignment between the two at professional levels is a characteristic of any successful design. Each level is inclusive to the cultural, behavioural and epistemological aspects about how usability and security work using available system functionalities. Karray et al. (2008) defines functionality of a system as a set of actions or services that it provides to the user, while usability of a system with specific functionality is the range and degree by which the system can be used efficiently to accomplish specific goals for the user. The authors concluded that, in reality, the effectiveness of that system is reached when there is a proper balance between functionality and usability of a system. This will be explained in the four optimal solutions OES (δ) scenarios described below.

Complete harmony between SMM_1 and SMM_2 will never happen as the mutual exclusiveness is inconceivable. Likewise, perfect security is not in the agenda of any security professional, yet widely open insecure systems are not good for usability either. SMM_1 and SMM_2 are intrinsically different, but this incompatibility should be kept at minimal levels to prevent system failure. Langan-Fox, Platania-Phung, and Waycott (2006) investigated the usability of services provided by a mobile phone network and found that there are substantial differences between the designer and novices' mental models. The authors added that in relation to system learning, usability should be evaluated according to the user's mental model. If a significant inconsistency exists between the system designer and the user's mental model, then there could be a problem with the instructional material or the intuitiveness of the system.

One of the very simple techniques used to transfer new cognitive expressions to users' mental models in conceptual models is the use of metaphors. Metaphors can stand for an item or a system, Nielsen (1990) reported that a metaphor may represent a model of the user's conceptual model of the computer system. However, the interpretation of a metaphor depends on the acquaintance of the actor with the represented item or system. This, in fact, is a distinguishing factor between the user and the designer's mental model. Gillan et al. (1995) studied the reactions of experts and novices to interface metaphors employing cognitive and computing capabilities. The authors found that both experts and non-experts have significantly different mental models. While experts interpret metaphors through their abstract attributes, novice users use their literal physical or concrete abilities in their interpretations. These capabilities are not inclusive in the case of the expert. Consequently, the concrete objects can conflict with the expert's mental model and may dilute their effects by adding abstractions that make it difficult for novice users to comprehend.

- *Usable Security Gap* (*USG*): The USG between users and designers can be expressed by the difference between γ_1 and γ_2. The designer uses heuristics of the mental model to describe, relate and explain the user's requirements and predicts the user's future needs. Nielsen (1990) noted that heuristics are essential for designers to abstract design dialogs; comprehend observations and make decisions from user testing, and field studies. The difference between γ_1 and γ_2 is virtually controlled by the factors contributing to the construction and balancing of the meta-model. Nevertheless, the ultimate objective of balancing the meta-model is to increase the size of the OES (δ) which will have direct effects on diluting the compromise of the trade-off. This is the most intriguing area of interaction, which can be demonstrated by application of usability principles using access control scenarios. In accordance with the meta-model, the definition of access control can be stated as the relationship among: (1) the user mental model (the subject); (2) the system through the software usability model (the object) and (3) the security model (the access control mechanism), where it involves the transfer of information between the user process and the system.

Information security controls must have insignificant impact on the ability of authorised users to interface with the system to perform their duties. In other words, restrictions imposed by security controls should not be too complicated for the average user to understand or waste time on them relative to the tasks being accomplished. Put differently, information must be protected by all possible security mechanisms, but it should not be overly protected to the extent that it becomes difficult for the user to use it. At the same time, the minimisation of the overprotection should contribute to the dilution of the trade-off effects. Access control is achieved through an entire set of security mechanisms as the user interacts

with the system and there are many scenarios that show the variations in the level of usability and the degree of security. The following four user-centred security scenarios demonstrate various applications of security controls through interface restrictions where security models considered software usability as the primary goal and provide opportunities for obtaining a higher OES (δ) that reduces usability security trading-off compromise effects:

(1) *Menus and shells*: The usability designer specifies a menu that offers novice users only particular options that are important for them to complete their tasks. Unwanted items of the menu may be contextually greyed out due to the policy implementing security principles such as 'least privilege' or the 'need to know'. Novice users are kept informed through a proper UI about what is available to them. Better restrictions are imposed by context-aware menu, but Zaphiris, Shneiderman, and Norman (2002) extended the usability improvement by comparing expandable indexes that provide full menu context with sequential menus which provide only partial context. The authors found that expandable indexes resulted in poorer performance. The usability designer also can design a shell that connects expert users, such as administrators to the operating system commands based on the role specified in the user's profile. In this scenario, security decisions are enforced by the navigation path and influenced by the user's mental model, which is entirely based on the level of experience and authority.
(2) *Database views*: Views in the databases that hide specific fields from being displayed in the menu of an application can be used for implementing Content Dependent Access Controls (CDAC). CDAC is achieved when the access is based on the content or the attributes of an object. Accordingly, usability designers may develop a User-Adaptive Interface (UAI) to select specific fields or content from a database table according to the user role or task context. In such user-centred design, the usability designer is aware of the business and the user's requirements trend, knowledge structures and expectations. Obviously, CDAC and UAI can be aligned, only if the designer is fully aware of the general user's behaviour and mental model.
(3) *Physical constrained interfaces*: The usability designer provides a physically restricted interface model of a keypad with limited special characters or numbers available to the user to interact with the system. This constrained interface presents an access control GUI method that limits the users' access to specific functional areas in applications such as the Automated Teller Machine (ATM). The keypad of the ATM is part of the usability of the machine, as Winter, Wagner, and Deissenboeck (2008) state that the usability model does contain both the logical UI and the physical UI. In other words, the external physically constrained interface reflects internal logical representation by menus and shells or database views. In this model, the usability is perfectly in congruity with security through manoeuvring the user mental model into particular directions to prevent errors or fraud. As a result, the predictions and the outcomes of the user mental model actions are restricted with certainty to the designer and the security professional.
(4) *Embedded controls*: Many security control mechanisms such as entrapment and enticement practices can be entirely embedded in UI. Entrapment is a process in which the interface inspires a person who has no intention to commit a crime to do so (Charles 2004; Scottberg, Yurcik, and Doss 2002). On the other hand, enticement is where the interface tempts the attacker to persist in committing the crime until caught. Regardless of the ethical concerns that entrapment and enticement may raise, their effectiveness solely depends on the level to which the GUI is perfected. A compelling design of a deployed pseudo-flaw may appear like a loophole that lures the attacker who may think it is an opportunity for a zero-day attack, but in fact, it is an implanted Trojan horse. This design aims to represent the opposite of the subject's mental image. Alternatively, embedded controls can also be employed in reducing risk by avoiding attacks, or preventing the user from intentionally breaching security or committing unintentional errors.

4. Implementation of the meta-model

The main objective behind the development of the organisational mental model for implementation of the SUM meta-model is to narrow the MMG or to increase the OES (δ) (Table 1). This will result in hardening systems without forfeiting usability and ameliorating usability without increasing the risk of vulnerabilities. The meta-model depends on the schema (knowledge structures) of the actors and the associated cognitive and behavioural processes as practised in the SMM setting. The participatory design as described by Shum (1998), Komlodi and Soergel (2002), Carroll (2006), Faily (2011) will establish itself and becomes effective, when the compartmentalised knowledge of the organisation

is shared among the entire organisation communities. Carroll (2006) defined participatory design or cooperative design as 'a large collection of attitudes and techniques predicated on the concept that the people who ultimately will use a designed artifact are entitled to have a voice in determining how the artifact is designed'. This requires the usability designers to understand how potential users interact with the application and among themselves. Thomas and Bostrom (2007) report that SMM is important in teamwork especially when the team is required to navigate unforeseen situations or complex problems as they arise, and it enables teams' timely predictions of coming needs and issues. All can be modified to improve the conceptualisation, interpretation and inference of complex interactions with UI and security controls. However, these practices are not universally applicable to usability and security designs; hence, there are no generalisable formulae per se. Any strategy developed in this area constitutes a class of its own as it depends on a pool of experiential settings and unique cultural aspects of the user community and must be meticulously amended before it can be applied to a different environment. Shneiderman and Hochheiser (2001) noted that to build universal usability the designer needs to account for a wide range of technology and users' diversification and depth of knowledge. Moreover, Gu and Shi (2008) stated that it is critical for the designer to understand the marriage of the implementation model and the conceptual model which results from the mental model in any product design. The design process can be envisioned as an outcome of an iterative process for nurturing and mobilising knowledge between all participants. Nielsen (1993) prescribed the iterative design to refine the interface based on lessons learned from previous iterations. However, the author believes that no matter how many iterations are carried out, the 'ultimate user interface' is still not fully understood and it needs more investigation.

In general, knowledge can be divided into two major classes, namely, explicit knowledge and tacit knowledge (Bassellier, Reich, and Benbasat 2001; Filipowski et al. 2012; Mariano and Casey 2007; Wyatt 2001). Explicit knowledge is represented by the tangible UI features and the software artefacts such as manuals, guides, searchable knowledge-base, etc. However, Molich and Nielsen (1990) warned that although these guidelines are considered necessary, it is unsatisfactory input to construct good human-computer interfaces. Tacit knowledge, on the other hand, is more intuitive to the user and is critical for understanding the match of the implementation model and the mental model in application development and design. Put differently, tacit knowledge is the main driving factor for narrowing MMG and increasing OES (δ) as shown in Figure 3. Kaipa (2000) who proposed an architecture for managing knowledge believed there is a difference between data, information and knowledge, and without context, culture and 'tacitness', knowledge will not be much different from information.

Lindman, Rossi, and Tuunainen (2013) defined data as a term related to storage and preservation of symbols, but having no meaning by itself and can become information when interpreted by an actor. The transformation from data to knowledge takes place through context and semantics during acquisition, nurturing and sharing processes. Nonaka and Takeuchi (1995) defined knowledge as a true and justified belief. In relation to information Johannessen, Olaisen, and Olsen (2002) define knowledge as systematising and structuring of information for one or more purposes. In an attempt to coalesce these definitions, Mohamed (2008) described the non-spatial distance between data and knowledge as a data-information-knowledge continuum. Within this continuum discrete data transforms into rich knowledge as it transfers through addition of context and value. The transformation from data to knowledge takes place through context and semantics during acquisition, nurturing and sharing processes. However, Davenport and Prusak (2000) recommended that before initiation of any knowledge initiative organisations must take a hard look at their culture. Gerami (2010) reported that understanding the culture is a key issue for the successful implementation of knowledge.

4.1. Tacit knowledge elicitation

Tacit knowledge forms the cornerstone of the mental model development process, as it transfers and transforms the skills and experiences of all those who are involved in the design and the usage of the system. The individual participant in the design process is regarded as the primary repository for tacit knowledge. This is well explained in the concepts of 'Personal Knowledge' by Polanyi (1958), personal mastery level by Senge (1990) and 'knowledge creation' by Nonaka and Takeuchi (1995). Tacit knowledge benefits from designing usability and security as crystalised from a complex intermixing of ontological perspectives of the user and the designer. However, the degree of 'tacicity' needed for bridging the MMG is characterised by the blurred boundaries of dispersed intellectual capacities. The user and the designer may face inherent difficulties in not only articulating tacit knowledge, but also managing and using it. Amidst these complex challenges of

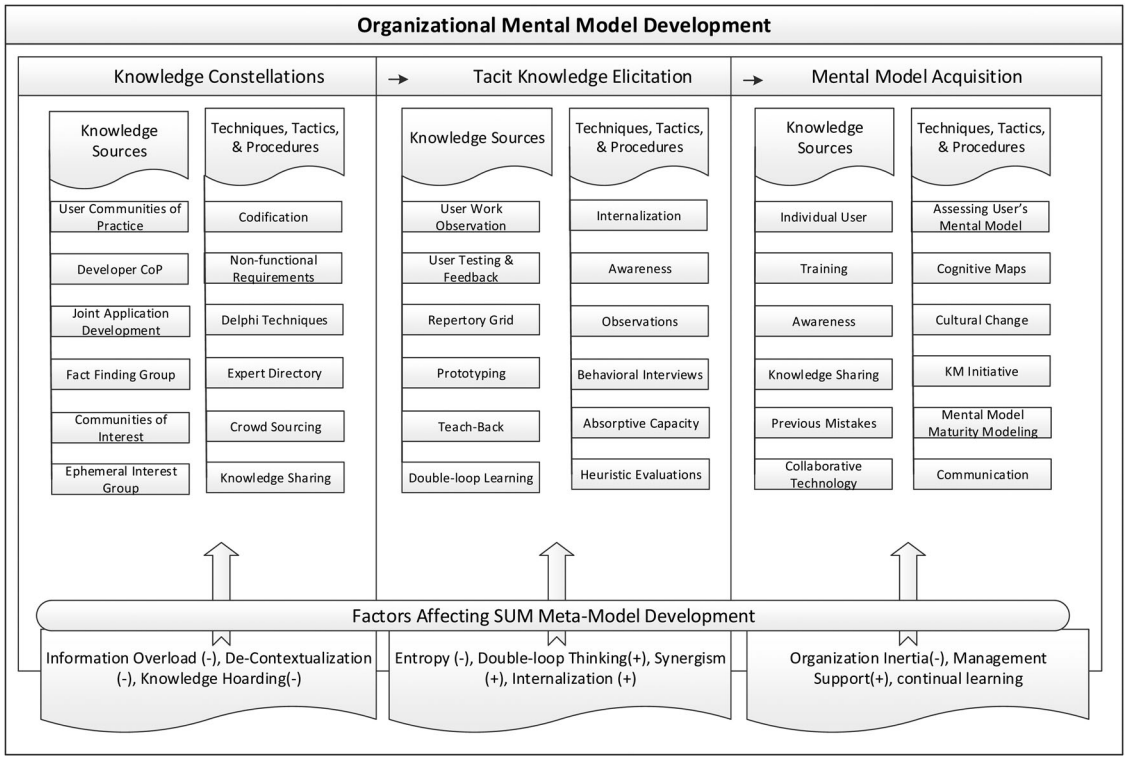

Figure 3. Knowledge transfer and transformation during mental model development. A (+) indicates a positive relationship, while a (−) indicates a negative relationship that affects the meta-model development phases.

assimilating and representing tacit knowledge, the designer must be able to translate this type of knowledge into the design that not only satisfies the user's current goals, but also fulfils the security requirements and the future trends of the system usage.

The essence of the user's tacit knowledge is built through internalisation (Nonaka and Takeuchi 1995), where internalised knowledge can be shared with the designer through externalisation or codification of both structured and unstructured knowledge to convey the user's requirements. Unsurprisingly, the process usually suffers some knowledge manipulation loopholes such as knowledge leaks, dilution, de-contextualisation and entropy. However, the ultimate success or failure of this unwieldy process depends on the ability of the designer to induce the highest mental model capabilities to express the system functions in the user's terms.

Capturing tacit knowledge can be accomplished through careful elicitation from individual users and from Communities of Practice (CoPs) with members that are not only aesthetically conscious, but also technically versed in their domains. This elicitation occurs through many techniques such as observation through association, where the designer observes the user's behaviour while using the system or providing feedback and analysis from testing or acceptance processes.

It is preferred that the designer or their representative sits with the user and carefully monitors how the user uses the system, during prototype testing phases, to accomplish her tasks and how the user employs her own heuristic decisions during system usage. The designer should also watch user behaviour and reflections upon the learning loops at intellective (cognitive) and agentive (body language) capacities.

4.2. Knowledge networks

Knowledge is a socially constructed cognitive structure, where users and designers within a group's interaction will result in collective brainpower that may lead to an optimal synergy for higher OES (δ) or better SMM levels. As depicted in Figure 3 knowledge constellations are self-organised groups of users, designers, architects and stakeholders established to 'de-layer' the rigid functional silos of knowledge and collaborate to improve the quality of systems. The benefits of these groups increase as more people with experience join each group (i.e. more intellectual capacities). In another publication, the principal author of this paper argued that Metcalfe's law of physical networks usually governs this relationship, where it states that the value of the network is proportional to the square of the number of connected users in the

system. Formally, this correlation can be expressed as:

$$\lambda = \eta^2,$$

where λ stands for value gained and η stands for the number of users or network nodes. This law can be extrapolated to represent social networks with some modifications to represent the synergy that results from human behaviour and interactions:

$$\lambda = \eta^2 + \Sigma\rho,$$

where $\Sigma\rho$ stands for the totality of the synergistic effects.

In general, systems built as the result of pooled contributions have a higher quality compared to systems based on individual inputs. This is in agreement with Brazier, Moshkina, and Wijngaards (2001) who observed that the usability product of collaborative and distributed design significantly differs from that of an individual designer working in relative isolation. In collaborative participatory design, the designer rationalises many fundamental elements including design partners, design culture and a shared understanding of the design problem, which are irrelevant when envisioned by a single agent design. In addition to formal coordination activities of interface development, Nielsen (1992) called for shared culture among the development groups for better decisions in the development of a highly usable interface. Hung, Laia, and Chang (2011) and Damodaran and Olphert (2000) required the cultural change for successful knowledge sharing.

Knowledge constellations (Figure 3) can also significantly contribute to narrowing the gap of tacit knowledge and transfer it from users to the designers to increase OES (δ) space. Examples of these constellations are the CoPs and Communities of Interest (CoIs). CoPs are voluntary where all members have the same goal of sharing knowledge and/or finding solutions for complex problems. The same definition can be applied to CoIs; however, CoIs are more specialised in what the members discuss and share. To discover what users want from the system, Nielsen (1997) proposed the use of focus groups for interactive systems development. Additionally, Brothers et al. (1992) introduced the notion of ephemeral interest groups as a short-lived virtual discussion group to solve usability problems in a wider community.

The best security and usability knowledge transfer among these groups occurs through face-to-face interaction. But when physical presence is not possible, then virtual communities can be established as described by Çakir (2002) and Carroll and Rosson (2003). In virtual communities, a collaborative platform technology or groupware may cautiously be used as a conduit for knowledge sharing where technology may result in knowledge de-contextualisation or dilution. The lead designer can facilitate or attend the group's meetings virtually or in person to extract knowledge from the group members. For addressing specific design and security problems, the designer may carry out panel interviews with CoP members from different domains such as a User CoP (UCoP) and a Designer CoP (DCoP). However, for issues that are more specific, the designer may be engaged with a special Fact-Finding Group (FFG) such as Joint Application Development (JAD) or SA focus groups. There are many Techniques, Tactics and Practices (TTPs) that can be implemented to coalesce a group's knowledge such as content management, crowd sourcing and Delphi techniques, which can be used to solicit ideas and requirements from users.

5. Mental model acquisition

The development of SMMs is a consistent regimen that can be achieved only if it becomes a de facto behaviour of the organisation that is willing to be a learning organisation. The purpose of mental models as discussed in this research is to improve usability and security through improving SMM or narrowing the MMG or enhancing OES (δ). This is based on the assumption that users take actions according to their mental model, which is indicative of their proficiency level. Baker (1998) discussed the basic nature of mental models and concluded that the development and adaptation of mental models takes place throughout a person's life span to result in 'expert performance'.

Developing a usability- and security-based culture in the user's community is a lengthy process that needs collective effort of the whole organisation and its leadership. The development of such culture includes progression in both security mechanisms and the mental model of the users. In fact, the development of a mental model requires the organisation to establish a new mindset and incorporate a different culture of collaboration along with developing broad programmes for sharing best practices and lessons learned within its environment, involving outside partners such as customers and other developers.

Zhang and Kim (2011) defined explicit knowledge as the knowledge that is 'expressed in words, and can be easily communicated and shared in the form of hard data, scientific formulae, reports, articles, manuals and patents as well as in software and charts, and codified procedures'. Explicit knowledge can be built through documenting the designer's current project and archiving of lessons learned from problem-solving techniques. These knowledge artefacts can be refined/modified,

stored and retrieved when needed in other development projects. In an attempt to determine best heuristics for solving usability problems, Nielsen (1994) recommended publishing sets of usability heuristics to compare them with database of existing usability problems collected from different projects to solve real usability problems. This process is similar to the accumulation of knowledge from previous research and lessons learned from success and failure factors in systems development, so the developer can adopt them or avoid their undesirable effects in the future.

Mental model acquisition and development are intrinsic to their environment. Hence, the effectiveness of mental model development TTPs varies among organisations, environments and cultures along with their inherent types of knowledge. The following TTPs are essential, but can be customised by blending the uniqueness of the environments into their implementation:

(1) *User's mental model assessment*: Understanding the user's conceptualisation trajectory and inference effectiveness is vital for the development of the users' mental model to address specific usability design parameters and/or security architecture. The user possesses the heuristics to understand the basis behind the interface or to manipulate it to solve a relevant problem. Khelifi and Suryn (2003) stated that usability is a central element in productivity and software acceptance. However, without the comprehensive acquaintance of the user with the system, the implementation and the learnability of the system becomes a foremost challenge.

Assessing the user's mental model for the design phase is critical for the design success. Puerta-Melguizo, Chisalita, and Van der Veer (2002) stated that usability designers must assess the mental model of the potential users and their behaviour when they plan to design a new system. These insights can be used to improve a user's cognition and expectations, which will directly improve system usability. Of course, the best way to express users' needs is to meet face-to-face with them, in participatory design sessions, to gather and analyse their data. However, due to the complexity of human knowledge acquisition processes, the discovery of which type of mental model to apply is a challenging task. In fact, in some cases, it is not feasible, while in other cases it is feasible but not recognisable.

Accordingly, the designer can design artefacts that can be contextually predictable by the user instead of concretely memorised. The security community has reached a conclusion that user behaviour plays a major part in security failures. However, Sasse, Brostoff, and Weirich (2001) argued that the real problem is the security design that leads to such behaviour. Abawajy (2014) reports that implementation of security depends on the user. This is also corroborated by Huang, Rau, and Salvendy (2010) who stated that 'no matter how well the system designed, security methods rely on individuals to implement and use them'. To resolve this noticeable issue, usability designers need to address human memory, conflicting task demands, training, support and motivation issues. The authors concluded that HCI knowledge and methodologies could be employed to minimise or eliminate such difficulties and produce effective and usable security.

(2) *Developing cognitive maps*: The cognitive map is a diagrammatic representation of declarative and partial procedural knowledge structures within the target environment. Knowledge structures express what, how and why we know a fact and what we think about it. Narrowing the MMG or increasing OES (δ) requires understanding of not only knowledge structure, but also potential mental representations. Hence, cognitive maps such as the one shown in Figure 2 can be used to represent the relationships and the differences between SMM_1 and SMM_2, which may lead not only to minimising incompatibility, but also to marrying the requirements with the design at the cognitive levels.

(3) *Changing the culture*: The development of a mental model cannot be achieved without a cultural shift towards behaviour that supports knowledge nurturing and mobilisation practices. In fact, Milne (2007) describes knowledge sharing itself as a journey of cultural change, besides Lin (2007), Richert (1999) and Trim and Lee (2008) reported that cultural change is required for implementing strategic KM and sharing. Pursing the same logic, Metaxiotis, Ergazakis, and Psarras (2005) argued that KM is not about managing knowledge, but it is about changing entire cultures and strategies of organisations to ones that value learning. Adebanjo and Kehoe (1998) observed that cultural change is increasingly being recognised as an imperative to total quality development. The cultural change that is necessary for mental model development can be accomplished through the following activities:

- Promote communication with previous system development teams and stakeholders to avoid previous mistakes and reinventing the wheel. Lin (2007) concluded that the communication climate and employee affective commitment are antecedents for a knowledge-sharing culture. In

fact, communication is central to the definition of culture itself as Herbig and Dunphy (1998) reported that culture is an all-inclusive system of communication. Without proper communication, a knowledge-sharing culture may fail. Al-Alawi, Al-Marzooqi, and Mohammed (2007) found that communication between staff of an organisation has a positive effect on the success of knowledge sharing. In addition, communication is a core characteristic of teamwork; as stated by Wang and Liu (2009), a team must nurture a communication culture, construct a SMM through a communication level, communication platform and communication mechanisms to improve performance.

- Instill knowledge creation and a sharing culture that facilitates participatory design by leveraging the broader skills of the community. Trindade et al. (2012) analysed the role of KM tools to promote knowledge creation in its CoP. The authors found that CoP knowledge contribution is demonstrated by sharing information, experiences and skills deemed necessary in the design of supporting tools for deaf communities. Komlodi and Soergel (2002) employed iterative participatory design that allowed users to design the interface. In fact, Carroll (2006) described participatory design as cooperative design where users become part of the development team.
- Develop a continuous learning culture that empowers users to exercise double-loop learning for developing requirements, performance testing and conducting experiments. Riedinger (2008) used designing and implementing a learning centre to promote continual learning and to change culture. Double-loop learning is an iterative process that begets creativity by changing the basic assumptions in the organisation. Stary (2014) described double-loop learning in two different phases, namely, knowledge generation and knowledge integration.
- Create collaborative working environments that support trustful relationships and quality-oriented culture. Xiao and Carroll (2007) reported that collaboration stimulated learning though interaction and extrapolated different ideas to create new knowledge. This is substantiated by Garrett and Caldwell (2002) who developed a model of human collaboration in distributed knowledge-sharing groups; the model consisted of face-to-face meetings for context sharing and using of Information and Communication Technologies (ICT) different UI design options. The author found that collaboration depends on the functionality of ICT to support performance.
- Stimulate teamwork and encourage partnership in various knowledge constellations. Strachan (1996) stated that team work fosters key features of learning organisation such as innovation and creativity. Kennedy (2011) attributed team creative processes to the two types of mental models, complementary and SMMs. El-Tayeh, Gil, and Freeman (2008) developed a methodology to assess the usability of prototypes for digital socialisation of virtual designers' teams and found that digital socialisation coalesced individuals to create group tacit knowledge that significantly enhanced the results of the collaborative work.

(4) *Installing knowledge management initiative*: The MMG can be remediated by different mechanisms including socio-technical solutions such as launching targeted KM initiatives. Major relevant KM practices can be used in preparing for and extracting knowledge for improving usability and security in the following ways:

- Develop a domain-specific tacit knowledge elicitation programme to extract users' intellectual contributions to improve the intuitiveness of the system.
- Establish social knowledge constellations as free zones of thinking, brainstorming and knowledge-sharing platforms.
- Deploy collaborative technology with knowledge sharing and collaboration modules such as expert directories, content management, lessons learned codification and best practices.
- Develop a broad training and awareness programme where users are able to participate in requirements gathering and be aware of security requirements. The lack of users' knowledge and awareness will lead them to use their own judgement about systems and security matters and in ways that are likely to be inadequate.

(5) *Defining model maturity*: Mental Model Maturity Model (M4) is a progressive process that describes the development of mental model dependencies and relationships in the organisation over time. M4 is achieved by advancing through different phases of mental model development to reach optimal levels where the user's tacit knowledge is translated into the design. It uses user satisfaction and heuristic principle to measure levels of complexity in mental model development and makes them available for use. The maturity model indicates how well an organisation's mental models are

articulated and understood as compared to predetermined benchmarks or best practices. There are no universal standards for M4 measurement; yet, but more mature organisations are typically characterised by a modest MMG. Mental model maturity should measure the capability of controlling the convergence area OES (δ) and how that affects the MMG magnitude. It is not the purpose of this paper to establish M4 for usability and security purposes. However, metrics and criteria for mental model development are needed to measure the congruity of the user and the designer's mental models. A sign of the organisation's mental model maturity is its ability to make the shift from procedural solutions to double-loop learning alternatives.

6. The bottom line

In the quest of achieving higher effectiveness of user-centred design without compromising the security posture of a system, this paper adopted a holistic approach to construct the SUM meta-model. The model has been developed to bridge the gap between the designer and the users' mental models. It assumes that security and usability components and their interactions are a result of the knowledge structures and cognitive processes that arise from blending the user and the designer's thinking. As substantiated by many investigators, the model considers the complete incongruence of usability and security as a flawed notion. Nonetheless, incompatibility exists in some areas of security and usability levels. The level of incongruity can be ordinated through the collective power of the mental model to produce higher levels of congruence. Therefore, this congruence of usability and security specifications are goals that can be fulfilled by carefully studying and marrying the requirements at the cognitive and behavioural levels of the user, the security professional and the designer. This will have a high impact on the practicality of both the security model and the usability model in a user's real life. For example, how closely the interface narrows the distance between online and brick-and-mortar shopping through intuitive navigation, while preventing unauthorised disclosure, will have a direct effect on the users' wallet.

The dissimilarity between the designers' mental model (SMM_1) and the users' mental model (SMM_2) should be exploited to achieve the maximum benefits of the participatory design.

The proportionality of the three prongs of the SUM meta-model determines the convergence area OES (δ) which varies according to the cognitive input of the participants in the environment. Therefore, the meta-model elements' contribution cannot be generalised over a diverse range of environments, unless refined to accommodate specific environment requirements. In effect, the SUM meta-model is not exhaustive by any means. It is an attempt to formally estimate and recognise the importance of the interaction between the three domains, which can be developed and validated through further research on its parameters and its implementation framework.

We argue that the construct and implementation of this model cannot be generalised over a wide range of environments. This is due to the intrinsic uniqueness of the behavioural aspects that govern knowledge sharing and mental model development TTPs. Therefore, the SUM meta-model needs future research for verification and validation to fit within multiple environments.

Acknowledgements

The authors would like to thank Dr Arthur Murray CEO of Applied Knowledge Sciences Inc. for his heedful review of the manuscript many times and his enlightening comments on the role of Knowledge Management in usable security. We also express our sincere gratitude to Dr Roger Seeholzer and Mr Eric Barlow of the US Department of Homeland Security in Washington, DC for their meticulous editing, proofreading and constructive comments on security issues.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

Abawajy, J. 2014. "User Preference of Cyber Security Awareness Delivery Methods." *Behaviour & Information Technology* 33 (3): 237–248.

Abubaker, H., K. Salah, H. AI-Muhairi, and A. Bentiba. 2015. "Cloud-based Arabic reCAPTCHA Service: Design and Architecture." 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), Marrackech, 1–6.

Adebanjo, D., and D. Kehoe. 1998. "An Evaluation of Quality Culture Problems in UK Companies." *International Journal of Quality Science* 3 (3): 275–286.

Ahn, L., B. Maurer, C. McMillen, D. Abraham, and M. Blum. 2008. "reCAPTCHA: Human-based Character Recognition via Web Security Measures." *Science* 321 (5895): 1465–1468.

Ahrama, T., W. Karwowskia, and B. Amaba. 2011. "Collaborative Systems Engineering and Social-Networking Approach to Design and Modelling of Smarter Products." *Behaviour & Information Technology* 30 (1): 13–26.

Ajjana, H., R. Hartshorne, Y. Caoc, and M. Rodriguez. 2014. "Continuance Use Intention of Enterprise Instant

Messaging: A Knowledge Management Perspective." *Behaviour & Information Technology* 33 (7): 678–692.
Al-Alawi, A. I., N. Y. Al-Marzooqi, and Y. F. Mohammed. 2007. "Organizational Culture and Knowledge Sharing: Critical Success Factors." *Journal of Knowledge Management* 11 (2): 22–42.
Aldridge, A., M. White, and K. Forcht. 1997. "Security Considerations of Doing Business via the Internet: Cautions to be Considered." *Internet Research: Electronic Networking Applications and Policy* 7 (1): 9–15.
Aljahdali, H., and R. Poet. 2014. "Challenge Set Designs and User Guidelines for Usable and Secured Recognition-based Graphical Passwords." IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, Beijing, 973–982.
Ashley, K., K. Brandon, and T. Cates. 2014. "Drivers of Student Retention: System Availability, Privacy, Value and Loyalty in Online Higher Education." *Academy of Educational Leadership Journal* 18 (6): 1–15.
Baker, P. 1998. "Mental Model and Lifelong Learning." *Innovations in Education & Training International* 35 (4): 310–318.
Baker, W., and L. Wallace. 2007. "Information Security under Control? Investigating Quality in Information Security Management." *IEEE Security and Privacy Magazine* 5 (1): 36–44.
Banday, M., and N. Shah. 2009. "A Study of CAPTCHAs for Securing Web Services." *International Journal of Secure Digital Information Age* 1 (2): 66–74.
Bassellier, G., B. Reich, and I. Benbasat. 2001. "Information Technology Competence of Business Managers: A Definition and Research Model." *Journal of Management Information Systems* 17 (4): 159–182.
Ben-Asher, N., J. Meyer, S. Möller, and R. Englert. 2009. "An Experimental System for Studying the Tradeoff Between Usability and Security." International Conference on Availability, Reliability and Security, Fukuoka, 882–887.
Bevan, N. 2001. "International Standards for HCI and Usability." *International Journal of Human Computer Studies* 55 (4): 533–552.
Bo, W., Y. Zhang, X. Hong, H. Sun, and X. Huang. 2014. "Usable Security Mechanisms in Smart Building." 17th International Conference on Computational Science and Engineering, Chengdu, 748–753.
Bravo-Lillo, C., L. F. Cranor, J. S. Downs, and S. Komanduri. 2011. "Bridging the Gap in Computer Security Warnings: A Mental Model Approach." *Security & Privacy* 9 (2): 18–26.
Braz, C., A. Seffah, and D. M'Raihi. 2007. "Designing a Trade-off Between Usability and Security: A Metrics Based-Model." Human-Computer Interaction – INTERACT 2007: Lecture Notes in Computer Science 4663, 114–126.
Brazier, F. M. T., L. V. Moshkina, and N. J. E. Wijngaards. 2001. "Knowledge Level Model of an Individual Designer as an Agent in Collaborative Distributed Design." *Journal of Artificial Intelligence in Engineering* 15 (2): 137–152.
Brothers, L., J. Hollan, J. Nielsen, S. Stornetta, S. Abney, G. Furnas, & M. Littman. 1992. *Supporting Informal Communication Via ephemeral Interest Groups*. Paper presented at the Conference Computer-Supported Cooperative Work, Toronto, Canada.
Bulgurcu, B., H. Cavusoglu, and I. Benbasat. 2010. "Information Security Policy Compliance: an Empirical Study of Rationality-based Beliefs and Information Security Awareness." *MIS Quarterly* 34 (3): 523–548.
Bushma, A. V. 2010. "Information Security for Optoelectronic Ergatic System." *Semiconductor Physics, Quantum Electronics & Optoelectronics* 13 (2): 170–172.
Çakir, A. E. 2002. "Virtual Communities – A Virtual Session on Virtual Conferences." *Behaviour & Information Technology* 21 (5): 365–371.
Camp, J. 2009. "Mental Models of Privacy and Security." *IEEE Technology and Society Magazine* 28 (3): 37–46.
Carroll, J. 2006. "Dimensions of Participation in Simon's Design." *Design Issues* 22 (2): 3–18.
Carroll, J., and P. Mcelellan. 1971. "The Data Security Environment of Canadian Resource-Sharing Systems." *Canadian Journal of Operational Research and Information Processsing* 9 (1): 58–68.
Carroll, J. M., and M. B. Rosson. 2003. "A Trajectory for Community Networks." *The Information Society* 19: 381–393.
Chan, M. T., and L. F. Kwok. 2001. "Integrating Security Design into the Software Development Process for E-Commerce Systems." *Information Management & Computer Security* 9 (3): 112–122.
Chang, S. E., and C.-S. Lin. 2007. "Exploring Organizational Culture for Information Security Management." *Industrial Management & Data Systems* 107 (3): 438–458.
Chao, C.-J., G. Salvendy, and N. Lightner. 1999. "Development of a Methodology for Optimizing Elicited Knowledge." *Behaviour & Information Technology* 18 (6): 413–430.
Charles, K. A. 2004. "Decoy Systems: A New Player in Network Security and Computer Incident Response." *International Journal of Digital Evidence* 2 (3): 1–9.
Chen, T. M. 2009. "Information Security and Risk Management." In *Encyclopedia of Multimedia Technology and Networking*, edited by M. Pagani. Hershey, PA: Idea Group.
Chowdhury, S., R. Poet, and L. Mackenzie. 2014. "A Study of Mnemonic Image Passwords." Twelfth Annual Conference on Privacy, Security and Trust (PST), Toronto, ON, 207–214.
Costas, L. 2000. "Smart Card Technology for Deploying a Secure Information Management Framework." *Information Management & Computer Security* 8 (4): 173–183.
Coursaris, C., and D. Kim. 2011. "A Meta-Analytical Review of Empirical Mobile Usability Studies." *Journal of Usability Studies* 6 (3): 117–171.
Cranor, L. F. 2008. "A Framework for Reasoning about the Human in the Loop." 1st Conference on Usability, Psychology, and Security, San Francisco, CA, 1–15.
Crespo, B. G.-N. 2013. "User Interface Harmonization for IT Security Management." Eighth International Conference on Availability, Reliability and Security (ARES), Regensburg, 829–835.
Damodaran, L., and W. Olphert. 2000. "Barriers and Facilitators to the Use of Knowledge Management Systems." *Behaviour & Information Technology* 19 (6): 405–413.
Damondaran, L. 1998. "Development of a User-Centred IT Strategy: A Case Study." *Behaviour & Information Technology* 17 (3): 127–134.
Davenport, T., and L. Prusak. 2000. *Working Knowledge: How Organizations Manage What They Know*. Boston, MA: Harvard Business School Press.

David, M. M. 2000. "Knowledge Objects and Mental Models." International Workshop on Advanced Learning Technologies Proceedings, Palmerston North, 244–246.
Davidson, E. E., B. McCredie, and W. Vikelis. 1994. *IBM Dictionary of Computing*. Edited by G. McDaniel. 10th ed. New York, NY: McGraw-Hill.
DeWitt, A. J., and J. Kuljis. 2006. "Aligning Usability and Security: A Usability Study of Polaris." Soups '06 Proceedings of the Second Symposium on Usable Privacy and Security, Pittsburgh, PA, 1–7.
Dinev, T., and Q. Hu. 2007. "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies." *Journal of The Association for Information Systems* 8 (7): 386–408.
Doddrell, G. R. 1995. "Security Environment Reviews." *Information Management & Computer Security* 3 (4): 3–14.
Doll, W. J., X. Deng, T. S. Raghunathan, G. Torkzadeh, and W. Xia. 2004. "The Meaning and Measurement of User Satisfaction: A Multigroup Invariance Analysis of the End-User Computing Satisfaction Instrument." *Journal of Management Information System* 21 (1): 227–262.
El-Tayeh, A., N. Gil, and J. Freeman. 2008. "A Methodology to Evaluate the Usability of Digital Socialization in "Virtual" Engineering Design." *Research in Engineering Design* 19: 29–45.
Faily, S. 2011. "A Framework for Usable and Secure System Design." PhD diss., University of Oxford, Oxford, England.
Fikre, Z., and A. Mostefaoui. 2012. "Caching for Data Availability in Mobile P2P Streaming Systems." 2012 International Conference on Selected Topics in Mobile & Wireless Networking, 48–53.
Filipowski, T., P. Kazienko, P. Bródka, and T. Kajdanowicz. 2012. "Web-based Knowledge Exchange Through Social Links in the Workplace." *Behaviour & Information Technology* 31 (8): 779–790.
Fisher, R., and S. Z. Chu. 2009. "Initial Online Trust Formation: The Role of Company Location and web Assurance." *Managerial Auditing Journal* 24 (6): 542–563.
Fitzgerald, K. J. 1995. "Security and Data Integrity for LANs and WANs." *Information Management & Computer Security* 3 (4): 27–33.
Flechais, I., C. Mascolo, and M. A. Sasse. 2007. "Integrating Security and Usability into the Requirements and Design Process." *International Journal of Electronic Security and Digital Forensics* 1 (1): 12–26.
Forget, A., S. Chiasson, P. C. V. Oorschot, and R. Biddle. 2008. "Persuasion for Stronger Passwords: Motivation and Pilot Study." *Persuasive Technology: Lecture Notes in Computer Science* 5033: 140–150.
Gao, H., X. Wang, F. Cao, Z. Zhang, L. Lei, J. Qi, and X. Liu. 2016. "Robustness of Text-based Completely Automated Public Turing Test to Tell Computers and Humans Apart." *IET Information Security* 10 (1): 45–52.
Garrett, S., and B. Caldwell. 2002. "Describing Functional Requirements for Knowledge Sharing Communities." *Behaviour & Information Technology* 21 (5): 359–364.
Gerami, M. 2010. "Knowledge Management." *International Journal of Computer Science and Information Security* 7 (2): 234–238.
Gillan, D. J., B. S. Fogas, S. Aberasturi, and S. Richards. 1995. "Cognitive Ability and Computing Experience Influence Interpretation of Computer Metaphors." The Human Factors and Ergonomics Society 39th Annual Meeting, Santa Monica, CA, 243–247.
González, R. M., M. V. Martin, J. M. Arteaga, FJÁ Rodríguez, C. A. Ochoa, and O. Zezzatti. 2009. "Web Service-Security Specification Based on Usability Criteria and Pattern Approach." *Journal of Computers* 4 (8): 705–712.
Graham, J., L. Zheng, and C. Gonzalez. 2006. "A Cognitive Approach to Game Usability and Design: Mental Model Development in Novice Real-Time Strategy Gamers." *Cyberpychology and Behavior* 9 (3): 361–366.
Grobauer, B., T. Walloschek, and S. E. Stöcker. 2011. "Understanding Cloud Computing Vulnerabilities." *IEEE Security & Privacy Magazine* 9 (2): 50–57.
Gu, X., and Y. Shi. 2008. "The Match of Implementation Model and Mental Model in Interactive Design." 9th International Conference on Computer-Aided Industrial Design and Conceptual Design, Kunming, 255–258.
Hanmer, R. S., D. T. McBride, and V. B. Mendiratta. 2007. "Comparing Reliability and Security: Concepts, Requirements, and Techniques." *Journal Bell Labs Technical Journal – Information Technology/Network Security Archive* 12 (3): 65–78.
Hashim, N., and A. B. M. Sultan. 2009. "Knowledge Management and Usability Model for Knowledge: Management System." *Computer and Information Science* 2 (3): 166–175.
Herbig, P., and S. Dunphy. 1998. "Culture and Innovation." *Cross Cultural Management: An International Journal* 5 (4): 13–21.
Hillena, F., and B. Höfleb. 2015. "Geo-reCAPTCHA: Crowdsourcing Large Amounts of Geographic Information from Earth Observation Data." *International Journal of Applied Earth Observation and Geoinformation* 40: 29–38.
Houmb, S. H., S. Islam, E. Knauss, J. Jürjens, and K. Schneider. 2010. "Eliciting Security Requirements and Tracing them to Design an Integration of Common Criteria, Heuristics, and UMLsec." *Requirements Engineering* 15: 63–93.
Hsieh, C.-C., and Z.-Y. Wu. 2013. "Anti-SIFT Images Based CAPTCHA Using Versatile Characters." 2013 International Conference on Information Science and Applications (ICISA), Suwon, 1–4.
Huang, D.-L., P.-L. P., Rau, & G. Salvendy. 2010. "Perception of Information Security." *Behaviour & Information Technology* 29 (3): 221–232.
Hung, S.-Y., H.-M. Laia, and W.-W. Chang. 2011. "Knowledge-Sharing Motivations Affecting R&D Employees' Acceptance of Electronic Knowledge Repository." *Behaviour & Information Technology* 30 (2): 213–230.
Hyun, K. S., Q.-H. Wang, and J. B. Ullrich. 2012. "A Comparative Study of Cyberattacks." *Communications of the ACM* 55 (3): 66–73.
Imgraben, J., A. Engelbrecht, and K.-K. R. Choo. 2014. "Always Connected, But are Smart Mobile Users Getting More Security Savvy? A Survey of Smart Mobile Device Users." *Behaviour & Information Technology* 33 (12): 1347–1360.
Irvine, C., T. Leven, J. W. Wilson, D. Shifflett, and B. Pereira. 2002. "An Approach to Security Requirements Engineering for High Assurance System." *Requirements Engineering* 7: 192–206.
ISO. 1998. Ergonomic Requirements for Office Work with Visual Display Terminals (VDT), ISO 9241-11: Part 11: Guidance on Usability. ISO ICS: 13.180; 35.180, 22.

ISO/IEC. 2006. Medical Device Software – Software Life Cycle Processes ISO/IEC Geneva, Switzerland. IEC 62304:2006(E), 11.
Jain, S., and B. Sivaselvan. 2012. "Usability Aspects of HCI in the Design of CAPTCHAs." IEEE International Conference on Computational Intelligence & Computing Research (ICCIC), Coimbatore, 1–4.
Jansson, K., and R. von Solms. 2013. "Phishing for Phishing Awareness." *Behaviour & Information Technology* 32 (6): 584–593.
Johannessen, J.-A., J. Olaisen, and B. Olsen. 2002. "Aspects of a Systemic Philosophy of Knowledge: From Social Facts to Data, Information and Knowledge." *Kybernetes* 31 (7/8): 1099–1120.
Jonas, G. A., and C. S. Norman. 2011. "Textbook Websites: User Technology Acceptance Behaviour." *Behaviour & Information Technology* 30 (2): 147–159.
Jøsang, A., B. AlFayyadh, T. Grandison, M. AlZomai, and J. McNamara. 2000. "Security Usability Principles for Vulnerability Analysis and Risk Assessment." Twenty-Third Annual Computer Security Applications Conference, Miami Beach, FL, 269–278.
Jøsang, A., B. AlFayyadh, T. Grandison, M. AlZomai, and J. McNamara. 2007. "Security Usability Principles for Vulnerability Analysis and Risk Assessment." Twenty-Third Annual Computer Security Applications Conference, Miami Beach, FL, 269–278.
Joshi, J. B. D., W. G. Aref, A. Ghafoor, and E. H. Spafford. 2001. "Security Models for Web-based Applications." *Communications of the ACM* 44 (2): 38–44.
Kahraman, G., and S. Bilgen. 2015. "A Framework for Qualitative Assessment of Domain-Specific Languages." *Software System Model* 14: 1505–1526.
Kainda, R., I. Flechais, and A. W. Roscoe. 2010. "Security and Usability: Analysis and Evaluation." ARES '10 International Conference on Availability, Reliability, and Security, Krakow, 275–282.
Kaipa, P. 2000. "Knowledge Architecture for the Twenty-First Century." *Behaviour & Information Technology* 19 (3): 153–161.
Ka-Ping, Y. 2004. "Aligning Security and Usability." *IEEE Security & Privacy Magazine* 2 (5): 48–55.
Karat, C.-M., C. Brondie, and J. Karat. 2006. "Usable Privacy and Security for Personal Information Management." *Communications of the ACM* 49 (1): 56–57.
Karray, F., M. Alemzadeh, J. Abou-Saleh, and M. N. Arab. 2008. "Human-Computer Interaction: Overview on State of the Art." *International Journal On Smart Sensing and Intelligent Systems* 1 (1): 137–159.
Kennedy, D. M. 2011. "Team Creative Processes: The Importance of Complementary and Shared Mental Models." 44th Hawaii International Conference on System Sciences (HICSS), Kauai, HI, 1–10.
Khansa, L., and D. Liginlal. 2009. "Quantifying the Benefits of Investing in Information Security." *Communications of the ACM* 52 (11): 113–118.
Khelifi, A., and W. Suryn. 2003. "Usability Meanings and Interpretations in ISO Standards." *Software Quality Journal* 11: 325–338.
Kim, S., K. Sekiyama, and T. Fukuda. 2009. "User-Adaptive Interface Based on Mental Model and Symbol Matching." IEEE/ASME International Conference on Advanced Intelligent Mechatronics, Singapore, 457–462.
Kiziloz, H., and K. Bicakci. 2015. "Towards Making Accessible Human-Interaction Proofs More Secure and Usable." 2015 IEEE Symposium on Computers and Communication (ISCC), Larnaca, 607–612.
Komlodi, A., and D. Soergel. 2002. "Attorneys Interacting with Legal Information Systems: Tools for Mental Model Building and Task Integration." *The Proceedings of the American Society For Information Science And Technology* 39 (1): 152–163.
Kwok, L.-F. 1997. "Hypertext Information Security Model for Organizations." *Information Management & Computer Security* 5 (4): 138–148.
Langan-Fox, J., C. Platania-Phung, and J. Waycott. 2006. "Effects of Advance Organizers, Mental Models and Abilities on Task and Recall Performance Using a Mobile Phone Network." *Applied Cognitive Psychology* 20: 1143–1165.
Law, E. L.-C., B. J. Blazic, and M. Pipan. 2007. "Analyses of User Rationality and System Learnability: Performing Task Variants in User Tests." *Behaviour & Information Technology* 26 (5): 421–436.
Lederer, S., J. I. Hong, A. K. Dey, and J. A. Landay. 2004. "Personal Privacy Through Understanding and Action Five Pitfalls for Designers." *Personal and Ubiquitous Computing* 8: 440–454.
Lei, T., Y. Yang, and Y. Zhang. 2006. "The Usability of Multimedia Interface Based on User's Mental Models." The 16th International Conference on Artificial Reality and Telexistence, Hangzhou, 168–173.
Li, L., E. Berki, M. Helenius, and S. Ovaska. 2014. "Towards a Contingency Approach with Whitelist- and Blacklist-based Anti-phishing Applications: What do Usability Tests Indicate?" *Behaviour & Information Technology* 33 (11): 1136–1147.
Li, C., A. Raghunathan, and N. K. Jha. 2010. "A Secure User Interface for Web Applications Running Under an Untrusted Operating System." The 10th IEEE International Conference on Computer and Information Technology (CIT 2010), Bradford, 865–870.
Liddy, C., and A. Sturgeon. 1999. "The Evolution of Certificate Model Architecture." *Information Management & Computer Security* 7 (2): 95–100.
Lin, H.-F. 2007. "Knowledge Sharing and Firm Innovation Capability: An Empirical Study." *International Journal of Manpower* 28 (3/4): 315–332.
Lindman, J., M. Rossi, and V. K. Tuunainen. 2013. "Open Data Services: Research Agenda." 46th Hawaii International Conference on System Sciences, Wailea, Maui, HI, 1239–1246.
Lineberry, S. 2007. "The Human Element: The Weakest Link in Information Security." *Journal of Accountancy* 204 (5): 44–47.
Liu, F., and X. Li. 2011. "Using Metadata to Maintain Link Integrity for Linked Data." IEEE international Conferences on Internet of Things, and Cyber, Physical and Social Computing, Dalian, 432–437.
Ma, Q., A. Johnston, and M. Pearson. 2008. "Information Security Management Objectives and Practices: A Parsimonious Framework." *Information Management & Computer Security* 16 (3): 251–270.
Mariano, S., and A. Casey. 2007. "The Process of Knowledge Retrieval: A Case Study of an American High-technology

Research, Engineering and Consulting Company." *VINE: Journal of Information and Knowledge Management Systems* 37 (3): 314–330.
McDougall, S. J. P., M. B. Curry, and O. de Bruijn. 2001. "The Effects of Visual Information on Users' Mental Models: An Evaluation of Pathfinder Analysis as a Measure of Icon Usability." *International Journal Of Cognitive Ergonomics* 5 (1): 59–84.
Metaxiotis, K., K. Ergazakis, and J. Psarras. 2005. "Exploring the World of Knowledge Management: Agreements and Disagreements in the Academic/Practitioner Community." *Journal of Knowledge Management* 9 (2): 6–18.
Mihajlov, M., Blažič, B. J., and Josimovski, S. 2011. "Quantifying Usability and Security in Authentication." 35th IEEE Annual Computer Software and Applications Conference. Munich, 626–629.
Mihajlov, M., S. Josimovski, and B. Jerman-Blazič. 2011. "A Conceptual Framework for Evaluating Usable Security in Authentication Mechanisms – Usability Perspectives." 5th International Conference on Network and System Security (NSS), 332–336.
Milne, P. 2007. "Motivation, Incentives and Organisational Culture." *Journal of Knowledge Management* 11 (6): 28–38.
Mitrakas, A. 2006. "Information Security and Law in Europe: Risks Checked?" *Information & Communications Technology Law* 15 (1): 33–53.
Mohamed, M. S. 2008. "The "Continuumization" of Knowledge Management Technology." *VINE: The Journal of Information and Knowledge Management Systems* 38 (2): 167–173.
Molich, R., and J. Nielsen. 1990. "Improving a Human-Computer Dialogue." *Communications of the ACM* 33 (3): 338–348.
Moody, J., J. E. Blanton, and M. A. Augustine. 1996. "Enhancing End-User Mental Models of Computer Systems through the Use of Animation." The 29th Annual Hawaii International Conference on System Sciences, Wailea, HI, 299–307.
Moraga, M. A., C. Calero, M. Piattini, and O. Diaz. 2007. "Improving a Portlet Usability Model." *Software Quality Journal* 15: 155–177.
Mylonakis, J., and M. Malioukis. 2010. "Identifying and Managing Enterprise Security Risks in Online Business Convergence Environments." *Business Management & Strategy* 1 (1): 1–8.
Nielsen, J. 1989. "What do Users Really Want?" *Internaional Journal of Human-Computer Interaction* 1 (2): 137–147.
Nielsen, J. 1990a. "A Meta-Model for Interacting with Computers." *Interacting with Computers* 2 (2): 147–160.
Nielsen, J. 1990b. "Traditional Dialogue Design Applied to Modern User Interfaces." *Communications of the ACM* 33 (10): 109–118.
Nielsen, J. 1992. "The Usability Engineering Life Cycle." *IEEE Computer* 25 (3): 12–22.
Nielsen, J. 1993. "Iterative User Interface Design." *IEEE Computer* 26 (11): 32–41.
Nielsen, J. 1994. "Enhancing the Explanatory Power of Usability Heuristics." Proceedings of the CHI'94 Conference, Boston, MA, 152–158.
Nielsen, J. 1997. "The Use and Misuse of Focus Groups." *IEEE Software* 14 (1): 94–95.
Nielsen, J., and J. Levy. 1994. "Measuring Usability – Preference vs. Performance." *Communications of the ACM* 37 (4): 66–75.
Nielsen, J., and V. L. Phillips. 1993. "Estimating the Relative Usability of Two Interfaces: Heuristic, Formal, and Empirical Methods Compared." Proceedings of ACM INTERCHI '93 Conference, Amsterdam, the Netherlands, 214–221.
Nonaka, I., and H. Takeuchi. 1995. *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation*. New York: Oxford University Press, xii, 284.
Olalere, A., J. H. Feng, J. Lazar, and T. Brooks. 2014. "Investigating the Effects of Sound Masking on the use of Audio CAPTCHAs." *Behaviour & Information Technology* 33 (9): 919–928.
Olaverri-Monreal, C., and J. Goncalves. 2014. "Collaborative System to Investigate Mental Models: The Information Architecture Automatic Tool (IAAT)." International Conference on Collaboration Technologies and Systems (CTS), Minneapolis, MN, 616–621.
Paivio, A. 1991. "Dual Coding Theory: Retrospect and Current Status." *Canadian Journal of Psychology/Revue Canadienne de Psychologie* 45 (3): 255–287.
Peltier, T. R. 2006. "Social Engineering: Concepts and Solutions." *Information Systems Security* 15 (5): 13–21.
Polanyi, M. 1958. *Personal Knowledge: Towards A Post-critical Philosophy*. London: Routledge and Kegan Paul.
Potter, T. C. 2012. "An Evaluation Methodology for the Usability and Security of Cloud-based File Sharing Technologies." Master of Science in Information Technology Management, Naval Postgraduate School.
Puerta-Melguizo, M. C., C. Chisalita, and G. C. Van der Veer. 2002. "Assessing Users Mental Models in Designing Complex Systems." International Conference on Systems, Man and Cybernetics, 7.
Raja, F., K. Hawkey, S. Hsu, K.-L. Wang, and K. Benznosov. 2011. "A Brick Wall, A Locked Door, and A Bandit: A Physical Security Metaphor for Firewall Warnings SOUPS." 11 Proceedings of the Seventh Symposium on Usable Privacy and Security, Pittsburgh, PA, 1–20.
Ratnasingham, P., and P. Swatman. 1997. "EDI Security: A Model of EDI Risks and Associated Controls." *Information Management & Computer Security* 5 (2): 63–71.
Renaud, K. 2003. "Quantifying the Quality of Web Authentication Mechanisms a Usability Perspective." *Journal of Web Engineering* 3 (2): 95–123.
Renaud, K., and A. De Angeli. 2004. "My Password is Here! An Investigation into Visuo-Spatial Authentication Mechanisms." *Interacting with Computers* 16 (6): 1017–1041.
Reza, S., S. Beheshti, and P. Liatsis. 2015. "How Humans Can Help Computers to Solve an Artificial Problem?" International Conference on Systems, Signals and Image Processing (IWSSIP), London, 291–294.
Richert, A. 1999. "An Evaluation of Quality Culture Problems in UK Companies." *Industrial and Commercial Training* 31 (7): 267–271.
Riedinger, J. 2008. "Using an Applied Learning Centre as a Vehicle for Culture Change." *The Journal of Information and Knowledge Management Systems* 38 (1): 95–103.
Rook, F. W., and M. L. Donnell. 1993. "Human Cognition and the Expert System Interface: Mental Models and Inference

Explanations." *IEEE Transactions On Systems, Man, And Cybernetics* 23 (9): 1649–1661.
Ruggles, R. 1998. "The State of the Notion: Knowledge Management in Practice." *California Management Review* 40 (3): 80–89.
Rukšènas, R., P. Curzon, and A. Blandford. 2008. "Modelling and Analysing Cognitive Causes of Security Breaches." *Innovations in Systems and Software Engineering* 4: 143–160.
Sae-Bae, N., N. Memon, K. Isbister, and K. Ahmed. 2014. "Multitouch Gesture-based Authentication." *IEEE Transactions On Information Forensics And Security* 4 (9): 568–583.
Sahar, F. 2013. "Tradeoffs Between Usability and Security." *IACSIT International Journal of Engineering and Technology* 5 (4): 434–437.
Saltzer, J. H., and M. D. Schroeder. 1975. "The Protection of Information in Computer Systems." *Proceedings of the IEEE* 63: 1278–1308.
Santos, O., and J. Boticario. 2015. "User-Centred Design and Educational Data Mining Support During the Recommendations Elicitation Process in Social Online Learning Environments." *Expert Systems* 32 (2): 293–311.
Sasse, M. A., S. Brostoff, and D. Weirich. 2001. "Transforming the 'Weakest Link' — A Human/Computer Interaction Approach to Usable and Effective Security." *BT Technology Journal* 19 (3): 122–131.
Schreuders, Z. C., T. J. McGill, and C. Payne. 2012. "Towards Usable Application-Oriented Access Controls: Qualitative Results from A Usability Study of SELinux, AppArmor and FBAC-LSM." *International Journal of Information Security and Privacy* 6 (1): 57–76.
Schultz, E. E., R. W. Proctor, M.-C. Lien, and G. Salvendy. 2001. "Usability and Security An Appraisal of Usability Issues in Information Security Methods." *Computers & Security* 20 (7): 620–634.
Scott, B., and D. Keyworth. 1998. "Initiating a Process Approach to Change Integration." GartnerGroup Washington, DC, USA DF-05-1855.
Scottberg, B., W. Yurcik, and D. Doss. 2002. "Internet Honeypots: Protection or Entrapment?" International Symposium on Technology and Society, 387–391.
Senge, P. M. 1990. *The Fifth Discipline: The art and Practice of the Learning Organization*. New York, NY: Doubleday/Currency.
Seyal, A. H., and R. Turner. 2013. "A Study of Executives' Use of Biometrics: An Application of Theory of Planned Behaviour Service Quality." *Behaviour & Information Technology* 32 (12): 1242–1256.
Shneiderman, B., and H. Hochheiser. 2001. "Universal Usability as a Stimulus to Advanced Interface Design." *Behaviour & Information Technology* 20 (5): 367–376.
Shum, B. 1998. "Evolving the Web for Scientific Knowledge: First Steps Towards an 'HCI Knowledge Web'." *Interfaces, British HCI Group Magazine* 39: 16–21.
Sivakorn, S., I. Polakis, and A. Keromytis. 2016. "I Am Robot: (Deep) Learning to Break Semantic Image CAPTCHAs." 2016 IEEE European Symposium on Security and Privacy, Saarbrucken, 388–403.
Skovira, R. J. 2007. "Framing the Corporate Security Problem: The Ecology of Security." *Issues in Informing Science and Information Technology* 4: 45–53.
Spicer, D. P. 1998. "Linking Mental Models and Cognitive Maps as an Aid to Organisational Learning." Career *Development International* 3 (3): 125–132.
Stary, C. 2014. "Non-disruptive Knowledge and Business Processing in Knowledge Life Cycles – Aligning Value Network Analysis to Process Management." *Journal of Knowledge Management* 18 (4): 651–686.
Stibel, J. M. 2005. "Mental Models and Online Consumer Behaviour." *Behaviour & Information Technology* 24 (2): 147–150.
Strachan, A. 1996. "Managing Transformational Change: The Learning Organization and Teamworking." *Team Performance Management* 2 (2): 32–40.
Sun, D.-W., G.-R. Chang, L.-Z. Jin, and X.-W. Wang. 2012. "Modeling a Dynamic Data Replication Strategy to Increase System Availability in Cloud Computing Environments." *Journal of Computer Science and Technology* 27 (2): 256–272.
Talhi, C., D. Mouheb, V. Lima, M. Debbabi, L. Wang, and M. Pourzandi. 2002. "Usability of Security Specification Approaches for UML Design: A Survey." *The Journal of Object Technology* 8 (6): 103–122.
Tam, L., M. Glassmana, and M. Vandenwauverb. 2010. "The Psychology of Password Management: A Tradeoff Between Security and Convenience." *Behaviour & Information Technology* 29 (3): 233–244.
Theofanos, M. 2007. "Common Industry Specification for Usability – Requirements." National Institute of Standards and Technology Washington, DC NISTIR 7432.
Thomas, D. M., and R. P. Bostrom. 2007. "The Role of A Shared Mental Model of Collaboration Technology in Facilitating Knowledge Work in Virtual Teams." The 40th Hawaii International Conference on System Sciences, Waikoloa, HI, 1–8.
Thovtrup, H., and J. Nielsen. 1991. "Assessing the Usability of a User Interface Standard." Proceedings of ACM CHI'91 Conference on Human Factors in Computing Systems New Orleans, LA, 335–341.
Ting, W. W., and D. R. Comings. 2010. "Information Assurance Metric for Assessing NIST's Monitoring Step in the Risk Management Framework." *Information Security Journal: A Global Perspective* 19: 253–262.
Tri, D. T., and T. K. Dang. 2009. "Security Visualization for Peer-to-Peer Resource Sharing Applications." *International Journal on Computer Science and Engineering* 1 (2): 47–55.
Trim, P. R. J., and Y.-I. Lee. 2008. "A Strategic Approach to Sustainable Partnership Development." *European Business Review* 20 (3): 222–239.
Trindade, D. D. F. G., C. Guimarães, D. R. Antunes, L. S. N. Garcia, R. A. L. da Silva, and S. Fernandes. 2012. "Challenges of Knowledge Management and Creation in Communities of Practice Organisations of Deaf and non-Deaf Members: Requirements for A Web Platform." *Behaviour & Information Technology* 31 (8): 799–810.
Uther, M., and H. Haley. 2008. "Back vs. Stack: Training the Correct Mental Model Affects web Browsing." *Behaviour & Information Technology* 27 (3): 211–218.
Vance, A., B. P. Lowry, and D. Eggett. 2013. "Using Accountability to Reduce Access Policy Violations in Information Systems." *Journal of Management Information Systems* 29 (4): 263–290.

Vance, C. M., and Y. Paik. 2005. "Forms of Host-Country National Learning for Enhanced MNC Absorptive Capacity." *Journal of Managerial Psychology* 20 (7): 590–606.

Van der Henst, J.-B. 2002. "Mental Model Theory Versus the Inference Rule Approach in Relational Reasoning." *Thinking and Reasoning* 8 (3): 193–203.

Van Schaik, P., D. Flynn, A. Van Werch, A. Douglass, and P. Cann. 2004. "The Acceptance of a Computerised Decision-Support System in Primary Care: A Preliminary Investigation." *Behaviour & Information Technology* 23 (5): 321–326.

Vicente, K. J. 1990. "Coherence- and Correspondence-Driven Work Domains: Implications for Systems Design: The Design of Human-Computer Systems." *Behaviour & Information Technology* 9 (6): 493–502.

Walle, B. V. d., M. Turoff, M. Chumer, R. Hiltz, R. Klashner, M. Alles, M. Vasarhelyi, and A. Kogan. 2004. "Assuring Homeland Security: Continuous Monitoring, Control & Assurance Of Emergency Preparedness." *Journal of Information Technology Theory and Application (JITTA)* 6 (3): 1–24.

Wang, A. J. A. 2005. "Information Security Models and Metrics." 43rd ACM Southeast Conference, Kennesaw, GA, 178–184.

Wang, Y., and G. Liu 2009. "Research on Relationships Model of Organization Communication Performance of the Construction Project Based on Shared Mental Model." International Conference on Information Management, Innovation Management and Industrial Engineering, Xi'an, 208–211.

Wells, J. D., and W. L. Fuerst 2000. "Domain-Oriented Interface Metaphors: Designing Web Interfaces for Effective Customer Interaction." The 33rd Hawaii International Conference on System Sciences, Maui, Hawaii, 1–10.

Westerink, J. H. D. M., B. G. M. M. Majoor, and M. D. Rama. 2000. "Interacting with Infotainment Applications: Navigation Patterns and Mental Models." *Behaviour & Information Technology* 19 (2): 97–106.

White, G. L. 2010. "The Evolution and Implementation of Global Assurance." *Issues in Information Systems* XI (1): 35–40.

Whitten, A., and J. D. Tygar. 2003. "Safe Staging for Computer Security." The Workshop on Human-Computer Interaction and Security Systems, Ft. Lauderdale, FL, 1–4.

Wilke, J., F. McInnes, M. A. Jack, and P. Littlewood. 2007. "Hidden Menu Options in Automated Human-Computer Telephone Dialogues: Dissonance in the User's Mental Model." *Behaviour & Information Technology* 26 (6): 517–534.

Willer, D., L. Rutström, L. B. Karr, M. Corra, and D. Girard. 1999. "A Web-Lab to Enhance Social Science Infrastructure: Experiments, Simulations and Archiving." *Journal of Knowledge Management* 3 (4): 276–287.

Winter, S., S. Wagner, and F. Deissenboeck. 2008. "A Comprehensive Model of Usability." *Engineering Interactive Systems: Lecture Notes in Computer Science* 4940: 106–122.

Wyatt, J. C. 2001. "Management of Explicit and Tacit Knowledge." *Journal of the Royal Society of Medicine* 94 (1): 6–9.

Xiang, C., Y. Lu, and S. Gupta. 2013. "Knowledge Sharing in Information System Development Teams: Examining the Impact of Shared Mental Model From A Social Capital Theory Perspective." *Behaviour & Information Technology* 32 (10): 1024–1040.

Xiao, L., and J. Carroll. 2007. "Fostering an Informal Learning Community of Computer Technologies at School." *Behaviour & Information Technology* 26 (1): 23–36.

Yee, K.-P. 2002. "User Interaction Design for Secure Systems." The 4th International Conference on Information and Communications Security, 278–290.

Yeratziotis, A., D. Pottas, and D. V. Greunen. 2012. "A Usable Security Heuristic Evaluation for the Online Health Social Networking Paradigm." *International Journal of Human-Computer Interaction* 29 (3): 678–694.

Zaphiris, P., B. Shneiderman, and K. L. Norman. 2002. "Expandable Indexes vs. Sequential Menus for Searching Hierarchies on the World Wide Web." *Behaviour & Information Technology* 21 (3): 201–207.

Zhang, W., and M. Kim. 2011. "Harnessing Explicit Knowledge." *Journal of Economics and Behavioral Studies* 2 (3): 97–107.

Zhang, X., and C. Shen. 2006. "Reliability Extended Security Model Combining Confidentiality and Integrity." 8th International Conference on Signal Processing, Beijing, 1–4.

Zhang, W., and P. Xu. 2011. "Do I Have to Learn Something new? Mental Models and the Acceptance of Replacement Technologies." *Behaviour & Information Technology* 30 (2): 201–211.

Zhang-Kennedy, L., S. Chiasson, and R. Biddle. 2013. "Password Advice Shouldn't be Boring: Visualizing Password Guessing Attacks." eCrime Researchers Summit, San Francisco, CA, 1–11.

Ziefle, M. 2002. "The Influence of User Expertise and Phone Complexity on Performance, Ease of use and Learnability of Different Mobile Phones." *Behaviour & Information Technology* 21 (5): 303–311.

Zurko, M. E. 2005. "User-Centered Security: Stepping Up to the Grand Challenge." Computer Security Applications Conference, 21st Annual, Tucson, AZ, 202–215.