Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2008 Proceedings

Americas Conference on Information Systems (AMCIS)

2008

Decision Support for Perceived Threat in the Context of Intrustion Detection Systems

Christopher S. Leberknight
New Jersey Institute of Technology, chris.leberknight@njit.edu

George R. Widmeyer
New Jersey Institute of Technology, george.r.widmeyer@njit.edu

Michael L. Recce
New Jersey Institute of Technology, michael.l.recce@njit.edu

Recommended Citation

Leberknight, Christopher S.; Widmeyer, George R.; and Recce, Michael L., "Decision Support for Perceived Threat in the Context of Intrustion Detection Systems" (2008). *AMCIS 2008 Proceedings*. 317.
http://aisel.aisnet.org/amcis2008/317

Decision Support for Perceived Threat in the Context of Intrusion Detection Systems

Christopher S. Leberknight
Department of Information Systems
New Jersey Institute of Technology
Newark, New Jersey 07102
chris.leberknight@njit.edu

George R. Widmeyer
Department of Information Systems
New Jersey Institute of Technology
Newark, New Jersey 07102
george.r.widmeyer@njit.edu

Michael L. Recce
Department of Information Systems
New Jersey Institute of Technology
Newark, New Jersey 07102
michael.l.recce@njit.edu

ABSTRACT

The objective of this research is to propose a novel approach for using a behavioral biometric known as keystroke analysis, to facilitate decision making in the context of an intrusion detection system (IDS). Regardless of the situation, individuals have a specific baseline or disposition to decision making based on two psychological factors: (1) indecisiveness, and (2) intolerance of uncertainty. The IDS provides a probability of intrusion and a set of objective situational characteristics. We propose a decision support system that allows the decision maker to state a level of perceived threat and to vary the security thresholds that determines the false acceptance rates of the IDS. Our hypothesis is that perceived threat depends not only on the keystroke technology but also on the social context and disposition toward decision making of the user. This research tests this hypothesis and provides guidance in the design of better security systems.

Keywords: DSS, intrusion detection, security, keystroke analysis, biometrics, perceived threat

INTRODUCTION

As society becomes increasingly dependent on technologies, such as electronic medical patient records, online banking, enterprise resource planning systems, emergency management systems, and wireless and pervasive technologies, organizations are faced with many questions on how to assess, maintain, adapt, and respond to security attacks. The 2007 E-Crime Watch Survey released by CSO Magazine on September 11, 2007 (http://www.csoonline.com/documents/pdfs/e-crime_release_091107.pdf), indicates that unauthorized access to or use of corporate information was one of the top five computer crimes committed by insiders and outsiders. In addition, the survey reports the methods used by insiders to commit e-crimes have changed compared to the previous year. Social engineering techniques (gaining access through manipulation of a person or persons who can permit or facilitate access to a system or data) have become the number one method for committing computer crimes, followed by individuals using compromised accounts, copying information to mobile devices like USB drives or iPods, and use of their own account.. The survey also found that the most effective technologies for preventing computer crimes were: Statefull firewalls, access controls, electronic access controls, application layer firewalls, and host-based anti-virus. The least effective technologies were: manual patch management, surveillance, password complexity, badging, and RBL-based SPAM filtering.

Due to the disparity between the most effective and least effective technologies to prevent computer crimes and the increasing threat of social engineering techniques , new methods for securing information beyond the traditional passwords and badging need to be investigated.

Despite the limitations with existing security systems, there is limited research contribution from the Information Systems (IS) discipline. In an article published in 2007 the authors state

> Our survey reveals that most information security research has focused on the technical context and on issues of access to IS and secure communication. The corresponding security issues have been resolved by

> using mathematical approaches as a research approach. The reference disciplines most commonly reflected have been mathematics, including philosophical logic. Based on this analysis, we suggest new directions for studying information security from an information systems viewpoint, with respect to research methodology and research questions." (Siponen and Kukkonen 2007, p.1)

In an effort to reduce costs and enhance security, many organizations are considering converging physical and logical security. The convergence of physical and logical security will create several challenges relating to the integration of the separate technologies, polices and controls. In addition, the lack of IS contributions to the field of information security warrants further investigation into the methods for preventing physical security threats.

Key background information related to physical security, intrusion detection, and biometrics is presented in the next section of this paper. We then present the research model with background literature to explain the constructs in the model, followed by a section regarding the research methodology and description of the research plan for testing the model. The final section includes conclusions and further discussion.

SECURITY BACKGROUND

The Department of Energy Office of Health, Safety and Security, defines physical security as the use of intrusion detection and assessment, entry and search control, barriers, communications, testing and maintenance, and supporting systems and interfaces to deter, detect, annunciate, assess, delay, and communicate an unauthorized activity. A physical security system, Figure 1, is designed to employ a complementary combination of these components. We focus on intrusion detection and assessment using biometrics.

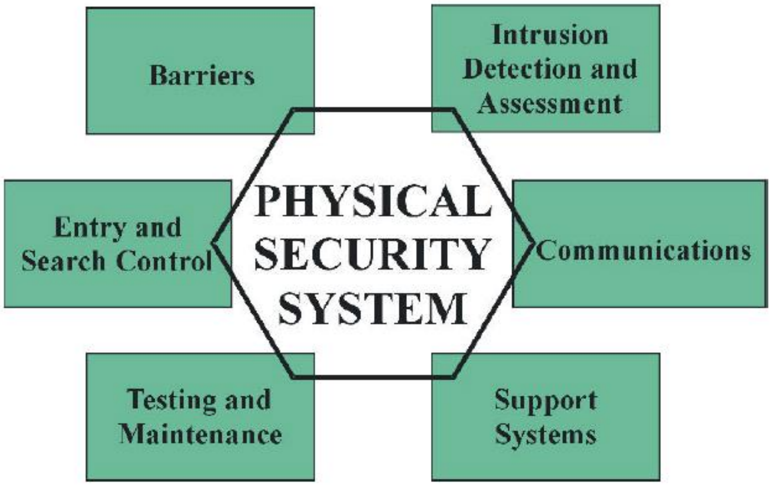

Figure 1. Physical Security System Components

(http://www.hss.energy.gov/IndepOversight/guidedocs/0009pssig/sec1.pdf p.5)

Intrusion Detection and Assessment

Intrusion-detection systems consist of an alarm and an assessment system, and are usually layered for both interior and exterior applications. Exterior systems are designed to provide the earliest possible detection of an unauthorized intrusion, as far away from the security interests as possible. Examples of intrusion detections systems for physical security include exterior perimeter sensors, interior sensors, perimeter closed circuit television (CCTV) systems, interior CCTV systems, and alarm processing and displays.

In many instances, the currently used intrusion detection systems do not provide any additional information other than alerting security that an intrusion has occurred. This equates to a significant opportunity cost relating to false alarms. The one exception is CCTV systems. However, they also pose several security challenges relating to weather extremes (ice fog, wind vibration), varying background light levels due to “bloom” from bright light sources (perimeter lighting, vehicle headlights), and visual obstructions (Department of Energy, 2000).

While there are many examples of intrusion detection systems for computer security (Debar et al 1999), advancements in physical security have lagged behind. The most prevalent types of technologies used for physical security include card reader and password based systems. Access cards can be easily stolen, duplicated or obtained through social engineering techniques. In addition there are several shortcomings associated with traditional passwords (De Ru and Eloff 1997, Braz and Robert 2006). Consequently, the limitations with these systems could have severe consequences on an organizations overall security. Many organizations are beginning to investigate the benefits of consolidating their physical and logical security infrastructures to address the challenge of justifying their security budget. (PriceWaterHouseCoopers, Global State of Information Security Survey, 2007). As a result, new methods to address the limitations with existing physical security systems are required.

In response to the limitations with current physical security systems we are proposing using a behavioral biometric, known as keystroke analysis, for perimeter defense and facility access.

Biometrics

Biometrics may be defined as a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition. Biometrics fall into two categories – behavioral and physiological. A behavioral biometric is a characteristic that is learned and acquired over time rather than one based primarily on biology. All biometric characteristics depend somewhat upon both behavioral and biological characteristic. Examples of biometric modalities for which behavioral characteristics may dominate include signature recognition and keystroke dynamics. A physiological or biological biometric is a characteristic based primarily on an anatomical or physiological characteristic, rather than a learned behavior. Examples of biometric modalities for which biological characteristics may dominate include fingerprint and hand geometry (National Science and Technology Council Subcommittee on Biometrics, http://www.biometrics.gov/docs/glossary.pdf).

The basic process for a biometric authentication system (BAS) involves two stages: registration or enrollment and authentication. During the enrollment process, the user trains the hardware device by repeatedly performing a specific task in order for the genetic algorithms to learn the unique characteristic pertaining to the identity of the individual. Once the unique characteristic or signature is obtained, it is stored in a database. The database will contain signatures or templates that will be analyzed for future access to the system. The future access, or the second stage, of a BAS is authentication. During this stage, the user trying to access the system will have his/her unique signature compared to the templates in the database to confirm or deny a match. The diagram in Figure 2 (Bhargav-Spantzel et al 2006) below illustrates the common components of a BAS.

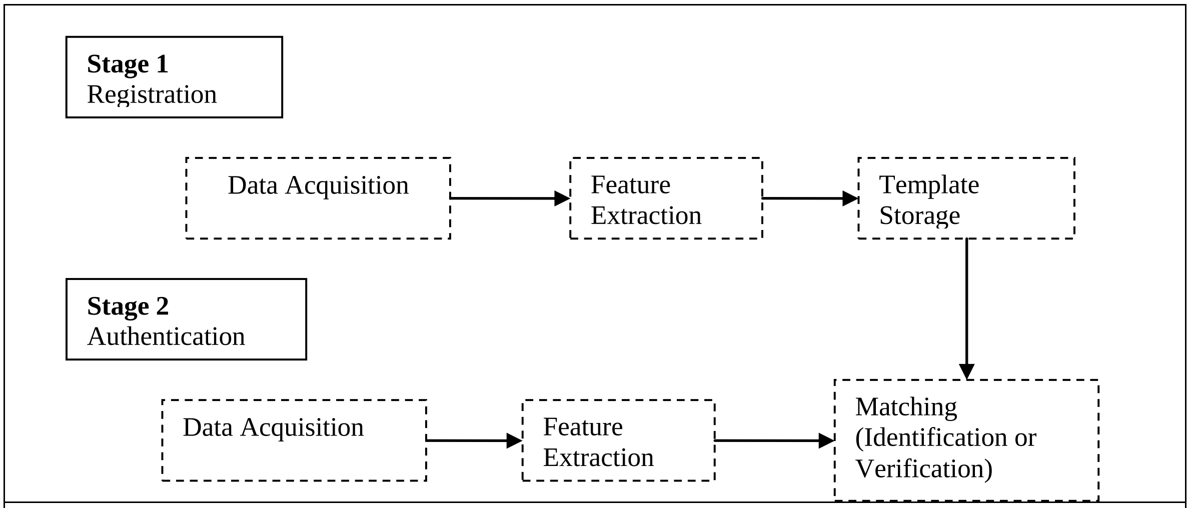

Figure 2. Generic Biometric System

Keystroke analysis is based on behavioral characteristics that are derived by analyzing patterns comprised of keystroke durations (key hold time, keywords) and digraph latencies (time between successive keystrokes) (Bergadano et al 2002). A physiological biometric is primarily used for access control, is more intrusive, and face many user acceptance issues. A unique quality of behavioral biometrics is that they can be implemented as a complementary and transparent security solution.

Instead of using the biometric for access control, we suggest using keystroke analysis as a monitoring, or intrusion detection system. When an individual attempts to access a particular location by typing his/her PIN onto a keypad, an application will monitor and collect the individuals' keystroke information in real-time. A data mining component will compare the keystroke data for current access attempts with data stored in a profile database and generate a probability of an intrusion. The data representing the probability of an intrusion will be sent to a security operations center and can be used to facilitate collaborative decisions to identify physical security incidents. Each security engineer will receive information relating to the probability of an intrusion and decide on the appropriate level of action.

The specific action that results from receiving the information is dependent on five parameters: (1) the role of the person accessing the location, (2) the importance of the location, (3) false alarm rate for the location, (4) the deviation of an individual's current keystroke pattern from his/her profile keystroke pattern, and (5) the deviation from an individual's normal access time pattern based on historical access logs. The iterative dichotomiser 3 (ID3) algorithm, developed by Quinlan (1987), will be employed to generate the smallest decision tree using all of the five parameters as input nodes. The decision tree will also contain three output nodes which correspond to 1. Retype password, 2. Ignore 3. Select threat level. Output 1, retype password, may be automated if the difference between the current keystroke data and the profile keystroke data is minimal.

A majority rule voting policy will be used to determine the final decision based on each engineer's output selection. A weighted average will be added to each engineer's vote based on his/her historical performance rate. The historical performance rate is computed based on the number of correct previous output selections. Therefore, some engineers vote may have a higher voting weight and have a higher impact on the final decision. In addition, the historical performance rate and the complexity or severity of the decision tree could be used to evaluate the most appropriate collaboration level. For example, if parameters 1, 2 and 3 are high the system could require a high collaboration level. That is, since the impact potential is high, more engineers would be required to evaluate the detected incident. If parameters 1, 2 and 3 are low, perhaps only one or two engineers are needed to make a decision. Our proposed biometric based intrusion detection system is depicted in Figure 3.

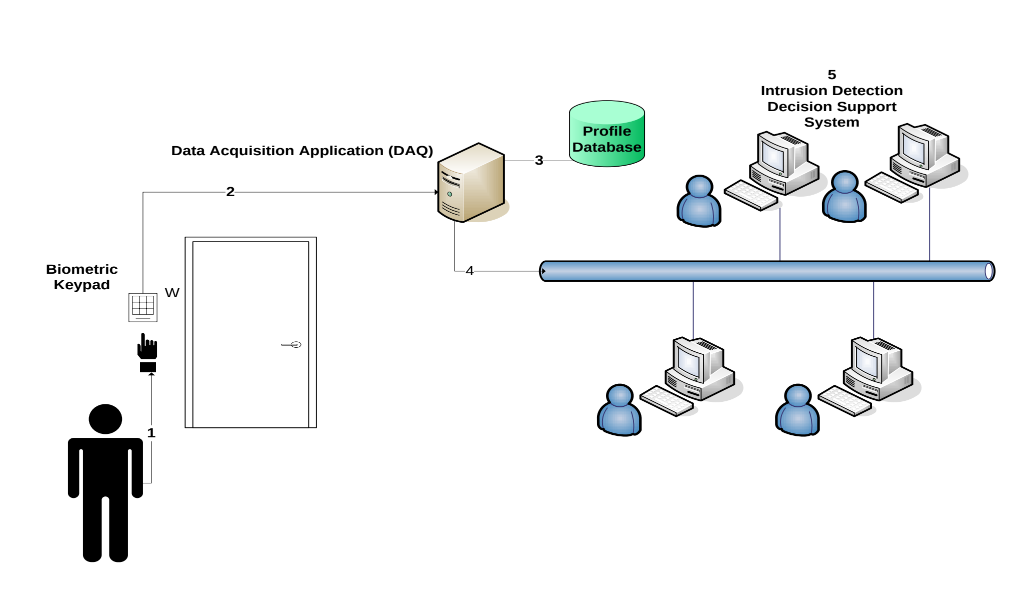

Figure 3. Real-time data driven biometric-based IDS for Physical Security

RESEARCH MODEL

So far we have described the motivation for new security controls and an intrusion detection application based on keystroke analysis. In the following section, we present previous research, which investigated the impacts of DSS on decision making, and our research model for evaluating perceived threat.

Previous Research

The specific factor we intend to address in our research model is to understand how different individuals respond to the same information. While there is existing literature regarding the effects of information presentation (Tractinsky and Meyer 1999, Lim and Benbasat 2000), and there is substantial research regarding decision confidence (Kasper 1995, Kottermann et al 1994 and Melone 1995), the information which influences an individual's perception of threat in the context of physical security has not been thoroughly investigated.

The effectiveness of any IDS can be evaluated in terms of the quality of the information, but the actions taken in response to the information are heavily influenced or impacted on how we perceive our ability to control the outcome. The illusion of control theory (Langer 1975) postulates that individuals often have a difficult time distinguishing between their ability to control the outcome of a skill related task versus a chance related task. Langer's theory was later evaluated in the context of decision support systems. Results from a study conducted by Kottemann and Remus (1991) which was based upon the theory of "illusion of control," concluded that decision makers may develop improper attitudes regarding the efficacy of what-if analysis for a production-scheduling task. A follow up to this research, Kottemann, Davis and Remus (1994), found that what-if analysis users expressed inflated confidence beliefs yet post-hoc analysis revealed that they actually performed significantly worse than nonusers. Unlike previous research, Melone et al (1995) presented results which indicated that decision support system (DSS) improved the subjects' objective quality of the decision, and there was no difference in the confidence levels between subjects who used and did not use the DSS. Subsequent research investigating decision confidence provides insight into three DSS design principles, expressiveness, visibility and inquirability for perfect calibration (Kasper 1995). Decision confidence denotes confidence in a specific event, a decision, as opposed to self-efficacy (Bandura 1977), inherent trust in technology, or other types of confidence (Kasper 1995). Research by Kahai (1998) demonstrated that active involvement, familiarity, and consistency of the normative decision with the problem frame during DSS use may bias a user's expectations of success. The majority of the research discusses various results relating to decision confidence without stressing the importance of contextual influential factors.

Once a security incident is detected, depending on the potential impact of the incident, which many times is difficult to quantify, individuals may have difficulty processing information or reacting to the incident. The inability to react during a crisis or threat situation is known at threat-rigidity (Staw 1981). In addition, due to time constraints quick decisions are often required, which can alter or impact our perception of risk or threat. Trust in the application as well as the perception of the information quality have been linked to both intention to use and decision outcome (McKnight et al 2002, Li et al 2006, and Nicolaou and McKnight 2006).

McKnight et al. (2002) developed a survey instrument to test their model of trust in the context of e-commerce. Li et al. (2006) expanded on McKnight's trust model by incorporating both attitude and subjective norm. Fisher et al (2003) evaluated the effects of data quality information on decision outcome based on demographics, time, experience, and task complexity and Nicolaou and McKnight (2006) evaluated trust, information quality, and risk as determinants for intention to use in the context of a B2B transaction.

In any security policy, risk assessment is paramount to protecting assets and limiting potential impacts. Early work regarding risk focused on understanding and anticipating public responses to hazards of nuclear and chemical technologies (Slovic 1987). Subsequently, there is also a vast amount of literature directed toward information systems which discusses various qualitative and quantitative approaches to risk assessment. (Alberts et al 2002, Suh and Han 2003, Yavagal et al 2005, Karabacak and Sogukpinar 2005, Jones 2007, den Braber et al 2007, and Page et al 2007). While both quantitative and qualitative approaches are concerned with risk, primarily from the perspective of information security, Weber et al (2002) presented a psychometric scale that assessed risk taking in five content domains: financial decisions (separately for investing versus gambling), health/safety, recreational, ethical, and social decisions. Results from their study indicated the respondents' degree of risk-taking was highly domain-specific. In addition to the qualitative and quantitative systematic approaches used for risk assessment, there are also certain psychological factors, which may relate to an individuals predisposition to decision confidence.

For example, intolerance of uncertainty may be defined as the excessive tendency of an individual to consider it unacceptable that a negative event may occur, however small the probability of its occurrence (Dugas, Gosselin, & Ladouceur, 2001) Bredemeier et al (2007) examined the relation between the intolerance of uncertainty and perceived threat, while Berenbaum et al (2007) hypothesized antecedents of perceived threat. Results indicated that perceived competence, other's benevolence and standards were all significantly correlated to perceived threat. In addition, Frost and Shows (1993) developed a survey instrument that measured individual differences in general indecisiveness. Research by Rassin and Muris (2005) indicated indecisiveness fosters worst case scenario reasoning, in that indecisive individuals tend to interpret ambiguous situations more readily as threatening. Patalano and Wengrovitz (2006) present research that explores the construct of indecisiveness across sex and culture. The relationship between the various aforementioned constructs, which led to the evolution of our research model, is illustrated in Figure 4 below.

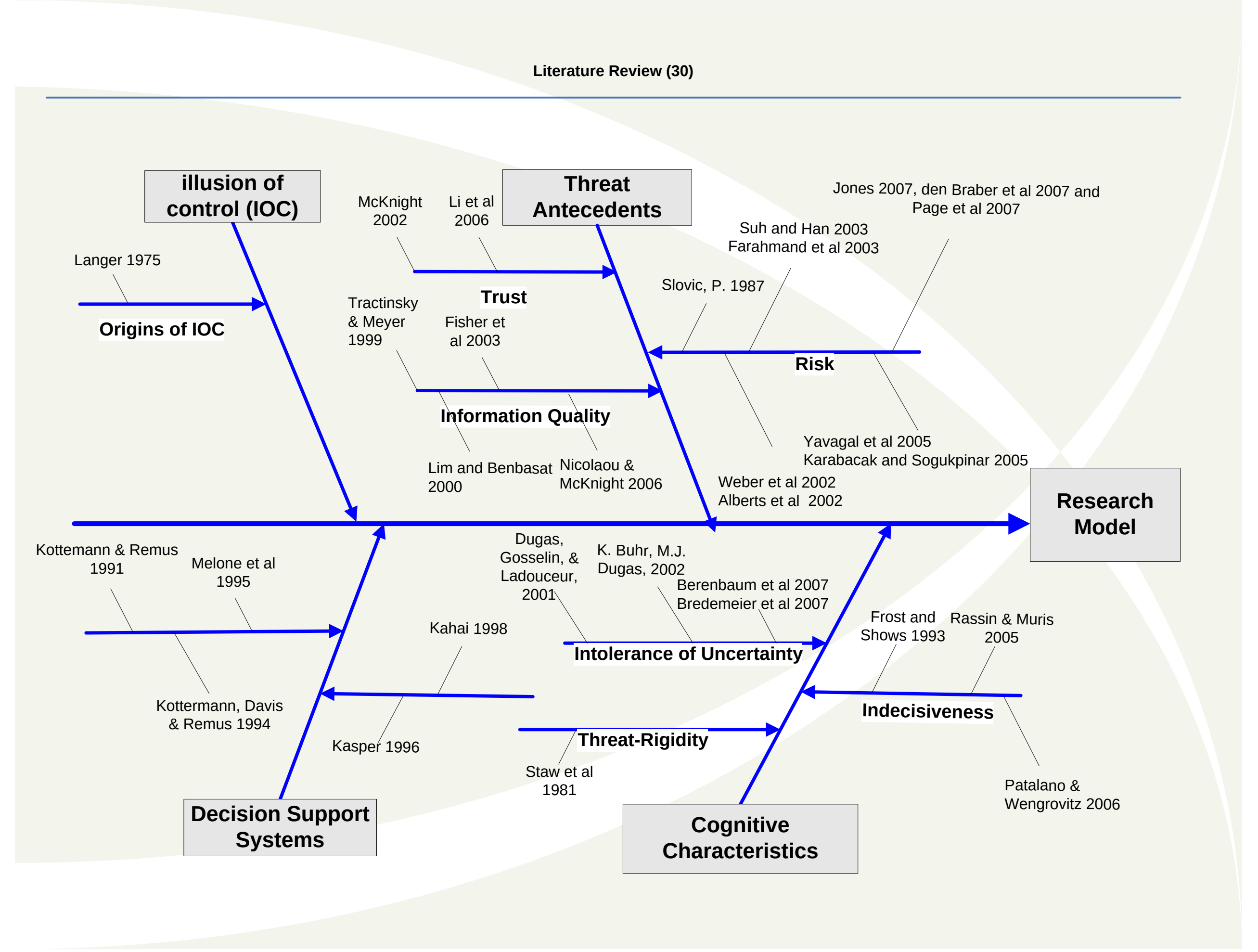

Figure 4. Evolution of Research Model

Proposed Model

Based on the previous research, we identify several determinants for perceived threat in order to help explain some of the contributing factors to decision outcome in the context of physical security. We claim that the following two independent variables: indecisiveness and intolerance of uncertainty are key determinants for disposition to decision making. We believe disposition to decision making will directly influence an individual's perception of threat. Our belief is based on the assumption that, prior to receiving any information, individuals who have a low disposition toward decision making will have a less accurate perception of the threat than individuals who have a high disposition toward decision making.

We propose the model depicted in Figure 5. It will be tested in future research to help identify and provide design considerations for DSS usage for security, threat, or crisis management. Descriptions of the constructs are listed in Table 1.

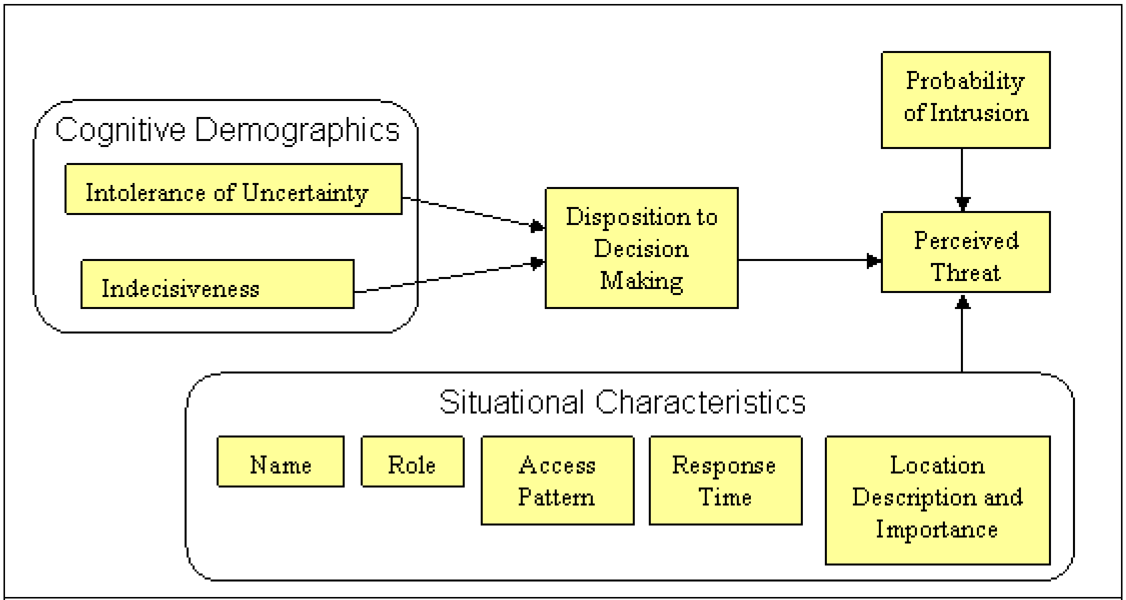
Cognitive Demographics
Intolerance of Uncertainty
Indecisiveness
Disposition to Decision Making
Probability of Intrusion
Perceived Threat
Situational Characteristics
Name
Role
Access Pattern
Response Time
Location Description and Importance

Figure 5. Proposed Research Model

Construct	Definition	Items
Indecisiveness (Rassin et al. 2007, Germeijs and Boeck 2003).	Literature differentiates between decision difficulties in one specific area (such as career planning) and difficulties in virtually all possible areas. The former has been referred to as "indecision", while the latter is termed "indecisiveness".	Measured on a seven-point scale, strongly agree to strongly disagree 1. I find it easy to make decisions. 2. After I have chosen or decided something, I often believe I have made the wrong choice or decision. 3. Once I make a decision, I feel confident that it is a good one.
Intolerance of Uncertainty (Dugas, Gosselin, & Ladouceur, 2001).	Intolerance of uncertainty may be defined as the excessive tendency of an individual to consider it unacceptable that a negative event may occur, however small the probability of its occurrence.	Measured on a seven-point scale, strongly agree to strongly disagree 1. Uncertainty stops me from having a strong opinion. 2. When I am uncertain, I can't function very well.
Situational Characteristics (new for this research)	Objective and historical information about the person trying to access the secure location	(1) Name of the person accessing the location, (2) their role, (3) the importance of the location, (4) the deviation from an individual's normal access time pattern based on historical access logs, and (5) the importance of the location
Probability of Intrusion (new for this research)	Conditional Probability based on intrusion detection hardware and processing algorithm	Situation specific result of the keystroke analysis algorithm and also background knowledge of the probability of a false positive and false negative
Disposition to decision making (derived measure, reflective construct)	An individual's tendency to make decisions	A function of Indecisiveness and Intolerance of Uncertainty

Construct	Definition	Items
Perceived Threat (Bredemeier and Berenbaum 2007)	Perceptions of the probabilities and costs of future undesirable outcomes (We assume the impact relating to the threat is always high.)	A variable measure determined by subjective estimates and the sensitivity versus specificity of the technology.

Table 1. Research Model: Constructs, Definitions, and Scales

When the decision maker assesses the level of perceived threat, he or she is aware of the outcome from the keystroke analysis algorithm which is based on a tunable sensitivity parameter that evaluates the physical measurement of the person who entered their access code. The null hypothesis is that the person's keystroke pattern matches their record in the data base and therefore admits them. There is a probability of a false acceptance (false match) in that a person is given access to the secure area when they should be denied and a false reject (false non-match) in that the person is denied access when they should be admitted. The sensitivity of the algorithm can be adjusted to reduce the false acceptance level but this raises the false reject level. The tradeoff between these two depends on the relative percentage of imposters to authorized users and on the relative cost of making positive and negative errors (Provost and Fawcett, 2001). The situational characteristic such as the person who is trying to access the area, the time of day, and the value of the resources in the secure area informs this tradeoff. We are developing a decision support system that presents these variables to the decision maker when they make their assessment to admit or deny a person.

We plan to survey senior security officers in both a university and a military context to understand how context affects the tradeoff. There is a certain level of false positive and false negative as a result of just using a password for access control. The tradeoff curve is determined by this technology and cannot be improved except by changing the system. Adding keystroke analysis in addition to the use of an access code is a change in the system that results in a new false positive / false negative tradeoff curve. We believe that the hardware and algorithm we are developing can make a significant improvement in this tradeoff, but the complete security system must include both social and technical dimensions. This is why we need to develop a decision support system.

CONCLUSION

The lack of IS research, the increase in computer crimes, the decrease in security spending, and the drive toward physical and logical security convergence have necessitated further investigation into ways to improve physical security.

We are currently evaluating the possibility of integrating a behavioral biometric, keystroke analysis, into Homeland Defense technologies. As part of this effort, we are investigating how individuals will respond to a security breach based on the information generated by a biometric device. The response, or decision quality, to a given scenario may vary depending on the individuals' perception of the threat. We claim that individuals have a disposition to decision making that is influenced by indecisiveness and intolerance to uncertainty. The disposition to decision making (a social factor), the decision context (an objective factor), and the probability of intrusion (a technological factor) influences perceived threat.

Mayer et al. (1995) proposed that perceived risk moderates the impact of trust on risk taking. However, research by Nicolaou and McKnight indicated that perceived risk did not moderate the effects of trusting beliefs on intention to use. (Nicolaou and McKnight 2006, p. 348), and neither situational importance nor risk propensity had a significant effect on perceived risk (Nicolaou and McKnight 2006, p. 346). Consequently, due to the conflicting results regarding trust, we intend to expand on previous work in future research by analyzing the moderating effects of trust and risk on perceived threat based on domain specific risk (Weber et al 2002).

In addition in future studies we will test the proposed model using scenarios and interviews of security officers. A decision support system based on the proposed model is being developed that will allow the security officers to vary the security thresholds that determines the false acceptance rates. We intend to interview the subjects regarding their decisions and observe their use of the decision support system. Our hypothesis is that perceived threat is a variable construct that depends not only on the keystroke technology but also on the social context and disposition toward decision making of the user. This research tests this hypothesis and provides guidance in the design of better security systems.

BIBLIOGRAPHY

Alberts, C., Dorofee, A., Stevens, J. and Woody, C. (2003) Introduction to the OCTAVE Approach, Carnegie Mellon Software Engineering Institute.

Ashford, B. M. and Kasper G. M. (2003) A Test of the Theory of DSS Design for User Calibration: The Effects of Expressiveness and Visibility on User Calibration, *Proceedings of the Second Annual Workshop on HCI Research in MIS*, Seattle, WA.

Bandura, A. (1977) Self-efficacy: Toward a Unified Theory of Behavioral Change, *Psychological Review* 84, 191-215.

Berenbaum, H., Thompson, R. J. and Bredemeier, K. (2007) Perceived threat: Exploring its association with worry and its hypothesized antecedents, *Behaviour Research and Therapy* 45, 2473-2482.

Bhargav-Spantzel, A., Squicciarini, A. and Bertino, A. E. (2006) Security, privacy and anonymity: Privacy preserving multi-factor authentication with biometrics, *Proceedings of the second ACM workshop on Digital identity management DIM '06*.

Braz, C. and Robert, J-M. (2006) Security and Usability: the case of the user authentication methods, *Proceedings of the 18th International Conference of the Association Francophone d'Interaction Homme-Machine IHM '06*.

Bredemeier, K. and Berenbaum, H. (2007) Intolerance of uncertainty and perceived threat, *Behaviour Research and Therapy*, (2007), doi:10.1016/j.brat.2007.09.006

Buhr, K and Dugas, M. J. (2002) The intolerance of uncertainty scale: psychometric properties of the English version, *Behaviour Research and Therapy* 40, 931-945.

den Braber, F., Hogganvik, I., Lund, M.S., Stølen, K., Vraalsen, F. (2007) Model-based security analysis in seven steps - A guided tour to the CORAS method, *BT Technology Journal*, 25, 1, 101-117.

Department of Energy Office of Safeguards and Security Evaluations (2000), Physical Security Systems Inspectors Guide, Appendix A p. 80, (http://www.hss.energy.gov/IndepOversight/guidedocs/0009pssig/appa.pdf)

Fisher, C. W., InduShobha C-S. and Ballou, D. P. (2003) The Impact of Experience and Time on the Use of Data Quality Information in Decision Making, *Information Systems Research* 14, 2, 170-188.

Davis, F. D.; Kottemann, J. E., Remus, W. E. (1991) What-if analysis and the illusion of control, *Proceedings of the Twenty-Fourth Annual Hawaii International Conference on System Sciences*, Volume iii, 452-460.

De Ru, W. G. and Eloff, J. H. P. (1997) Enhanced password authentication through fuzzy logic., *IEEE Expert* 12, 6, 38-45.

Dugas, M. J., Gosselin, P. and Ladouceur, R. (2001) Intolerance of uncertainty and worry: Investigating narrow specificity in a non-clinical sample. *Cognitive Therapy and Research* 25, 551-558.

Freeston, M. H., Rhe´aume, J., Letarte, H., Dugas, M. J. and Ladouceur, R. (1994) Why do people worry? *Personality and Individual Differences* 17, 791–802.

Frost, R. O. and Shows, D. L. (1993) The nature and measurement of compulsive indecisiveness. *Behaviour Research and Therapy* 31, 683–692.

Jones, A. (2007) A framework for the management of information security risks, *BT Technology Journal* 25, 1, 30-36.

Kahai, S. S., Solieri, S. A. and Felo, A. J. (1998) Active Involvement, Familiarity, Framing, and the Illusion of Control During Decision Support System Use, *Decision Support Systems* 23(2), 133-148.

Karabacak, B. and Sogukpinar, I. (2005) ISRAM: information security risk analysis method, *Computers & Security* 24, 2, 147-159.

Kasper, G. M. (1996) A Theory of Decision Support System Design for User Calibration, *Information Systems Research* 7, 2, 215-232.

Kottemann, J. E., Davis, F. D. and Remus, W. E. (1994) Computer-Assisted Decision Making: Performance, Beliefs, and the Illusion of Control, *Organizational Behavior and Human Decision Processes* 57, 1, 26-37.

Langer, E. J. (1975) The Illusion of Control, *Journal of Personality and Social Psychology* 32, 2, 311-328.

Li, X., Hess, T. J. and Valacich, J. S. (2006) Using attitude and social influence to develop an extended trust model for information systems, *ACM SIGMIS Database* 37, 2&3, 108-124.

Lim, K.H. and Benbasat, I. (2000) The effect of multimedia on perceived equivocality and perceived usefulness of information systems." *MIS Quarterly*, 24, 3, 449-471.

Melone, N. P., McGuire, T. W., Chan, L. W. and Gerwing, T. A. (1995) Effects of DSS, Modeling, and Exogenous Factors on Decision Quality and Confidence, *Proceedings of the 28th Annual Hawaii International Conference on System Sciences*.

Nicolaou, A. I. and McKnight, D. H. (2006) Perceived Information Quality in Data Exchanges: Effects on Risk, Trust, and Intention to Use, *Information Systems Research* 17, 4, 332-351.

Page, V., Dixon, M. and Choudhury, I. (2007) Security risk mitigation for information systems, *BT Technology Journal* 25, 1, 118-127.

Patalano, A.L. and Wengrovitz, S.M. (2006) Cross-cultural exploration of the Indecisiveness Scale: A comparison of Chinese and American men and women, *Personality and Individual Differences* 41, 5, 813-824.

Provost, F. and Fawcett, T. (2001) Robust Classification for Imprecise Environments, *Machine Learning*, 42, 3, 203-231.

PriceWaterHouseCoopers, Global State of Information Security Survey 2007
http://www.pwc.com/extweb/pwcpublications.nsf/docid/114E0DE67DE6965385257341005AED7B

Quinlan, J.R. (1987) Simplifying decision trees, *International Journal of Man-Machine Studies*, 27, 221-234.

Rassin, E. and Muris, P. (2005) Indecisiveness and the interpretation of ambiguous situations, *Personality and Individual Differences* 39, 7, 1285-1291.

Staw, B. M.. Sandelands, L. E. and Dutton, J. E. (1981) Threat-Rigidity Effects in Organizational Behavior: A Multilevel Analysis, *Administrative Science Quarterly* 26, 4, 501-524.

Siponen, M. T. and Oinas-Kukkonen, H. (2007) A review of information security issues and respective research contributions, *ACM SIGMIS Database* 38, 1, 60-80.

Slovic, P. (1987) Perception of Risk, *Science* 236, 280-285.

Suh, B. and Han, I. (2003) The IS risk analysis based on a business model, *Information & Management* 41, 2, 149-158.

Tractinsky, N. and Meyer, J. (1999) Chartjunk or Goldgraph? *MIS Quarterly* 23. 3, 397- 420.

Weber, E. U., Blais, A-R, E. and Betz, N. E. (2002) A Domain-specific Risk-attitude Scale: Measuring Risk Perceptions and Risk Behaviors", *Journal of Behavioral Decision Making* 15, 263–290.

Yavagal, D. S., Lee. S. W., Ahn, G-J. and Gandhi, R. A. (2005) Security: Common criteria requirements modeling and its uses for quality of information assurance (QoIA), *Proceedings of the 43rd annual Southeast regional conference*, Volume 2, ACM-SE 43.