Designing Systems for Risk Based Decision Making

Andrew M'manga
Department of Computing and Informatics
Bournemouth University
Fern Barrow, Poole
Dorset, BH12 5BB
UK
ammanga@bournemouth.ac.uk

A common challenge security analysts face, is in making decisions on risk when facing uncertain conditions especially when risk management procedures are inapplicable. Though analysts may have experience and their intuition to depend upon, these have sometimes proven to be insufficient and it has also been identified that risk and uncertainty may be magnified by personal, system and environmental factors. Risk decision making is an integral part of security analysis, a role facilitated by system automation and design. However, designing for usable security has not sufficiently considered the implications of design to risk based decision making and more so in relation to security analysts. The research aims to address this by coming up with recommendations for design, for risk based decision making.

Information Security, Risk Analysis, User Centered Design, Human Cognition

1. BACKGROUND

Risk is often perceived as a source of fear and something to be transferred or mitigated as quickly as possible. Designing for security and usability means considering risk as early as possible and providing assurance that different design options are understood by the users and provide confidence that certain risks are being addressed.

Traditionally, risk management has followed sets of predefined procedures that weigh risk response alternatives and aim at identifying the most suitable option. However, actual risk analysis rarely follows such structural and well-defined procedures as decision makers encounter uncertainties resulting from unforeseen and evolving conditions. Decision makers, therefore, result in addressing these conditions based on their knowledge and intuition (Klein, 2011). Concerns are raised as research has shown that decision making is not always a rational process, a problem magnified by the lack of guiding procedures, and even experts have shortcomings that contribute to erroneous choice (Fischhoff, 1979). To illustrate, the identification of false positives from vulnerability scanners comes with experience and the contextual understanding of events in a system environment. However, systems that could amalgamate disparate data sources and present interfaces for contextual analysis (e.g. identifying a firewall protecting vulnerable applications), could ease false positive identification, improve decision making and reduce experience requirements.

To identify how risk based decision making may be improved through design; we investigate the activities of security analysts as an exemplar of decision makers due to the tangible and visible constraints they encounter. Security analysts oversee systems security infrastructures by enforcing and maintaining security goals. Their role is crucial in areas where automation cannot fully be applied and human intervention is necessary (human in the loop). While human assistance is a prerequisite, it is the mutual relationship achieved through human-computer interaction that elevates awareness and decision making. Failure in risk decision making by those charged with enforcing security may pose a great risk as it would violate security objectives and could be difficult to detect. For example, Internet Relay Chat (IRC) use is synonymous with attackers (Werlinger et al., 2010). But does the presence of IRC on a network signify an attack? What information

should be made available to validate this and enable rapid and effective responses?

Requirements to facilitate risk decision making have mostly been proposed as secondary contribution to research on usability requirements from system-centric (Yee, 2002, Smetters and Grinter, 2002) and user-centric positions (Zurko and Simon, 1996, Wixon et al., 1990). System-centricity focuses on the evaluation of systems requirements in regards to usability and interfaces, while user-centricity focuses on eliciting user requirements using techniques such as contextual design and cognitive task analysis to improve system and interface design.

Examples of work at the early stages of design on requirements and decision making has sought to understand the influence of analogies to design (Hassard, 2011), the procedures taken for security requirements prioritisation (Butler, 2003), and the identification of techniques for making security requirements relatable to the business (Coles-Kemp and Overill, 2007). However, the factors to be taken into account, to facilitate risk based decision making have not really been considered.

2. RESEARCH OBJECTIVE AND AIMS

2.1. Objective

The objective of this research is to identify what system design principles should be taken into account to facilitate decision making during risk and uncertainty.

With an aim of understanding decision making from a socio-technical perspective, we divide the research objective into the following three aims:

- To identify the factors that contribute to risk perceptions held by cyber security risk based decision makers.
- To identify the factors that promote or constrain decision making on risk by cyber security risk based decision makers.
- To devise techniques used to elicit, specify and validate requirements for systems with cyber security risk based decision makers as stakeholders.

2.2. Thesis

The thesis is a framework for integrating system-centric and user-centric requirements to design systems for risk based decision making.

3. KEY LITERATURE

The literature review will be based on three areas pertinent to risk based decision making in security. These are; security and risk, human cognition, and system design. To better understand the analyst's activities leading to decision making, we will consider the literature addressing them in security.

3.1. Security and risk

Security is synonymous with risk. This, therefore, implies that research on security typically addresses risk, though not always stated. Additionally, risk is perceived differently at personal and organisational levels (Adams, 1995, Schneier, 2008). Understanding the techniques analysts use to make decisions on risk is a step towards understanding how to design for them. Li et al. (2010) surveyed the handling of uncertainty and risk management in cyber security. They highlight that risk and uncertainty are products of internal and external factors. They illustrate this by classifying risk uncertainty as static - originating from flaws in system design or as dynamic - the product of external and dynamic real-time events, such as attacks.

Focussing on the internal design or static aspect of risk, others have investigated techniques analysts use to specify requirements. For example, Butler and Fischbeck (2002) argue that conventional risk assessment techniques are inadequate in directing which security requirements should be implemented when resources are limited. They propose a framework for quantitatively prioritising requirements. Hibshi (2015) investigates how security analysts use their experience to come up with security requirements, while Hassard et al. (2009) investigates the persistence of analogies in decision making during design.

The body of work on the external or dynamic aspects of risk and uncertainty has covered areas such as; Awareness (Paul and Whitley, 2013, Botta et al., 2011), Security Tools (Botta et al., 2007, Xiao et al., 2014), and Security Operations (D'Amico et al., 2005, Werlinger et al., 2010).

Although analyst's decision making has widely been researched from an internal and external risk and uncertainty point of view, there has been little focus on how the analysts may be aided in risk decision making through design recommendations.

3.2. Human cognition

Work on human cognition plays a vital part in research on decision making as it explains the logic behind choice. Risk is a probabilistic subject and the assumption has been that decisions are made by

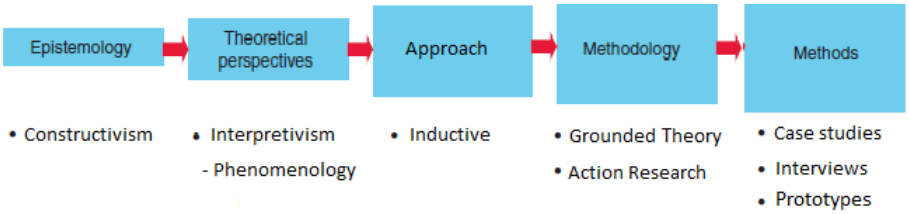

Figure 1: *Methodology*

carefully weighing alternatives. However, research on human cognition has shown that the weighing of alternatives may sometimes be prone to cognitive errors (Fischhoff, 1979), or decisions may be made intuitively without weighing alternatives (Klein, 1993). As it pertains to the analysts, the reasoning behind prompt reactions to certain risks over similar ones may be investigated and understood through cognitive analysis techniques.

Central to the notion of cognitive error in decision making are heuristics and biases (Tversky and Kahneman, 1973). Heuristics are mental shortcuts people subconsciously make when faced with uncertainty and time limitations. These shortcuts are used to quickly validate perceived assumptions by matching the limited available data against known facts. However, factors such as inaccurate perception lead to inaccurate heuristics and therefore, incorrect decisions. The constant reliance on incorrect heuristics leads to what are known as biases (Tversky and Kahneman, 1974). Due to the lab based nature of research on heuristics and biases, questions have been raised about their validity and applicability to real-world settings (Gigerenzer, 1991).

3.3. System design

As alluded to in section 1, designing for security and usability means considering risk as early as possible and providing assurance that different design options are understood by the users. To relate this to security analysts and decision making on risks, it entails considering the implications of security requirements at design and ensuring proposed models and designs are understandable and correspond to user mental models (Norman, 1983). Mental models are defined as mental representations of domains of understanding that support reasoning and prediction (Gentner, 2001). However, usability still raises the question of whether systems should be designed to match the user's mental models, be simplistic to ease understanding or place the responsibility of learning on the user (Carroll et al., 1987).

User-centered security addresses this situation and is described by Zurko and Simon (1996) as security models, mechanisms, systems, and software that have usability as a primary motivation or goal. Zurko and Simon proposed three methods to achieving usable security, namely; applying usability techniques to secure systems, developing security mechanisms for user-friendly systems, and considering user needs as a primary motivator when considering security requirements at the start of system development. The latter being the most appropriate, in this case.

Considering users at design also implies identifying techniques adequately capable of eliciting and specifying these requirements. Though there are various elicitation techniques complementing conventional interviews such as; Contextual Design (Wixon et al., 1990), Critical Decision Method (Klein et al., 1989), Cognitive Work Analysis (Rasmussen, 1986) and specification techniques such as; Problem Frames (Jackson, 2001), UML (Miles and Hamilton, 2006). The essence lies in identifying techniques that do not only focus on testing existing systems, but that are also workable before system implementation.

4. RESEARCH METHODOLOGY AND APPROACH

From a theoretical perspective, the research aims to follow a qualitative interpretivist approach (Crotty, 1998, Gray, 2013). At a lower level, this will first be an inductive Grounded Theory approach aimed at understanding the problem domain, and an Action Research approach, aimed at formulating solutions to identified problems. These approaches avoid proposing a hypothesis early in the research but allow it to be generated from empirical evidence. We propose these approaches to learn from the environment and avoid restricting the work by binding it to an early hypothesis. Figure 1 illustrates the detailed methodological approach.

In respect to the three aims, the research will follow the following phases.

In the first phase, literature will be reviewed covering the three main literature areas highlighted in section 3. Based on the findings, factors that contribute to awareness and the perception of risk will be identified and modelled in accordance to their interrelation in a socio-technical environment.

In the second phase, interviews will be carried out with security analysts to identify the steps analysts take in risk analysis, the factors that promote decision making during risk analysis and the constraints that inhibit it. Grounded Theory (Corbin and Strauss, 2008) will then be used for data analysis and Distributed Cognition (Hollan et al., 2000) for modelling the relationships between the analysts and artefacts used in decision making. At this point, the literature based findings from phase one will also be validated by the empirical data.

Based on the findings and lessons learned from the first two phases, elicitation and specification techniques for design to facilitate risk based decision making will be devised in the third phase. This will involve contextually analysing user understanding and objectives during risk based decision making through the use of Goal-Directed Design (Cooper et al., 2014), where techniques such as; Personas, Scenarios (Cooper, 2004) and goal models (Yu, 2011) will be used. To ease the application and use of the formulated techniques, tool support will be designed in the form of prototypes or integration will be made with frameworks such as IRIS (Faily, 2011) that support contextual design.

To validate the techniques, they will be applied to a minimum of three case studies using Action Research, a five-step methodology (1.Diagnosing 2.Action planning 3.Action Taking 4.Evaluating 5.Specifying Learning) that applies interventions to diagnosed problem situations (Baskerville, 1999). Where systems have been implemented, the objective will be to validate the techniques in comparison with the existing system. Where systems have not been implemented, the objective will be to elicit and specify requirements. Feedback, validation and modifications will be considered as part of the Evaluation and Specifying Learning phases of Action Research. The case studies will aim at validating both the prototype and the formulated techniques.

5. INITIAL RESULTS

Having conducted ten interviews with security analysts from three different organisations, we identified areas from a system perspective (Automation and Interface Design), and areas from the user perspective (Mental Models, Heuristics and Biases) that contribute to risk perceptions. We also identified that central to the perception of risk is Context. We have defined the followings as the elements of Context in risk based decision making: Intelligence, Environment, Correlation and State. These are illustrated in figure 2 and elaborated in M'manga et al. (2017)

We also identified that the factors that aid the analysts in risk analysis and decision making are Communication, Awareness, Individuals Capabilities (experience and training) and System Capabilities (ease of use and analytical abilities). Lastly, we identified that the main constraints to decision making by security analysts are conflicts in objectives originating from goal conflicts. For example, an organisation may establish a policy that all communications with external parties should be encrypted. However, a goal conflict arises when there is a need to communicate with an external party lacking encryption capabilities.

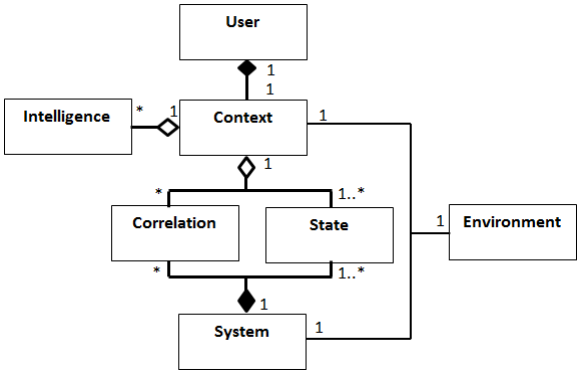

Figure 2: *Context model*

6. MAIN CONTRIBUTIONS

As an overall, the research aims to provide a framework to better enable design for risk based decision making.

The research will also contribute to tool support through prototyping and the integration with existing usable security frameworks such as IRIS.

Lastly, the research will provide common ground for the analysis and understanding of decision makers, and insight into their operations of security analysts through case studies and interview data.

7. PERSONAL BIO

Andrew is a security by design doctoral researcher under the cyber security research group at Bournemouth University. He worked as an information technology (IT) auditor for seven years before joining the University of Bradford for a Masters degree in cyber security in 2014 and Bournemouth University for a PhD in 2016. At Bournemouth, he coordinates the cyber security reading group.

REFERENCES

Adams, J. (1995). *Risk*. London [England] : Bristol, PA: UCL Press.

Baskerville, R. L. (1999). Investigating information systems with action research. *Communications of the AIS 2*(3es), 4.

Botta, D., K. Muldner, K. Hawkey, and K. Beznosov (2011). Toward understanding distributed cognition in IT security management: the role of cues and norms. *Cognition, Technology & Work 13*(2), 121–134.

Botta, D., R. Werlinger, A. Gagn, K. Beznosov, L. Iverson, S. Fels, and B. Fisher (2007). Towards understanding IT security professionals and their tools. In *Proceedings of the 3rd symposium on Usable privacy and security*, pp. 100–111. ACM.

Butler, S. A. (2003). *Security attribute evaluation method*. Ph. D. thesis, Carnegie Mellon University Pittsburgh, PA.

Butler, S. A. and P. Fischbeck (2002). Multi-attribute risk assessment. In *Symposium on Requirements Engineering for Information Security*.

Carroll, J. M., N. S. Anderson, J. R. Olson, and others (1987). *Mental models in human-computer interaction: Research issues about what the user of software knows*. Number 12. National Academies.

Coles-Kemp, L. and R. E. Overill (2007). On the role of the facilitator in information security risk assessment. *Journal in Computer Virology 3*(2), 143–148.

Cooper, A. (2004). *The inmates are running the asylum*. Indianapolis, IN: Sams.

Cooper, A., R. Reimann, D. Cronin, and C. Noessel (2014). *About face: The essentials of interaction design*. John Wiley & Sons.

Corbin, J. M. and A. L. Strauss (2008). *Basics of qualitative research: techniques and procedures for developing grounded theory* (3rd ed ed.). Los Angeles, Calif: Sage Publications, Inc.

Crotty, M. (1998). *The foundations of social research: meaning and perspective in the research process*. London ; Thousand Oaks, Calif: Sage Publications.

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

Faily, S. (2011). *A framework of usable and secure system design*. Ph. D. thesis.

Fischhoff, B. (1979). Informed consent in societal riskbenefit decisions. *Technological Forecasting and Social Change 13*(4), 347–357.

Gentner, D. (2001). Mental Models, Psychology of. In *International Encyclopedia of the Social & Behavioral Sciences*, pp. 9683–9687. Elsevier.

Gigerenzer, G. (1991). How to make cognitive illusions disappear: Beyond heuristics and biases. *European review of social psychology 2*(1), 83–115.

Gray, D. E. (2013). *Doing research in the real world*. Sage.

Hassard, S. (2011). *The persistence of analogies in design decision-making*. Ph. D. thesis, UCL (University College London).

Hassard, S. T., A. Blandford, and A. L. Cox (2009). Analogies in design decision-making. In *Proceedings of the 23rd British HCI group annual conference on people and computers: celebrating people and technology*, pp. 140–148. British Computer Society.

Hibshi, H. (2015). Discovering Decision-Making Patterns for Security Novices and Experts. Technical report, King Abdul-Aziz University.

Hollan, J., E. Hutchins, and D. Kirsh (2000). Distributed cognition: toward a new foundation for human-computer interaction research. *ACM Transactions on Computer-Human Interaction (TOCHI) 7*(2), 174–196.

Jackson, M. (2001). *Problem frames: analysing and structuring software development problems*. Addison-Wesley.

Klein, G. (1993). Naturalistic decision making: Implications for design. Technical report, DTIC Document.

Klein, G. (2011). *Streetlights and shadows: Searching for the keys to adaptive decision making*. MIT Press.

Klein, G., R. Calderwood, and D. MacGregor (1989, June). Critical decision method for eliciting knowledge. *IEEE Transactions on Systems, Man, and Cybernetics 19*(3), 462–472.

Li, J., X. Ou, and R. Rajagopalan (2010). Uncertainty and risk management in cyber situational awareness. In *Cyber Situational Awareness*, pp. 51–68. Springer.

Miles, R. and K. Hamilton (2006). *Learning UML 2.0* (1st ed ed.). Beijing ; Sebastopol, CA: O'Reilly. OCLC: ocm69706455.

M'manga, A., S. Faily, J. McAlaney, and C. Williams (2017). System Design Considerations for Risk Perception. In *11th IEEE International Conference on Research Challenges in Information Science*. IEEE.

Norman, D. A. (1983). Some observations on mental models. *Mental models 7*(112), 7–14.

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

Rasmussen, J. (1986). Information processing and human-machine interaction. An approach to cognitive engineering.

Schneier, B. (2008). The psychology of security. In *International Conference on Cryptology in Africa*, pp. 50–79. Springer.

Smetters, D. K. and R. E. Grinter (2002). 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*, pp. 82–89. ACM.

Tversky, A. and D. Kahneman (1973). Availability: A heuristic for judging frequency and probability. *Cognitive psychology 5*(2), 207–232.

Tversky, A. and D. Kahneman (1974). Judgment under uncertainty: Heuristics and biases. In *Utility, probability, and human decision making*, pp. 141–162. Springer.

Werlinger, R., K. Muldner, K. Hawkey, and K. Beznosov (2010). Preparation, detection, and analysis: the diagnostic work of IT security incident response. *Information Management & Computer Security 18*(1), 26–42.

Wixon, D., K. Holtzblatt, and S. Knox (1990). Contextual design: an emergent view of system design. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 329–336. ACM.

Xiao, S., J. Witschey, and E. Murphy-Hill (2014). Social influences on secure development tool adoption: why security tools spread. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*, pp. 1095–1106. ACM.

Yee, K.-P. (2002). User interaction design for secure systems. In *International Conference on Information and Communications Security*, pp. 278–290. Springer.

Yu, E. S. K. (Ed.) (2011). *Social modeling for requirements engineering*. Cooperative information systems. Cambridge, Mass: MIT Press. OCLC: ocn459208266.

Zurko, M. E. and R. T. Simon (1996). User-centered security. In *Proceedings of the 1996 workshop on New security paradigms*, pp. 27–33. ACM.