Extending the Technology Acceptance Model to Adopting ECG Wearable Authentication Devices

By
T. Thomas Lahoud

Submitted in partial fulfillment of the requirements for the degree of
Doctor of Professional Studies

Seidenberg School of Computer Science and Information Systems
Pace University

May 17, 2019

We hereby certify that this dissertation, submitted by T. Thomas Lahoud, satisfies the dissertation requirements for the degree of Doctor of Professional Studies in Computing and has been approved.

_____

Dr. Charles Tappert
Chairperson of Dissertation Committee Date

_____

Dr. Lixin Tao
Dissertation Committee Member Date

_____

Dr. Ronald Frank
Dissertation Committee Member Date

Seidenberg School of Computer Science and Information Systems
Pace University, Pleasantville, NY

Abstract

The availability, affordability and pervasiveness of mobile and wearable devices is at an all-time high. New applications are constantly being developed and deployed to increase the functionality and usefulness of wearable devices in order to enhance and improve quality-of-life areas such as communications, workplace productivity, electronic commerce, personal fitness, and healthcare.

At the same time, the increasing magnitude of security breaches, including sophisticated hacking methods, ransomware, malware and phishing attacks, have reached alarming levels. Fortune 500 companies and government institutions are at the forefront of such breaches. In most incidents, Personally Identifiable Information (PII) was compromised, such as login credentials, credit card information and healthcare records (Berghel, 2017; Bonner, 2012; Armerding, 2018). In spite of the availability of tools to protect our records, such as the use of multi-factor authentication protocols, possession protocols, or inherence protocols, the threat remains persistent.

My research will attempt to understand how the workplace and societal perceptions of wearable ECG-based authentication will ultimately impact how readily a new form of mobile technology will be adopted within the workplace. The framework of this research is based on extending the Technology Acceptance Model into ECG-based wearable authentication devices in order to define and evaluate whether such devices will be accepted and used to the extent

possible to prevent fraudulent activities by validating identity, granting access or authorizing usage. Furthermore, this research will gather data from participants in a field study, irrespective of their demographic profile so as to gain insights into user-specific perceptions of interacting with an ECG-based wearable form of technology and will assess the users' perceptions of the technology as it relates to ease of use, perceived usefulness and the workplace factors that influence usage decisions. A theoretical model featuring 12 hypotheses was developed and tested against the empirical data collected using a survey instrument. A measurement model was established using structural equation modelling with partial least squares to validate the hypotheses. Findings of this research confirmed the hypotheses suggesting that the Technology Acceptance Model indeed offers a suitable, robust and predictive framework for the acceptance of ECG-based wearable authentication devices in the workplace.

Acknowledgments

I would like to express my deepest appreciation to my committee chair and advisor, Dr. Charles Tappert, for his guidance and support throughout the dissertation writing process. His suggestions and recommendations to continuously improve my research were instrumental, and without his persistent help, this research would not have been possible. I also would like to thank my committee co-chairs, Dr. Lixin Tao and Dr. Ronald Frank, for their availability, insightful comments and encouragement.

My sincere thanks also goes to Dr. Li-Chiou Chen who was gracious in extending her assistance during various phases of this research.

Last but not the least, I would like to thank my family; words cannot express how grateful I am for their support throughout writing this dissertation.

Dedicated to my wife Deborah -

“I've made the most important discovery of my life. It's only in the mysterious equation of love that any logical reasons can be found. I'm only here tonight because of you. You're the only reason I am...you're all my reasons.”

— John Nash

Table of Contents

List of Figures

List of Tables

Chapter 1. Introduction

As technology becomes more ubiquitous in almost every aspect of daily activities, there will be an expectation for technology to always be available, all of the time. For this to occur, a technology ecosystem needs to be designed so that it is easily accessible, easily portable, always on and secure. Such a system must also employ a robust security framework for access control, by identifying the fundamentals through which the right individual is granted access to the right resources for the right reasons and at the right time.

1.1 Significance of the Problem

When new technology systems are implemented, certain challenges are anticipated such as compatibility with existing hardware or software platforms. Steps to mitigate and minimize disruption or downtime are taken by IT departments and subject matter experts. However, a new set of un-anticipated problems may become apparent as the deployment is underway or following its conclusion. The significance of the research problem is divided into two areas: the current state of authentication in the workplace; and, the specific difficulties faced by the employer as well as by the employee when addressing daily needs for authentication, authorization and access.

1.1.1 Significance of the Problem - Current State

Although many wearable devices and smartphones today boast ease of use, affordability and availability factors, their ultimate implementation and usage does not necessarily achieve its goals without a careful study of the workplace ramifications of interacting with those devices.

This is especially important when an organization is faced with investing in a new technology platform while weighing upfront costs, life cycle maintenance costs and user adoption costs. Consider, for example, why certain wearable devices succeed or fail in a social setting. It is not necessarily the cost factor or ease of use for such device, but rather how technology adoption is affected by user behavior that requires unfamiliar actions. For instance, Bluetooth headsets are often used as a hands-free alternative when making mobile phone calls. That device is socially acceptable even though it usage makes users appear to talk to themselves - that is, acting outside of normal behavior (Rico, et al., 2010). The acceptance of Bluetooth headsets as well as other wearable devices will be driven by their social acceptance.

In this study, the focus is on the workplace, where ECG-wearable authentication is mandated by the employer. When usage is voluntary (as in social settings), understanding the acceptance of a wearable device is largely dependent on how acceptable the resulting behavior is, based on prevailing cultural and social norms (Campbell, 2007). Therefore, an early identification of acceptance of use parameters should precede the deployment of a wearable authentication device in order to classify the workplace acceptability guidelines between the user, the wearable device and the environment in which such a device will be deployed. Defining device interaction parameters will largely be the responsibility of the industry, yet the social as well as the workplace acceptance parameters can only be discovered when the device is on-body and in effective use. Hence, the industry can benefit by identifying where and how individuals will want to use these devices to help understand the feasibility of product implementation and adoption.

1.1.2 Significance of the Problem - Authentication, Authorization & Access Validation Events

As physical and logical security measures have become an integral component in the workplace, the ability of employees to adopt such measures into their daily activities becomes a critical success factor. By contrast, the burden of such measures has become intrinsic to such activities. Consider the process of gaining access to my workplace, which requires numerous checkpoints as depicted in Figure 1 and explained below:

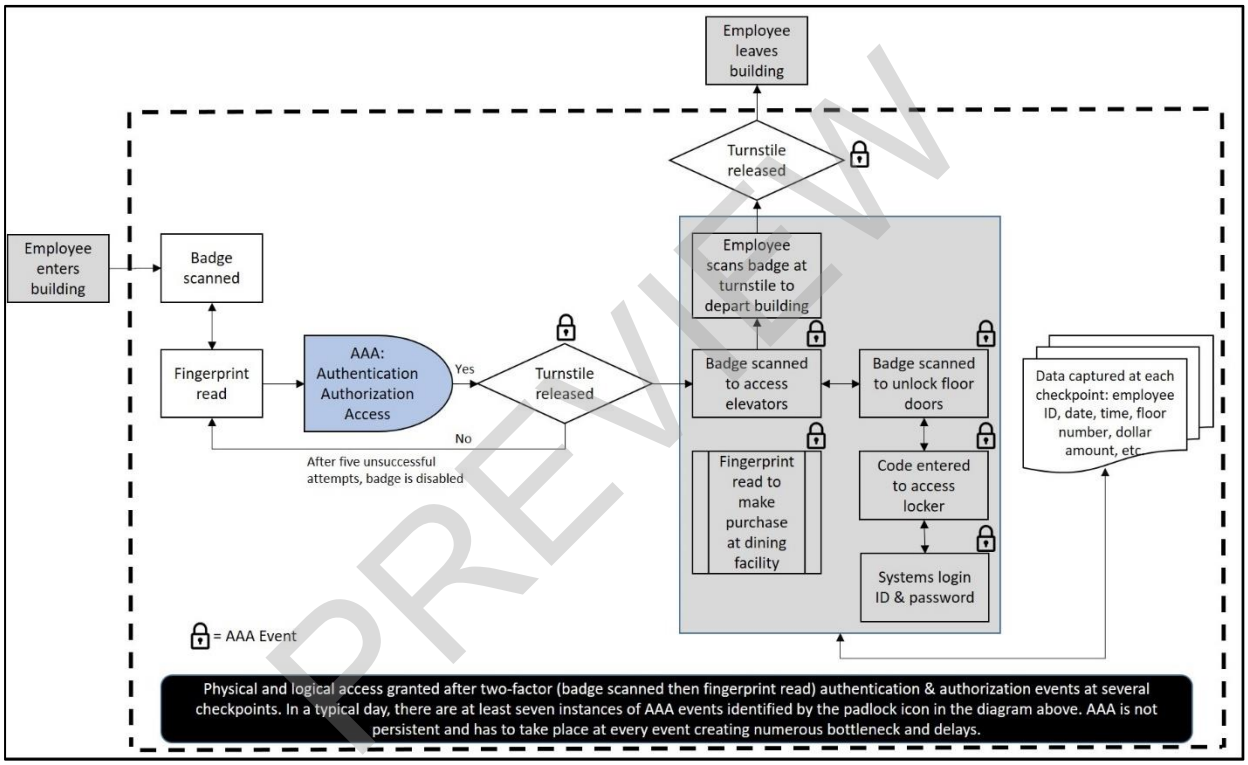

Figure 1 - Authentication, Authorization & Access Events (author's workplace)

- Upon entering the workplace structure, a two-factor authentication procedure is encountered at several turnstiles; first the employee places a badge containing a magnetic stripe against a card reader. Subsequently, the employee places the index finger of the right-hand onto a biometric scanner. Upon successful authentication of the badge and the fingerprint, the employee gains physical access to the workplace.

This is referred to as an AAA Event: authenticate, authorize, access. This procedure frequently fails. I often have to repeat the biometric scan due to residue on skin or on scanner, step to the side to allow another employee to conduct AAA, and then try again. During rush hour, my employer estimates that more than 30% of AAA events fail, causing delays, frustration and frequent complaints.

- When AAA is successful, the employee then proceeds to one of several elevators in order to reach their work floor. The employee selects a floor and places their badge against another reader. The employee enters the elevator and ascends to the designated floor. Note that the employee's badge only allows access to certain floors based on the company's organizational structure.

- Once the employee reaches the floor, he/she places his/her badge against another reader in order to unlock the doors to that floor. The employee walks to a designated locker in order to retrieve their laptop. A 6-digit unlock code is required to open the locker.

- With the laptop powered on, the employee is required to login to the corporate network using a login name and a login password. Upon successful authentication, the employee is now allowed to access the corporate network. However, some software applications require additional logins such as the timekeeping systems or requisition systems.

- When the employee decides to purchase a meal at the company's dining facilities, he/she needs to swipe his/her badge and place his/her index finger onto a biometric reader so that the purchase price is charged to a credit card on file.

- At the conclusion of the workday, many of the aforementioned authentication, authorization and access procedures (AAA events) must be repeated. For example, the employee cannot leave the workplace unless they uses their badge and biometric fingerprint to depart the turnstiles.

The authentication, authorization and access protocols described above are illustrated in Figure 1. The entire process showcases a robust and redundant security framework with multiple checkpoints to ensure that only authorized employees are allowed access to the workplace and its systems. Although the verification at the physical and logical levels is thorough, it adds significant complexity to the process. Fingerprint biometric authentication is known to be problematic. Additional inconvenience can be attributed to an employee having forgotten or lost their badge. Further risks can be associated with badge theft, when the badge is damaged or if the employee's right-hand index finger sustains an injury rendering the fingerprint useless. This cumbersome process is very time consuming, leads to needless AAA events and is difficult to maintain. An ECG-wearable authentication device, on the other hand, offers always-on authentication, is unique to the end user, is practically impossible to forge and is guaranteed to allow access to the designated employee and not an impostor.

1.2 Goals of the Study & Solution Proposal

The problem that my research will attempt to uncover is related to the feasibility of changing one's behavior pattern so that an ECG-wearable authentication device is used to conduct AAA Events in the workplace. Specifically, I will investigate the feasibility of device acceptance by using the Technology Acceptance Model and then by extending it to include additional variables in order to define, understand and evaluate whether such devices will be accepted, deployed and used to the extent possible to prevent fraudulent activities by validating identity, granting access or authorizing usage. A survey instrument will be distributed to users in the workplace through which targeted data is collected and analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM).

1.3 Why Is The Research Problem Significant?

The significance of this problem is primarily related to the uncertainty of acceptance. My research will attempt to answer questions related to whether users will adopt such devices, through the study of the Technology Acceptance Model along with a unique extension featuring three additional attributes: Experience, Subjective Norm and Perceived Risk.

Technology life cycles often witness convergences of devices and applications. We are in the midst of a proliferation of wearable devices for a variety of lifestyle applications such as bioinformatics and fitness. The widespread usage of mobile devices is accompanied by an increased reliance on these devices to conduct daily activities such as communications (email, text, video chat), financial transactions (account balances, bill pay), electronic commerce (retail and online purchases), and secured access (boarding pass).

Due to reduced cost factors and increased competition, we are also seeing a convergence of wearables and mobile devices that extend into unique applications such as authorization of access and authentication of identify. It is therefore a matter of time before we start seeing more usage of wearable devices to extend beyond the examples stated above, such as the usage of ECG to conduct AAA Events.

1.4 What Is Known About The Research Problem?

While smartphone availability, affordability and relative ease of use have caused widespread adoption, wearable devices that are mostly geared to bioinformatics or using ECG-authentication such as the Nymi band, are still in the early stages of adoption. Although convergence is expected to occur with advances in sensors found in smartphones and added features in fitness bands, some of the challenges I will face as I research this problem include:

- Lack of acceptance data due to lack of industry standards towards commercial development, support, and deployment
- Uncertainty towards adoption by private enterprises
- Competition from traditional, well established and less costly biometric authentication systems including fingerprints, iris scans or voice recognition.

1.5 What Is Unknown About The Research Problem?

Wearable technology is becoming more affordable. Innovations are driven by demand, features and usability. Although numerous studies have been conducted on the acceptance and deployment of wearables such as garments, fitness bands, necklaces, eyewear, smart watches, and smart jewelry, the usage of ECG authentication in a wearable device remains a capability

that has yet to be fully and reliably implemented. As a result, it is unknown if ECG wearable authentication will be a viable solution in the workplace; or, if it will be easily added as a feature to smartphone or other wearable devices.

1.6 Expected Contributions

After conducting the survey and studying all outcomes and results, I expect to find evidence that supports TAM extension hypotheses where by users are likely to accept using an ECG-based wearable authentication device when conducting AAA Events. Further, I expect to find support to the hypotheses that using such wearable devices requires behavior modification in attitude, perceived use and perceived ease of use which are the fundamental foundations of the Technology Acceptance Model.

The ultimate contribution of this research is to lend significant credibility to the potential usage of ECG-wearable authentication devices on a personal scale, to protect one's private personal data and reduce incidents of identity theft. Consequently, the wearables industry can benefit by understanding product implementation acceptance factors while identifying where and how individuals will want to use ECG-wearable authentication devices. Although some limitations will be present, this study will attempt to remain age, gender and culture neutral so as to provide unbiased findings, results and recommendations.

1.7 How This Dissertation is Organized

Following this introduction, the remainder of the dissertation is organized into these chapters:

- **Chapter 2: Literature Review & Foundational Elements**. In this chapter, a comprehensive review of research literature and foundational elements is presented. First, the reasons for using the Technology Acceptance Model are explained by visiting antecedent concepts such as the Information Integration Theory, the Theory of Reasoned Action, the Theory of Planned Behavior, and the Diffusion of Innovation theory. This historic perspective is important as it explains and validates the choice of using the Technology Acceptance Model to aid the goals of this study. Second, an explanation of the Electrocardiogram and its potential of biometric authentication is provided. Evidence is presented, through existing research, which supports a variety of classification and authentication modalities for ECG usage as a biometric. This leads the study into combining TAM with ECG biometric authentication to form the research models of technology acceptance presented in Chapter 3.

- **Chapter 3: Problem Solution Design - PLS-SEM & Study Hypotheses.** This chapter begins by explaining why Structural Equation Modeling with Partial Least Squares was chosen as the research methodology for this study. SEM is often used in market research to test single or multi-order causal models and is suitable for research that is exploratory in nature, where latent (unobservable) constructs are frequently used. Next, detailed inner and outer models are constructed, a determination is made to select the reflective model, and then sample size determination is performed to ensure the validity