An Empirical Investigation of Factors Affecting Resistance to Using Multi-Method Authentication Systems in Public-Access Environments

Joseph Marnell – Advisor: Dr. Yair Levy

Introduction

Recent research suggests that electronic-commerce (e-commerce) transactions are not the primary source of identity theft (IDT) (Collins, 2003; Newman, 2004). However, Shareef, Kamur, and Vinod (2012) proposed that IDT plays a substantial role in purchase resistance for consumers of e-commerce. Increasing demands to prevent IDT are advocated in recent literature, newspapers, and government policies. According to Shareef et al. (2012), "current research addresses the issues of identity theft; source, type, and preventative measuring tools" (p. 30). Additional studies indicated that inadequate user authentication (UA) methods are a contributing factor for IDT (Fichtman, 2001). A national survey conducted by the Federal Trade Commission (FTC) (2008) revealed that 4.7% of American adults experienced IDT that involved the loss of personal identifying information (PII). Industry responses to combat the aspects of IDT are focused on the verifiable identification of individuals through the development of acceptable multi-method authentication systems (Bellah, 2001). While current research has shown significant advances in biometric recognition, users continue to resist using biometric technology to enhance password security (Levy & Ramim, 2009). This resistance is attributed to concerns related to protecting their PII, invasion of privacy (IOP), and authentication complexity (AC).

Problem Statement

The research problem this study will address is identity-theft (IDT) incidents due to breaches of personal identifying information (PII) (Venkatesh, Morris, Davis, & Davis, 2003; Zviran & Erlich, 2006). Such PII breaches are significant threats to invasion of privacy (IOP) during e-commerce activities by users in public-access environments (Venkatesh et al., 2003; Zviran & Erlich, 2006). Kim, Jeong, Kim, and So (2011) identified PII as financial card numbers, usernames, passwords, medical records, driver's licenses, and Social Security numbers (Kim et al., 2011). These PII represent targets of online theft during e-commerce activities. Doolin, Dillon, Thompson, and Corner (2005) defined e-commerce as information networks that enable data flow for business, capital, and logistic support. Existing methods to protect PII during e-commerce activities are based on three types of authentication: username/password, tokens/smart cards, and biometrics (Levy & Ramim, 2009; Millett & Holden, 2003).

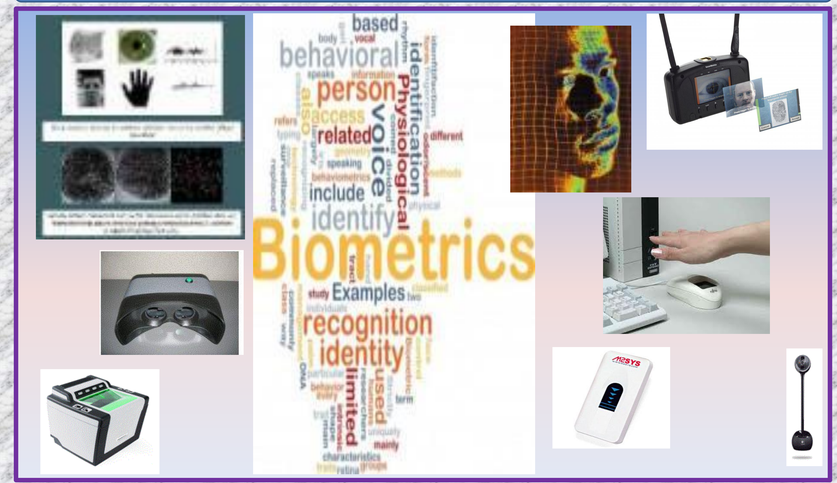
Research Goals

The main goal of this proposed research study is to assess empirically individuals' perspectives about the perceived value of protecting their personal identifying information (PVP), perceived invasion of privacy (IOP), and authentication complexity (AC) on their resistance to using multi-method authentication systems (RMS) in public-access environments. Assessing RMS during e-commerce activities may reveal how best to lower IDT losses (Doolin et al., 2005; Roussos & Moussouri, 2004). According to research conducted by Levy and Ramim (2009), using multi-method authentication systems to support and expand traditional authentication systems is a viable means of improving the privacy of PII. This proposed study builds on previous research by Altinkemer and Wang (2011), as well as Roussos and Moussouri (2004), which suggested that the integration of multi-method authentication systems for identity verification in public-access environments could minimize IDT. Furthermore, Altinkemer and Wang (2011) recommended additional research into multi-method authentication systems is needed to secure user authentication entries. Prior research by Klaus, Wingreen, and Blanton (2010) suggested that reducing losses from goods and services purchased illegally through IDT will require institutions to provide a means of minimizing the number of users affected by AC.

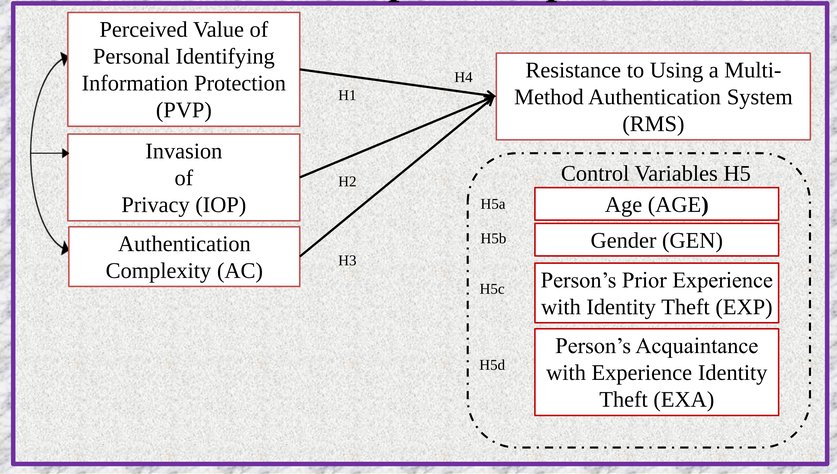
Research Question

The main research question (RQ) that this study will address is: What is the contribution of PVP, IOP, AC, and their interaction on individuals' resistance to using multi-method authentication systems in public-access environments?

User Authentication Methods



Conceptual Map



Hypotheses

In addressing the main RQ, this proposed study will seek to uncover eight specific hypotheses (noted in null form):

H1: *PVP* will have no statistically significant influence on individuals' resistance to using a multi-method authentication system (*RMS*) in public-access environments.

H2: *IOP* will have no statistically significant influence on individuals' resistance to using a multi-method authentication system (*RMS*) in public-access environments.

H3: *AC* will have no statistically significant influence on individuals' resistance to using a multi-method authentication system (*RMS*) in public-access environments.

H4: There will be no significant interaction effect of *PVP*, *IOP*, and *AC* on individuals' resistance to using a multi-method authentication system (*RMS*) in public-access environments.

H5a: *PVP*, *IOP*, *AC*, and *RMS* will have no statistically significant difference based on age (*AGE*).

H5b: *PVP*, *IOP*, *AC*, and *RMS* will have no statistically significant difference based on gender (*GEN*).

H5c: *PVP*, *IOP*, *AC*, and *RMS* will have no statistically significant difference based on person's prior experience with identity theft (*EXP*).

H5d: *PVP*, *IOP*, *AC*, and *RMS* will have no statistically significant difference based on person's acquaintance identity theft experience (*EXA*).

Key Terms

- **Identity theft (IDT)** – An imposter's intentional theft of PII to obtain credit, merchandise, or services in the name of the victim (Eisenstein, 2008; Kim et al., 2011).
- **Personal identifying information (PII)** – Credit and debit card numbers, usernames, passwords, medical records, driver's license, and social security number representing an individually unique person (Kim et al., 2011).
- **Invasion of privacy (IOP)** – Privacy is considered to be freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual (Jerman-Blažič & Klobucar, 2005).
- **Perceived value of identifying information (PVP)** – The value an individual places on the potential loss of his or her personal identifying information represented by his or her driver's license, credit card, social security number, and personal health information that places him or her at a great risk if discovered (Doolin et al., 2005).
- **Access complexity (AC)** – The degree to which an innovation is perceived as relatively difficult to understand and use for access and authentication for electronic-data transfer in public-access environments (Uzoka & Ndzinge, 2009).
- **Resistance to using multi-authentication systems (RMS)** – A measure of someone's aversion to using a certain type of authentication based upon type and sensitivity (Jones, 1991; Wang & Petrison, 1993), intrusiveness, and encroachment on personal privacy (Zviran & Erlich, 2006).
- **Identity theft experiences (EXP)** – Incidents in which individuals are actually affected by the intentional theft of PII by an imposter to obtain credit, merchandise, or services in the name of the victim (Kim et al., 2011).
- **Authentication** – Any process of forming identifiers that distinguish individual usernames and passwords along with smart cards, retina scans, voice, or other forms of recognition (Millett & Holden, 2003).

Key References

- Allison, S., Schuck, A., & Lersch, K. (2005). Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. *Journal of Criminal Justice, 33*(1), 19-29.
- Furnell, S., Dowland, P., Illingworth, H., & Reynolds, P. (2000). Authentication and supervision: A survey of user attitudes. *Computers and Security*, *19*(6), 529-539.
- Levy, Y., & Ramim, M. M. (2009). Initial development of a learners' ratified acceptance of multibiometrics intentions model (RAMIM). *Interdisciplinary Journal of E-Learning and Learning Objects*, *5*, 379-397.
- Roussos, G., & Moussouri, T. (2004). Consumer perceptions of privacy, security, and trust in ubiquitous commerce. *Personal Ubiquitous Computing*, *8*(6), 416-429.
- Shareef, M. A., & Kumar, V. (2012). Prevent/Control Identity Theft: Impact on Trust and Consumers' Purchase Intention in B2C EC. *Information Resources Management Journal (IRMJ), 25*(3), 30-60.
- Tsalakanidou, F., Malassiotis, S., & Strintzis, M. G. (2007). A 3D face and hand biometric system for robust user-friendly authentication. *Pattern Recognition Letter, 28*(16), 2238-2249.
- Venkatesh, V., Morris, M., Davis, F., & Davis, G. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, *27*(3), 425-478.
- Zviran, M., & Erlich, Z. (2006). Identification and authentication: Technology and implementation issues. *Communications of the Association for Information Systems*, *17*(4), 90-105

Next Steps

- Propose Research Method and Expansion of the Literature Review
- Addressing Advisor feedback through a Document of Records
- Approval of the Idea Paper
- Establish the committee
- Complete the Institute Review Board (IRB) training and document approval.