System design considerations for risk perception.

M'MANGA, A., FAILY, S., MCALANEY, J. and WILLIAMS, C.

2017

System Design Considerations for Risk Perception

Andrew M'manga, Shamal Faily, John McAlaney
Bournemouth University
Fern Barrow, Poole, UK
{ammanga,sfaily,jmcalaney}@bournemouth.ac.uk

Christopher Williams
Defence Science and Technology Laboratory
Porton Down, UK
cwilliams@mail.dstl.gov.uk

***Abstract*—The perception of risk is a driver for security analysts' decision making. However, security analysts may have conflicting views of a risk based on personal, system and environmental factors. This difference in perception and opinion, may impact effective decision making. In this paper, we propose a model that highlights areas contributing to the perception of risk in a socio-technical environment and their implication to system design. We validate the model through the use of a hypothetical scenario, which is grounded in both the literature and empirical data.**

I. Introduction

Designing secure systems that people can use has become a multi-disciplinary concern, with contributions from areas such as Computer Security, Information Systems and Human Computer Interaction. When considering the body of work in this area, the literature has focused on two broad approaches: system-centricity, and user-centricity. System-centricity focuses on the evaluation and systems requirements in regards to usability and interfaces. User-centricity focuses on eliciting user requirements using techniques such as contextual enquiry and cognitive task analysis to improve the system and interface design [36].

Despite the growing body of literature in this area, there is a general lack of research focusing on design requirements for decision making by security analysts. A large part of a security analyst's time (work) is spent on decision making about risks (analysis and response) which have design implications crossing several areas. This encompasses user cognition, system design and the user's environment where the context of the decision is derived [34]. Few decisions are made in the absence of uncertainty and that uncertainty is a norm, not an exception [22].

An example of perception and decision making was observed in the media recently with the Microsoft Windows 10 upgrade prompt. While tradition and established beliefs dictate that the "X" on the top-right corner of a window should close the window and take no further action, clicking it provided consent to the upgrade [9]. Here, the interface design was neither too complex for the user to understand, nor were there any features beyond the comprehension of typical Windows users. The problem lay in misunderstandings between the perceived model (mental model) of the system held by the user, and the actual system model. Such situations might occur in information security operations, where the consequences are greater due to higher risk levels, and a more dynamic threat environment.

To design for decision making, the user, system and environment must all be considered. To understand the role these different elements play, this paper presents a model of risk perception within socio-technical environments. Our work contributes to security design by highlighting areas of a socio-technical environment that need to be considered when designing for decision making. We consider the related work in design and decision making in Section II before presenting our approach for building the model, and the model itself in Sections III and IV respectively. We illustrate the model using a hypothetical scenario in Section V, and discuss the implications of our model and future work in Section VI.

II. Related Work

A. Complexities of Studying Decision Making

Several researchers have examined the activities of security analysts and the decision they make. While their approaches and interests have been different, their general goal has been in understanding the perception security analysts have about risk, its various guises, and how the security analysts respond to it. The difficulties uncovering cognitive information from participants has meant that the results obtained have not always been conclusive.

Paul & Whitley [28] discuss the approach that security analysts use to gain awareness of a network by using interviews and a card sorting exercise. The drawback of presenting information to participants lies in the clarity and validity of the information. For example, the card sorting exercise asks: *"Are there more or less bad guys attacking my network than normal? What did the bad guys take?"* From the exercise, we raise the following questions:

- Who is a bad guy and how may this be defined?
- Are inside attackers classified as bad guys and how about network anomalies that result from slips, lapses and mistakes [7]?
- What was the security analysts perception of this during card sorting?

Security analysts might addresses these questions differently based on the information presented to them. Hibshi et al. [21] describe how security analysts use steps of situation awareness to perceive future threats and the way this aids in identifying security requirements. They presented participants

with security artefacts from which decisions are assessed, and comparisons were drawn between steps taken by expert and novice security analysts. There was, however, no explanation for why their findings show that experts do not follow all the expected steps of situation awareness, a finding that contradicts one of their study expectations. A possible explanation for this is considered in the decision making models in Section II-C.

B. The Security and Usability Trade-Off in Design

Designer help bridge the gap between the system and the user [25]. Given the fact that security and usability have long been considered a matter of trade-off, the designers have typically emphasised one over the other [33]. The idea of designing for risk perceptions in security illustrates that usability can actually be used to improve security. For example, Cranor & Garfinkel [11] promote the need for not treating security and usability goals as a trade-offs. Their concern was on what an agreeable definition for this would be. Work by Faily & Fléchais [16] attempted to address this problem, where the activities associated with designing secure and usable systems were their focus. They found that a large proportion of work in security and usability focussed only on the usability of security controls. To address this, they developed IRIS: a framework synthesising usability, security and requirement perspectives when specifying usable and secure systems [16]. An alternative perspective taken by [30] identified that improving usability of secure systems only solves one part of the problem; there is a still a need to design *useful*, usable and secure systems. For example, a security goal should be implicit in the application goal requiring no extra effort from the user. Of these different approaches to security and usability, none have considered the role and implications of decision making for security.

C. Decision Making Models

A common approach to understanding perception has been to determine one's situation awareness under conditions of risk and uncertainty. Situation awareness can be explained as one's knowing of what is going on to determine what to do next. There are several models used for situation awareness; these are unrelated and have slight variations in their definition of situation awareness but share common aspects. Azuma et al [3] divide decision making models into two categories: Rational and Naturalistic.

Rational models are procedural, and follow predefined orders during decision making. They assume that the decision maker will collect sufficient information and have a clear set of options to select from. Questions are typically asked, such as "what are the objectives" and "Compare and evaluate the alternatives". Two prominent examples of these are the Observe Orient Decide Act (OODA) model [6] and Endsley's situation Awareness Model [15].

Naturalistic models are action based, and do not depend on information gathering. The decision maker tries the first action they believe to be the most suitable based on their experience on previous incidents. If the action fails, the decision maker notes the failure, and reacts based on the observation. A prominent example of this is the Recognition Primed Decision Making (RPDM) model [23]. There is no evidence that one class of models is better than the other, but both are applicable in certain environments.

III. Approach

Our study is based on a multidisciplinary literature review that correlates the findings of research areas such as human cognition, HCI-Security, and Human Computer Interaction. We then collected empirical data by carrying out seven interviews with security analysts from two different organisations. We analysed the transcripts from these interviews to verify and validate our literature-based model. More detail on the analysis and findings from this interview study will be the subject of future work.

Our approach to the model development is inspired by Endsley's situation awareness [15]. We found this to be suitable due to its focus on factors in a socio-technical environment, as opposed to a sole focus on cognitive processes. It is important to define the environment in which the situation in question evolves [34].

IV. The Model

The model highlights areas that contribute to the perception of risk, and how these may be considered in system design. The model is divided into the three domains - *User*, *System*, and *Context*. Each domain consists of attributes that influence perception in the domain.

Our approach for selecting the domains was that a domain should be a central part that dictates the relationship of the attributes. This reasoning led to the selection of *Context* as a domain over *Environment*. As we illustrate in Section IV-C, it is the Context that has a direct and transitive relationship with the attributes of the domain and not Environment.

To illustrate the relationships and dependencies, the models are presented as UML class diagrams [24].

A. System Domain

A System aids security analysts in achieving their goals through task automation [27]. To do this, systems interact with the analysts through various levels of abstraction and provides cues to aid and improve the user's experience [14]. A system also provides sufficient and timely feedback to user actions. [25].

The following are areas identified where a security analyst's perception may be affected as a result of system design. The interrelationship among the *System* domain and its attributes is illustrated in Figure 1.

- **Automation**
  Security automation is defined as any system or technology that effectively removes the security decision process from the user [14]. The paradox of system automation is that although it shields users from making complex decisions through abstraction and simplifications, it also creates complications. Over-reliance on automation may

influence user perceptions and affect decision making. This is evident in situations where users take all automated information at face value, and lose the propensity for analysis where false positive could be discovered. Over dependence on automation may also lead to skill degradation, and "out-of-the-loop unfamiliarity" [27] incapacitating security analysts when systems fail or are incomprehensible. In other situations, automation is put in place where a user is incapable; the skills gap between the user and the systems also affects the users perception and understanding [4].

- **Interface**
  An interface is a medium for communication between systems and users. As a bridge for communication, an interface can affect user perceptions based on *functional* (feedback and affordance) or *non-functional* (complexity and ambiguity) aspects of its design. Examples of the two have been described below.
  - **Feedback**: when a user interacts with a system, feedback is expected when actions are executing or completed. The lack of feedback may wrongly signify no change in state or successful execution, impeding the user from carrying out a follow up action or diagnosing a situation accurately. This is known as the "gulf of evaluation" [25].
  - **Affordance**: An affordance is the possibility of an action on an object [18]. Originally coined by Gibson [18], affordances exist whether a user perceives them or not. Norman later introduced the notion of *perceived* affordances [25]. These are properties perceived to be actionable. For example, all computer screens can afford touching but only touch-sensitive screens will detect and respond [26]. Perceived affordance would be the user's ability to discern the touch-sensitive capabilities of a screen. The device must, however, be designed to hint towards this. The lack of affordances on a device is known as the "gulf of execution" [25]
  - **Complexity**: System interfaces may have many components for user interaction and configuration such as menus and sub-menus. As security mechanisms grow in complexity, so does usability [5].
  - **Ambiguity**: A system could have interface designs with low complexity and sufficient cues, but still present perception and usability problems. Ambiguous interfaces are a result of the inappropriate, inexplicit and inconsistent use of interface objects. Clarity is a prerequisite for good decision making [35].

B. User Domain

It has long been claimed that humans are the weakest link in socio-technical environment [2]. To attend to this, systems should be designed to be useful to both the expert and non-expert user [10]. The understanding of cognitive shortfalls is the first step towards solving the problem. We identify Mental Models, Heuristics and Biases as three cognitive factors that contribute to the perception of risk.

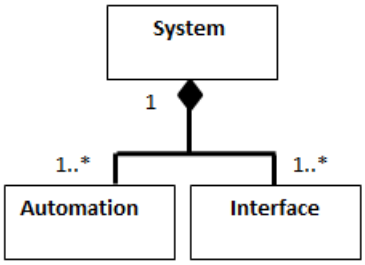

Fig. 1. System Domain

- **Mental Models**
  Mental models are a human way of understanding unfamiliarity, and a product of ones knowledge and beliefs [8]. Mental models may be defined as conceptual models in peoples minds that represent their understanding of how systems work (not limited to technical systems). Mental models are dynamic and constantly evolve as new knowledge is acquired [17].
  Mental models may generally be grouped into two groups. The first is task-based where the system user has no theory on how the system functions or its internal workings. Here the user mostly operates through memorised sequences based on beliefs. The second is based on knowledge of a systems workings and the understanding of system components, processes and their relation [8]. The designer should strive to design systems where the second group of mental models are attainable. Mental models can either be correct or incorrect. Poorly conceived mental models are products of low experience, lack of technical know-how and the factors covered in section IV-A . Incorrect mental models that work in a certain context of use may sometimes never be detected if the context remains unchanged [17].

- **Heuristics**
  Unlike the mental models, which are one's assumptions and beliefs of how things work, heuristics are mental short cuts one subconsciously takes to solve problems quickly. For example, Werlinger et al [32] report that security analysts identify attack activity just by spotting Internet Relay Chat (IRC) traffic on a network. IRC is not a signal of an attack but is in this case, guilty through association due to its popularity amongst hackers. In the event that IRC was used by a legitimate user, the security analysts would wrongly assume an attack was taking place. There is a broad range of identifiable heuristics, an area thoroughly covered by [31]. For example the availability heuristic refers to the fact that people will tend to think something is more likely to happen if they can easily visualise it. This heuristic could lead security analysts to think that the attack types they are more familiar with through personal experience or which have

been in the news are more likely to happen, because it is easier to visualise one of those attacks taking place. This means they will also tend to underestimate the risk of any attack types that they have less experience with. The dependency on incorrect heuristics leads to what are know as biases [1].

- **Biases**
  Biases have many origins such as incorrect mental models, incorrect heuristics, culture and background. One example important to system design is the framing bias. Envision an intrusion detection system (IDS) that reports 40% of incoming traffic as malicious to one that reports 60% of incoming traffic as non-malicious. The two are identical, but a security analyst's interpretation of each may be different, affecting the decision made [20]. An alternative argument is that biases are not a problem as such, but a necessary evil that protects us from bigger problems. With respect to the examples above, they would say that it is better to wrongly assume an attack is imminent than to ignore an actual one [22].

Figure 2 illustrates the relationships between User cognitive attributes.

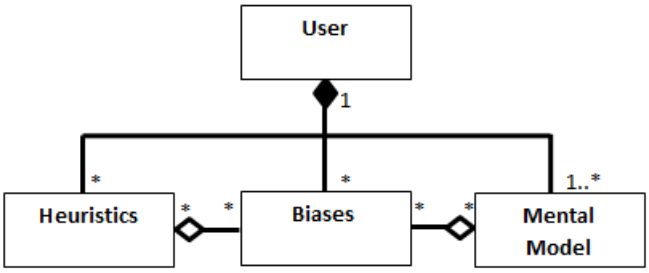

Fig. 2. User Domain

C. Context Domain

The System and User domain's focii are concerned with perceptions particular to them. However, the Context domain bridges the other two. Context is defined as "information that can be used to characterise the situation of an entity"[13]. In this case, the entity is a system user. We can further elaborate by saying that context is how a user perceives the environment and all other interactions, and the user has control over context. The relationship between Context and its attributes is illustrated in Figure 3. We identify Correlation, State, Intelligence and Environment as the factors that contribute to the perception of risk.

1) Correlation: Correlation is one of the two system to user relationships, based on context. We define correlation as the requirement to perceive multiple pieces of information from a system to create a full picture and understanding of events. In terms of the system, this is the need to provide the multiple pieces of information required for understanding. A security analyst rarely relies on one piece of information to fully understand a situation [12]. For example, the results from a vulnerability scan indicating that vulnerabilities exist on a system may require additional checks for false positives. These could be verifications with patch management tools. If a system can make provisions for the two and correlate the data, the perception of events and decision making would be simplified. Correlation also involves the need to perceive competing information. For example, how will the security analysts decide which alert to pay attention to on a busy network? And what are the filters a system should provide to control this? [29].

2) State: State is the second system to user relationship, based on context. State is a system's ability to present an up-to-date position in time [29]. From a security analyst's point of view, this pertains to an ever-changing threat landscape as new attacks and zero days are discovered. However this does not mean systems should continuously provide live updates to users, but that a current state should be accessible on demand if an informed decision is to be made.

3) Intelligence: Intelligence is the composition of all information that does not originate from a system that helps define the context of a situation. Intelligence may include threat alerts, zero-day discoveries, and all other threat and vulnerability-related information. Though not from the system, the use of intelligence helps contextualise the threat landscape to improve the security analyst's decision making. We found the term "intelligence" more suitable than "threat intelligence", which is widely used in information security, because the data requirements for decision making cover more than threats alone. We also identified that the term "information" was unsuitable based on its lack of value in problem solving. Intelligence is an element of value and an enabler that can be applied to problem solving. Information, on the other hand, is processed data but may be inapplicable to a problem [19]. From the three prominent decision making models mentioned in Section II-C , it is only OODA that appears to consider the use of outside information (intelligence) for decision making.

4) Environment: An environment is where the user operates; it is dynamic and shaped by external factors. The environment is independent of the user and the system. The user does not control the environment but the environment influences both the user and the system.

V. Hypothetical Scenario

We now present a hypothetical scenario used to illustrate our model. The scenario was grounded in empirical data collected from interviews, and our review of the literature. The scenario was validated by one of the security analysts interviewed. Risk perception considerations from the model identified in this scenario are highlighted in brackets.

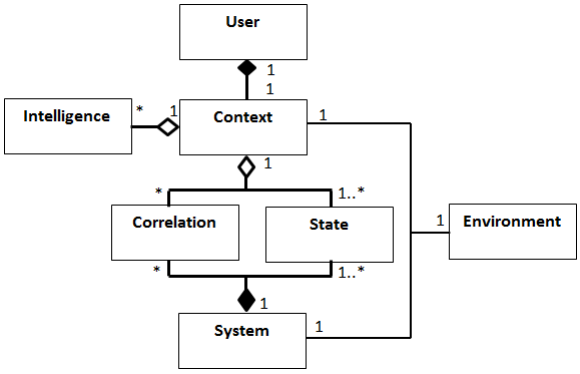

Fig. 3. Context Domain

Sally is a security analyst for Dynamics Ltd in London, UK. Her role is to monitor, identify and remediate threats and vulnerabilities on her organisation's network. Dynamics has approximately 50 staff members, with a team of 3 in IT. The organisation is run by Sam the managing director, who has a secretary, Tilly.

Sally notices an unusually prolonged increase in network traffic around midday *(State)*. Given her 2 years in the organisation, she identifies this as an anomaly *(Heuristic)*. Sam is normally out for lunch at that time *(Environment)*. Sally monitors the logs on Dynamics' IDS, and analyses the network traffic on their network monitoring tool *(Correlation)*. She identifies that the traffic uses an RTSP protocol on port 554, and is destined for Sams IP address. This is the connection used for video conferencing, but the source IP address is not from the regular connections.

A check on other logs *(Correlation)* shows Sam logged onto the network two hours before his regular time. When Sam is out for lunch, Tilly usually connects to Facebook *(Environment/Heuristic)*. Sally scans for Facebook traffic on Tillys IP address and identifies that Tilly is connected to Facebook. Given the situation, Sallys experience and her network events expectations *(Mental model)*, Sam is most likely out of the office and an attack could be in progress *(Possible bias)*. Sally has the option to terminate the connection but she chooses not to go with her gut feeling and seek further confirmation by calling Tilly. Tilly confirms that Sam is in and that he had started the day early to prepare for a video conference meeting with their new partners in New York. The nature of the meeting did not require Tillys assistance, so she continued her lunch break, and interaction with social media *(Intelligence)*.

If Sally had followed her assumption based on heuristics and mental models, Sam meeting could have come to an abrupt end. Had the system also not provided up to date and multiple pieces of information, Sally would never have questioned the scenario in the event of a real attack. Fortunately for Dynamics, the findings of the scenario were false positives.

VI. Discussion and Conclusions

In this paper, we presented a model that illustrates the contribution of different factors in a socio-technical environment to risk perception. This model highlight relationships and dependencies between domains, and also defined *context* as a novel way of modelling the relationship between a user, system and environment.

Our work producing the model identified a broad spectrum of work touching different research areas. We demonstrated the importance of considering these areas in design through the use of a common model. Unlike previous literature that has looked at decision making in a process-oriented manner (e.g steps of situation awareness), we followed a distributed approach with a focus on the parts of a socio-technical environment. In each section, we provided recommendations or implications to design by highlight areas for consideration when designing for decision making in an environment where risk and uncertainty are present.

The premise behind the validation of the model using a hypothetical scenario lies in the diverse number of possibilities the model presents that cannot be validated in a short period of time. This is also evident in the scenario where the systems domain was not covered as it would have required more characters and a longer script that would have been unrealistic.

As alluded to in Section I, the model highlights areas leading to the perception of risk. The model highlights these areas at a high level with perception as a first class object. A challenge we faced in building our model was the accessibility of security analysts, and restrictions studying their decision making processes. As a part of future work, we will collect additional data, and further examine each domain and their interrelationships. This will both strengthen the validity of our model, and identify low level principles that can establish design requirements.

Acknowledgments

The research was funded by Bournemouth University studentship DSTLX1000104780R_BOURNEMOUTH_PhD_RBDM. We are grateful to DSTL for their sponsorship of this work.

References

[1] A Tversky and D Kahneman, *Judgment under uncertainty: Heuristics and biases*. Springer, 1975.

[2] A. Adams and M. A. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, 1999.

[3] R. Azuma, M. Daily, and C. Furmanski, "A review of time critical decision making models and human cognitive processes," in *Aerospace Conference, 2006 IEEE*. IEEE, 2006, pp. 9–pp.

[4] L. Bainbridge, "Ironies of automation," *Automatica*, vol. 19, no. 6, pp. 775–779, 1983.

[5] M. Bishop, *Psychological acceptability revisited. In Security and Usability: Designing Secure Systems that People Can Use. Edited by L. Cranor and S. Garfinkel*. OReilly, 2005.

[6] J. Boyd, "The essence of winning and losing," *Unpublished lecture notes*, vol. 12, no. 23, pp. 123–125, 1996.

[7] S. Brostoff and M. A. Sasse, "Safe and sound: a safety-critical approach to security," in *Proceedings of the 2001 workshop on New security paradigms*. ACM, 2001, pp. 41–50.

[8] J. M. Carroll, N. S. Anderson, J. R. Olson, and others, *Mental models in human-computer interaction: Research issues about what the user of software knows*. National Academies, 1987, no. 12.

[9] B. Chacos, *How Microsoft's tricky new Windows 10 pop-up deceives you into upgrading*, May 2016. [Online]. Available: http://www.pcworld.com/article/3073457/windows/how-microsofts-nasty-new-windows-10-pop-up-tricks-you-into-upgrading.html

[10] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Even experts deserve usable security: Design guidelines for security management systems," in *SOUPS Workshop on Usable IT Security Management (USM)*. Citeseer, 2007, pp. 1–4.

[11] L. F. Cranor and S. Garfinkel, *Security and usability: designing secure systems that people can use*. " O'Reilly Media, Inc.", 2005.

[12] A. D'Amico, K. Whitley, D. Tesone, B. O'Brien, and E. Roth, "Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts," in *Proceedings of the human factors and ergonomics society annual meeting*, vol. 49. SAGE Publications Sage CA: Los Angeles, CA, 2005, pp. 229–233.

[13] A. K. Dey, "Understanding and using context," *Personal and ubiquitous computing*, vol. 5, no. 1, pp. 4–7, 2001.

[14] W. K. Edwards, E. S. Poole, and J. Stoll, "Security automation considered harmful?" in *Proceedings of the 2007 Workshop on New Security Paradigms*. ACM, 2008, pp. 33–42.

[15] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 37, no. 1, pp. 32–64, 1995.

[16] S. Faily and I. Flchais, "A meta-model for usable secure requirements engineering," in *Proceedings of the 2010 ICSE Workshop on Software Engineering for Secure Systems*. ACM, 2010, pp. 29–35.

[17] D. Gentner, "Mental Models, Psychology of," in *International Encyclopedia of the Social & Behavioral Sciences*. Elsevier, 2001, pp. 9683–9687.

[18] J. J. Gibson, *The ecological approach to visual perception*, 17th ed. New York: Psychology Press, 2011, oCLC: 838999303.

[19] J. Goldfarb, *What is the Difference Between Information and Intelligence? \textbar SecurityWeek.Com*, Jun. 2016. [Online]. Available: http://www.securityweek.com/what-difference-between-information-and-intelligence

[20] C. Gonzalez, J. Dana, H. Koshino, and M. Just, "The framing effect and risky decisions: Examining cognitive functions with fMRI," *Journal of economic psychology*, vol. 26, no. 1, pp. 1–20, 2005.

[21] H. Hibshi, T. Breaux, M. Riaz, and L. Williams, "Towards a framework to measure security expertise in requirements analysis," in *Evolving Security and Privacy Requirements Engineering (ESPRE), 2014 IEEE 1st Workshop on*. IEEE, 2014, pp. 13–18.

[22] D. D. Johnson, D. T. Blumstein, J. H. Fowler, and M. G. Haselton, "The evolution of error: Error management, cognitive constraints, and adaptive decision-making biases," *Trends in ecology & evolution*, vol. 28, no. 8, pp. 474–481, 2013.

[23] G. A. Klein, *Decision making in action: models and methods*. Norwood, N.J.: Ablex Pub., 1993.

[24] R. Miles and K. Hamilton, *Learning UML 2.0*, 1st ed. Beijing ; Sebastopol, CA: O'Reilly, 2006.

[25] D. Norman, *The design of everyday things: Revised and expanded edition*. Basic books, 2013.

[26] D. A. Norman, "Affordance, conventions, and design," *interactions*, vol. 6, no. 3, pp. 38–43, 1999.

[27] R. Parasuraman, T. B. Sheridan, and C. D. Wickens, "A model for types and levels of human interaction with automation," *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*, vol. 30, no. 3, pp. 286–297, 2000.

[28] C. L. Paul and K. Whitley, "A taxonomy of cyber awareness questions for the user-centered design of cyber situation awareness," in *Human aspects of information security, privacy, and trust*. Springer, 2013, pp. 145–154.

[29] N. B. Sarter and D. D. Woods, "Situation awareness: A critical but ill-defined phenomenon," *The International Journal of Aviation Psychology*, vol. 1, no. 1, pp. 45–57, 1991.

[30] D. K. Smetters and R. E. Grinter, "Moving from the design of usable security technologies to the design of useful secure applications," in *Proceedings of the 2002 workshop on New security paradigms*. ACM, 2002, pp. 82–89.

[31] A. Tversky and D. Kahneman, "Availability: A heuristic for judging frequency and probability," *Cognitive psychology*, vol. 5, no. 2, pp. 207–232, 1973.

[32] R. Werlinger, K. Hawkey, and K. Beznosov, "Security practitioners in context: their activities and interactions," in *CHI'08 Extended Abstracts on Human Factors in Computing Systems*. ACM, 2008, pp. 3789–3794.

[33] A. Whitten and J. D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." in *Usenix Security*, vol. 1999, 1999.

[34] C. D. Wickens, "The trade-off of design for routine and unexpected performance: Implications of situation awareness," *Situation awareness analysis and measurement*, pp. 211–225, 2000.

[35] K.-P. Yee, "User interaction design for secure systems," in *International Conference on Information and Communications Security*. Springer, 2002, pp. 278–290.

[36] M. E. Zurko and R. T. Simon, "User-centered security," in *Proceedings of the 1996 workshop on New security paradigms*. ACM, 1996, pp. 27–33.