2018-02-01

Keystroke Dynamics: Utilizing Keyprint Biometrics to Identify Users in Online Courses

Jay Richards Young
Brigham Young University

Keystroke Dynamics: Utilizing Keyprint Biometrics to Identify Users in Online Courses

Jay Richards Young

A dissertation submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

Randall Davies, Chair
Jeffrey Jenkins
Ross Larsen
Richard West
Stephen Yanchar

Department of Instructional Psychology and Technology

Brigham Young University

ABSTRACT

Keystroke Dynamics: Utilizing Keyprint Biometrics to Identify Users in Online Courses

Jay Richards Young
Department of Instructional Psychology and Technology, BYU
Doctor of Philosophy

This study examined the potential use of keystroke dynamics to create keyprints (typing fingerprints) to authenticate individuals in online assessment situations. The implications of this study are best understood in terms of the keystroke behavioral biometric. While previous studies considered the degree to which keystroke typing patterns are unique, this study was set up to determine how well keyprints are able to identify individuals when typing under various treatment conditions (copy typing, free typing, and typing with mild or moderate impediments). While authentication can be difficult when attempting to correctly identify individual users, the results of this study indicate that keyprints can be a solid indicator of negative cases (i.e., flagging situations where a typing sample is likely not the correct individual). As anticipated, typing with a temporary impediment does diminish the algorithms' ability to identify students. This is also the case when user samples are typed under conditions different from those in which the keyprint baseline signature was captured (i.e., copy versus free typing). The ability to identify individuals is also challenging when using small comparison samples. However, the ability of the system to identify negative cases functions fairly well in each instance.

Keywords: keystroke dynamics, keyprint signatures, online assessment

ACKNOWLEDGEMENTS

To my wife and children whom I love more than I have words to express. To my mentor and friend, Randall Davies, who believed in me and worked with me to accomplish this study. And finally, I would be remiss not to acknowledge that this work is made possible by those who cheat and deceive, attempting to get something for nothing by getting someone else to do their work. Without them, this kind of research would not be needed.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

The prevalence of online education has increased dramatically in the past decade due in part to several significant benefits online learning offers (The United States Higher Education System, 2016; Freidman, 2016; Newton, 2015). Among those benefits are accessibility, schedule flexibility, and affordability (Li & Irby, 2008). However, along with the benefits of online learning come several challenges, one of which is academic dishonesty among students (Grijalva, Nowell, & Kerkvliet, 2006; King, Guyette, & Piotrowski, 2009; Sewell, Frith, & Colvin, 2010).

Unethical behavior in schools is rampant (King et al., 2009), including prestigious universities (Pérez-Peña, 2012). While cheating in school is not new, it has taken on new forms and is becoming easier to undertake due to increased use of technology to facilitate instruction and testing (King et al., 2009; Sewell et al., 2010). One particular problem for providers of online courses is the challenge of verifying the identity of students completing an online course (i.e., making sure the person doing the work and taking the test is the same person getting credit for completing the course). Moini and Madni (2009) stated, "the anecdotal body of evidence suggests that 'cyber cheating' is far more widespread than originally believed because it is nearly impossible to verify the identity of an individual being assessed online" (p. 469).

In 2008, the United States government picked up on this issue and passed the higher education opportunity act (HEOA). This act requires higher education institutions to "make greater access control efforts for the purposes of assuring that students of record are those actually accessing the systems and taking online exams by adopting identification technologies as they become more ubiquitous" (Monaco, Stewart, Cha, & Tappert, 2013, p. 2). To comply with the requirements of this law, institutes of higher education who provide online courses have

begun exploring the use of biometrics to authenticate students. This includes how science and technology can be utilized to identify physiological or behavioral attributes that are unique to individual students (Karnan, Akila, & Krishnaraj, 2011).

Commonly used biometric indicators (e.g., finger or palm prints, iris scans, facial and voice recognition) are effective because technology can fairly accurately authenticate a user's identity by comparing samples of unique physiological characteristics (Karnan et al., 2011). The main concern with using biometrics in the authentication process is systems needed to capture and compare these metrics can be prohibitively expensive to implement (Panchumarthy, Subramanian, & Sarkar, 2012; Jenkins, Grimes, Proudfoot, & Lowry, 2014). They can also be somewhat intrusive (e.g., taking facial recognition videos while working on a course). These biometrics are good *gatekeeper* measures (i.e., verifying entry into the system similar to using a password); however, they do not serve well as in-system verification tools (i.e., once admitted into the learning system by a verified user, who is actually completing the work). Behavioral traits such as handwriting, signatures, *keystroke dynamics*, and mouse dynamics can be used like physiological characteristics to identify individuals (Karnan et al., 2011). Metrics using keystroke and mouse dynamics can examine the behavior of those admitted into the learning system to verify the person completing the course work is the person signed up to take the course. These metrics can be somewhat less accurate than physiological characteristics as they often change slightly depending on circumstances, but they are less obtrusive and obtained during the process of an individual completing work in the course rather than merely at the beginning of a work session (Marsters, 2009).

Joyce and Gupta (1990) speculated that keystroke dynamics in *online assessment* could lead to increased security when a learner is completing a test unsupervised at a distance using technology. Keystroke dynamics record and analyze the way a user types, based on habitual typing patterns (Monrose & Rubin, 2000). Like a fingerprint or a signature, we theorize that individuals can be identified using keystroke dynamics to create what we call a *keyprint* that represents their typing behavior. Monrose and Rubin (1997) suggest that the use of keystroke dynamics to create a typing signature for individuals is the most reasonable and cost-effective approach for institutions of higher-education looking to improve their online assessment security. Multiple studies verify that keystroke dynamics work in free text and password scenarios and using multiple analysis techniques (Giot, El-Abed, & Rosenberger, 2011; Flior & Kowalski, 2010; Killourhy & Maxion, 2009; Killourhy & Maxion, 2008; Gaines, Lisowski, Press, & Shapiro, 1980; Spillane, 1975).

Research Purpose

The purpose of this proof of concept study extends the work done on keystroke dynamics as a potential tool to authenticate students as they complete work in an online course. It considers the ability of keystroke detection algorithms to identify students typing under various conditions. Specifically, this study was designed to consider the ability and accuracy of using keyprints to identify typing samples under various conditions that might decrease the accuracy of the authentication process (i.e., task difficulty and typing impediments). This study also considered the possibility of using a reduced keyprint profile rather than a full keyprint signature as a baseline when comparing typing samples.

Research Questions

This study was designed to answer four questions.

Question 1: To what degree do keyprint signatures provide accurate user identifications of individuals when using a full keyprint signature as a baseline comparison? We hypothesized that our findings would be similar to findings from previous studies that found this technique to be a viable solution to the problem of user identification.

Question 2: To what degree do keystroke dynamics provide accurate user identification of individuals when using a reduced keyprint profile as a baseline comparison? We hypothesized that using a reduced set of keystroke characteristics that included only those keystroke features that were unusual or somewhat outside the norm for individual typists would provide a more accurate identification of individuals in terms of reduced false positive and false negative results.

Question 3: To what degree does task difficulty impede the ability of keyprint authentication to accurately identify individual typists? We hypothesized that there would be a reduction in accuracy when individuals free type a response as compared to copy typing text.

Question 4: To what degree does typing with a mild or moderate impediment alter the ability of keyprint authentication to accurately identify individual typists? We hypothesized that there would be a considerable drop off in user identification accuracy when individuals were typing with a mild or moderate impediment.

CHAPTER 2: REVIEW OF LITERATURE

Biometrics authentication is "the science and technology of authentication by identifying the living individual's physiological or behavioral attributes" (Karnan, Akila, & Krishnaraj, 2011, p. 1565). Keystroke dynamics is defined as the process of analyzing the way a user types in an attempt to identify individuals based on typing patterns (Monrose & Rubin, 2000). Online assessment is "the application of formative [and summative] assessment within learning online and blended settings where the teacher and learners are separated by time and/or space and where a substantial proportion of learning/teaching activities are conducted through web-based ICT [Information Communication Technology]" (Gikandi, Morrow, & Davis, 2011, p. 2337). Online identity verification is the confirmation of a focal person identity using supporting evidence (Meng & Agarwal, 2007). Online assessment security is the process of decreasing the actual and probable occurrences of cheating in an online course context (Caldarola & MacNeil, 2009).

Online Assessment Security

The role of online assessment security is to secure the institution against improper manipulation by the students (Graf, 2002). Cheating is easier due to technology providing anonymity for the actual user; as a result, there is a greater need for security in the form of student verification for online courses and with online assessments. For example, when taking a non-proctored online test, a student could use the internet to search for answers to the questions posed, or could have a friend, who excels in the subject, take the exam for them. Such manipulation discredits the exam being taken as well as potentially implies a false level of competence for a student. Examples of the myriad of ways students have been caught cheating include: plagiarism (McMurtry, 2001), checking notes on their mobile device during exams,

texting friends for answers to test questions, warning others of quizzes, telling others of test answers (O'Shaughnessy, 2009), accessing full exams online, hiring a surrogate, pay-to-pass, emailing friends for answers, emailing friends the test answers, and taking pictures of the exam and disseminating (Simkin & McLeod, 2010).

Online assessment security decreases the occurrences of cheating (Caldarola & MacNeil, 2009). This is accomplished by using deterrent factors such as strategically placing integrity reminders encouraging students not to cheat (Hricko & Howell, 2006), employing authentication verification using biometrics (Ahmed & Traore, 2007; Saevanee, 2014), and specifically using keystroke dynamics as the primary biometric by which online assessment should be governed (Tapert, Villani, & Cha, 2009; Yu & Cho, 2004).

Biometrics collect "behavioral or physiological characteristics to establish or verify a precise identity" (Ahmed & Traore, 2007, p. 165). Accuracy depends on the specific biometric used. "Physiological biometrics—including finger scan, iris scan, retina scan, hand scan, and facial scan" (p. 165) are quite accurate in precision, however, the cost for such precision in most cases is high (Monrose & Rubin, 2000; Yu & Cho, 2004). Behavioral biometrics measure human actions (Ahmed & Traore, 2007, p. 165) which are accurate, although not as accurate as physiological biometrics can be, and almost free to implement (Gunetti & Picardi, 2005; Jenkins, Grimes, Proudfoot, & Lowry, 2013; Monrose & Rubin, 2000; Yu & Cho, 2004). With cost being a significant issue for higher education institutions, keystroke dynamics becomes a logical step to improving user identification authentication in online assessment security.

Keystroke Dynamics: The Method

"Keystroke dynamics are the patterns of rhythm and timing created when a person types" which can then be used to verify identity (Yu & Cho, 2004, p. 428,). This is done by monitoring and measuring an individual's keystroke dwell times (the amount of time a key is depressed) interwoven with flight times (time between the previous key up and the next key depression) (Chang, Tsai, Yang, & Cheng, 2011; Yu & Cho, 2004) and then identifying them based on their habitual rhythm typing patterns (Monrose & Rubin, 2000). The identification is done by using inexpensive software or code to track a user and match their usage against their usage history (Keystroke dynamics, 2015).

Tracking is done using "keystroke digraph latency times" (Leggett, Williams, Usnick, & Longnecker, 1991, p. 862). Software measures the amount of time that lapses between two adjacent letters. For example, if a student named Mary were typing her name, she would sequentially type M, A, R, and Y. Keystroke digraph latency measures the "time elapsed between the keypresses for the letters of the digraph", in this case "MA," "AR," and "RY" (Leggett et al., 1991). These data on Mary's individual way of typing enable the software to identify Mary in future interactions.

There are additional ways to extract data from keystrokes that go beyond digraph latency according to Rybnik, Tabedzki, and Saeed (2008). They claimed that in addition to dwell and flight times, keystroke data can be extracted using:

- **"typing speed** – average number of keystrokes per time interval,
- **overlapping of specific keys combinations** (especially 'shift' or 'Caps lock' for writing capital/small letters, but also overlapping of letters predicated by fast typing),

- **amount of errors** (and how often a user uses delete or backspace keys),
- **method of error correcting** (selecting text before or deleting letters one by one, as well as a manner of typing used for corrections that may be very distinct as in most cases only one key will be pressed),
- **cursor navigation-specific keys** (keys like arrows, home, end, page up, page down, etc.)" (p. 226).

Flior and Kowalski (2010) added two additional ways to extract keystroke data:

- **keystroke seek time** defined as "different letters take a different amount of time for the user to locate and press. This can be rather unique, as a typical keyboard has 105 keys, which gives at most 105 potential combinations of seek-time, assuming the seek time for each key is different;" and
- **examination of characteristic errors** including "holding the shift-key for too long, resulting in backspacing, or simply common typographical errors. If these common errors can be recorded, they also provide a reference against which the user's identity can be checked" (p. 490).

Jenkins et al. (2014), added **transition time,** defined by latency between key presses.

According to Joyce and Gupta (1990), keystroke dynamics were effective in identifying individuals who fraudulently tried to have someone else do the task for them. They did this by capturing the patterns of thirty-three users typing; each user typing their login and password info at least eight times. Each user then logged into their account five separate times, while six of the users were randomly selected to have their accounts potentially hacked by the twenty-seven other users yielding 810 total imposter attempts. Of those attempts, only two imposters were not caught (99.75% success rate). This miniscule imposter rate is because each user has his or her

own distinct typing pattern which consists of overlapping of specific keys combinations, amount of typical errors they make, method of error correcting, and/or cursor navigation-specific keys usage (Karnan, et al., 2011). Our typing behavior is similar to a fingerprint, a voice, a retinal pattern, or a physical description; it is unique to us and difficult to duplicate. In other words, it is "not what you type, but how you type" (Monrose & Rubin, 2000, p. 353).

For Rybnik, Tabedzki, and Saeed (2008), however, keystroke dynamics have issues because typing precision changes as skill improves; it is not a static ability. Additionally, a user's health state being altered (e.g., injury to a finger or hand) can affect keystroke dynamics. Software can address these kinds of changes in keyboard ability but requires updating typing samples first (Gunetti & Picardi, 2005). According to Lau, Liu, Xiao, and Yu (2004), the disadvantages to using keystroke dynamics include inconsistent typing patterns based on fatigue, mood, and health; differences in which keyboard is being used; and differences in whether the typist is standing, sitting, using good posture, or multitasking. The advantages include keystroke dynamics being unobtrusive, inexpensive, easy-to-collect data and can be done from virtually anywhere using an internet connection (Lau et al., 2004). Keystroke dynamics are non-invasive for users. Non-invasive does not necessarily mean concealed. While users do not have to know it is being used to track their keystrokes, it may be obvious to users when they are asked to type to authenticate themselves.

In their study of keystroke dynamics accuracy with passwords, Killourhy and Maxion (2009) collected data to evaluate anomaly detection results seeking to understand if there was a change in the way passwords were input compared to imposter attempts. They gathered their data from fifty-one subjects who typed over 400 passwords each with the "three top-performing detectors achiev[ing] equal-error rates between 9.6% and 10.2%" (p. 125). It is important to

point out that anomaly-detection is one of many different techniques used in keystroke dynamics to identify imposters, and also very different from the detection percentages Joyce and Gupta's study identified. For Killourhy and Maxion, a 10% error rate was decent, but was in their estimation too high. It should be noted that less than .001%, is the European standard for access-control systems (2009, p. 125). As an attempt to supplement anomaly detection, Flior and Kowalski (2010) developed a software solution combining HTML, PHP, MySQL and JavaScript to record key events (dwell and seek) and calculate the correlation between them. Such software solutions provide ways to continuously authenticate and track student progression through an exam, thus improving online assessment security.

Security Methods

One way to know who is taking online courses is to have students provide a government-issued ID. However, that kind of ID could potentially be forged and it is still unclear, even after the ID is provided, if they are who they say they are. Because of these insufficiencies, many universities have embraced additional measures such as video recording the student taking a course, face-to-face observation, or appealing to the personal integrity of the student. Even with these extra measures, the person taking the assessment is not necessarily the person enrolled in the course.

There is a need for stronger online assessment security. Keystroke dynamics are a security feature that has potential to help strengthen online assessment security by mitigating cheating and authenticating identity (Ahmed & Traore, 2007; Giot, Dorizzi, & Rosenberger, 2015; Jenkins et al., 2013; Miguel, Caball, Xhafa, & Prieto, 2015; Sewell et al., 2010).

Implications for using keystroke dynamics. There are some important implications for including keystroke dynamics with online assessment that need to be addressed because it would force some important behavioral changes. For example, there would be greater awareness by students that they need to do their own authentic work. "Knowing ahead of time that the system will be determining whether or not the student is actually answering the questions provides a deterrent effect, impressing on the students that the work must be their own" (Flior & Kiwolski, 2010, p. 492).

Additionally, administrators and instructors would have more concise evidence on where to focus their administrative resources. Keystroke dynamics reporting would flag problem areas (i.e., who is potentially cheating) allowing school administration to more precisely allocate scarce human resources. Using keystroke dynamics in online exams would alert administrators and instructors to areas of concern as well as give them "reason to suspect that the [student] who wrote the examination is not the student registered in the class" (p. 492). Armed with such evidence, administrators and instructors would potentially be able to mitigate the issue more meaningfully for all parties involved.

Another implication for including keystroke dynamics with online assessment is the saving of time. Students could theoretically take their exams in a non-proctored environment—freeing up both student and instructor time (Alexander, Bartlett, Truell, & Ouwenega, 2001). Online testing is convenient for students and instructors. For example, students would not need to worry about travel time (which for some is extensive, depending on where they live in proximity to the university or proctor), travel preparation (e.g., putting gas in the car, clearing the snow off), travel issues (e.g., traffic, accidents), or parking issues (e.g., finding a space).

Instructors would not need to worry about similar issues, plus they would have added time savings such as convenience for scheduling the exam (can be completed at 11:59 pm while the professor sleeps), fewer to grade because much of it is done by the computer, and automatically entering the grades (2001).

Implementation cost. Including keystroke dynamics in online assessment security would also save money. Most institutions, like the University of Georgia, already administer many of their exams online, but there is a need for proctoring, which demands money and human resources (University Student Services, n.d.). Keystroke dynamics could assist in refining where resources are allocated by potentially removing the need for face-to-face proctors in administering online exams.

In addition to saving time and lowering costs, school administrators would need to consider some of the technical implications associated with keystroke dynamics like how to use it (i.e., in online exams, throughout the entire course). Using keystroke dynamics in these ways could help identify if a student is having someone else do their work for them.

Successful use of keystroke dynamics. Keystroke dynamics could be paired with mouse dynamics to increase user authentication information data and improve the identification authentication process. Mouse dynamics involve "a signature that is based on selected mouse movement characteristics, which are computed using statistical techniques" (Ahmed & Traore, 2007, p. 165). Combining keystroke dynamics with mouse dynamics "would increase the complexity of input data for analysis but surely [limit] the possibility of similar inputs for two different identities" (Rybnik et al., 2008, p. 230). Having these two data points would potentially improve imposter detection accuracy percentages as well.

In the current online marketplace, existing professional test-taking services offer services to students to take an entire course for them--as the student--guaranteeing a high grade. These services are not cheap, costing as much as or more than the fee to take the course. However, with little effort, students can deceive the administration of a higher institution of learning, fraudulently improve their GPAs, and deceitfully increase their potential options for acceptance into harder-to-get-into graduate schools or access to higher-paying or more prestigious jobs. One class sometimes makes all the difference.

Current utilization of keystroke dynamics. Such an advantage, dishonestly gained, creates an unfair playing field for students, harming both the integrity of the student and the institution where they are studying. Federal laws, like the previously mentioned HEOA, demand institutions ensure appropriate technologies are in place to guarantee a student's ID. In addition to the governmental regulations, accrediting bodies have made this a part of their accreditation practices. As of their latest printing, The Southern Association of Colleges and Schools standard 4.8.1 asserted that an institution offering distance or correspondence education needs to demonstrate that the student who enrolls in a course needs to be "the same student who participates in and completes the course or program and receives the credit by verifying the identity of a student who participates" (p.40). If an institution does not meet this standard, the likelihood of receiving accreditation decreases. In response to these pressures, institutions like Coursera, a "social entrepreneurship company that partners with universities to offer free courses online" (Vrankuli, January 2013, para. 1), have begun using keystroke dynamics to verify the identities of their students. They are doing this by having students "create a biometric profile of their unique typing patterns by typing a short phrase. When a student submits work in the course, they authenticate their identity by typing the same short phrase, with which identity can

be verified through comparison to their recorded typing samples" (2013, para. 3). Coursera is not alone in its employment of keystroke dynamics. MIT and Harvard are also using it with their massively open online courses (MOOCs), by requiring students to type out a preselected phrase and then using that phrase to verify a student's identity (Talavera-Franco, April 2014). Using keystroke dynamics as a way to mitigate fraudulent academic activity and to ensure student identification is wise for an institution of higher learning to incorporate.

A quick Google search for keystroke dynamics software yields multiple decently effective software packages available for free download. Of course, these free versions are basic packages limited to small quantities of users with more users available for a higher cost. For institutions of higher learning where users will most likely be in the thousands, an enterprise license will likely need to be negotiated, depending on specific institutional needs and goals. Coursera, for example, used an enterprise contract and an institutional strategy to track every key typed (KeyTrac, 2016) by their fifteen million-plus student users (EdSurge, 2015). But this approach is expensive for course providers and it caps the number of authentications and identifications that can be completed, limiting the effectiveness of potential continuous authentication. EdX (5 million-plus users) and Udacity (four million-plus users), competitors of Coursera, do not employ keystroke dynamics—opting for face-to-face discussions and competency interviews (2015). They do this partially because they believe the qualitative assessment gives them a better feel of authenticity than keystroke dynamics can, and because they have the money to do so. While not the choice of all institutions, keystroke dynamics is suggested as the most reasonable and cost-effective approach for higher-education institutions looking to improve their online assessment security (Monrose & Rubin, 1997).

Conclusion and the Need for Further Research

Online assessment security is aimed at decreasing the actual and probable occurrences of cheating (Caldarola & MacNeil, 2009) as well as securing an institution against cheating by students (Graf, 2002). Keystroke dynamics aids in preventing cheating by monitoring and analyzing a user's keyboard inputs based on his or her habitual rhythm typing patterns (Monrose & Rubin, 1999). Since its inception, keystroke dynamics has shown to be valuable in authenticating users (Ahmed & Traore, 2007; Flior & Kowalski, 2010; Graf, 2002; Gunetti & Picardi, 2005; Joyce & Gupta, 1990; Killourhy & Maxion, 2009; Lau, Liu, Xiao, & Yu, 2004; Monaco et al., 2013; Pfost, 2007; Saevanee, 2014), especially for the cost (Ali, Tappert, & Qiu, 2015; Gunetti & Picardi, 2005; Guven & Sogukpinar, 2003; Jenkins et al., 2013; Monrose & Rubin, 1997; Yu & Cho, 2004).

Combining keystroke dynamics with online assessment security, while not without its problems, is potentially an inexpensive and impactful tool that higher education institutions could look at more closely to help mitigate academic fraud.

Implementing keystroke dynamics in online assessments is likely the next step for online education. Each institution needs to be aware of its assessment goals and strategies and how keystroke dynamics can help reach them. Administration and IT departments should work closely to develop clear and meaningful policies and execution strategies.

This literature review suggests that keystroke dynamics can potentially lead to increased online assessment security. More exploration is needed, but what is clear is that while keystroke dynamics has been around for a while, little is published about its use in education journals. This means there is an opportunity for further research in this arena, in journals that reach the education audience, bringing more attention to the discipline and the topic.

Education conferences could include more topics relevant to keystroke dynamics and online assessment security, including having keynote speakers from Coursera, Keytrac, and other keystroke dynamics practitioner institutions.

The conversation about and application of keystroke dynamics usage in online assessment needs to include more voices from higher education. At these institutions, enrolling in and taking an online course is more and more a normal part of the learning experience, and so are the opportunities to cheat. Cheating is not new, and with more technology involved in the learning process, it enables more cheating. The ability to correctly identify who is taking a test online is of paramount importance to national and educational governing bodies. To follow the instituted laws, higher education institutions have begun exploring biometrics as one method for identifying users.

While biometrics are certainly a viable part of the identification process, there are some concerns. A concern with biometrics in general is that they can be prohibitively expensive, making the likelihood of usage challenging (Jenkins, Grimes, Proudfoot, & Lowry, 2014; Panchumarthy, Subramanian, & Sarkar, 2012). The keystroke dynamics biometric is potentially part of the solution, because it can reliably authenticate a user with a high degree of accuracy while remaining affordable (Lau, Liu, Xiao, & Yu, 2004).

From the literature we see two main gaps. First, there seems to be minimal research on authenticating an individual while they are participating in common assessment typing situations, such as free typing. Second, there seems to be minimal research on utilization of keystroke dynamics with typing authentication where injuries or impediments exist. Critically important to being able to address these gaps is knowing how these contexts affect keystroke dynamics verification in free typing generative list task and free typing explanatory activities as well as

with minor and moderate injuries and impediments. The research in this dissertation attempts to fill some of that gap by finding answers to these important questions. Overall, keystroke dynamics has not been used extensively in online education, and is thus still largely unknown. That will change as more research is conducted and published about the value and strength keystroke dynamics adds to online assessment security.

CHAPTER 3: METHODS

To contribute to the research needed in this area, we decided to employ a proof-of-concept (POC) methodology. This study was set up to replicate data collection and analysis from other studies. Similar to Flior and Kowalski (2010), we created a proof of concept software system to capture our data using HTML, MySQL, and JavaScript. Like Gunetti and Picardi (2005), who gathered fifteen typing samples from forty volunteers, we gathered six typing samples under various treatment conditions from seventy-eight volunteers. Like Killourhy and Maxion (2009), we used multiple methods to analyze our findings but decided on the use of a simple mean difference *t* test method. Like Yu and Cho (2004), we used ROC charts to plot data accuracy; and similar to the linguistic profiling concept Saevanee (2014) developed, we created keyprint signatures and keyprint profiles based on a set of keystroke dynamics. We set up our research design to determine the degree to which individuals had unique typing patterns similar to Joyce and Gupta (1990). In addition to simulating the methods in previous studies, the study was designed to establish and verify the degree to which keyprints might be used to identify individuals typing under more specific treatment conditions (copy typing, free typing, and typing with mild or moderate impediments). Table 1 presents terms and definitions used in this study.

Table 1

Key Terms Used in This Study

Term	Explanation
Keyprint Signature	Baseline used for comparison that includes all available data points
Keyprint Profile	Baseline used for comparison, which includes only those data points somewhat outside the norm
Match Range	Value at which paired data points in two samples were considered a match in initial analysis
Match Threshold	Percentage of matched data points required for the samples to be considered a match
Z-score Cut-Point	Value at which a dwell time or transition times were considered unusual enough to be place in the Keyprint profile
True Match	Instances when the algorithm correctly matched samples known to come from the same individual
False Negative	Instances when the algorithm failed to match samples known to come from the same individual
False Positive	Instances when the algorithm matched two samples known to come from different individuals
Critical Point for False Negatives	Point at which false negatives reach zero

Participants

University students from an Introduction to Management Information Systems course were recruited to participate in this study. Roughly 150 students were offered extra credit to provide data for this study. The class was structured in such a way that students could get extra credit points by participating in various activities or completing specific tasks. Initially eighty-four participants chose to provide data; however, data obtained from six individuals was found to be incomplete, leaving a total of seventy-eight usable sets of data. The participants were all

undergraduate students, many of whom were majoring in information systems; each possessed requisite basic typing abilities. Students who volunteered to provide data were emailed instructions (see Appendix A) directing them how to access the data capture webpage where their keystroke data could be captured as they completed six typing tasks. Participants were originally given seven days to complete the typing task, but at that time, there were just over sixty participants who had completed the activity. Since we had set a goal of getting 100 participants we extended the data collection period for another three weeks. During this time, we garnered another twenty-five participants. The majority of participants completed the typing tasks on their personal laptops; the others completed it on a personal computer.

Individuals who provided typing samples for this study were directed to an HTML page that presented them with a consent form that each participant had to complete in accordance with our approved institutional review board (IRB) procedures. Completing the consent form was not only important for IRB requirements, but it also allowed us to identify participants with unique IDs so we knew which samples were provided by specific individuals. Each participant was asked to provide six samples of typing under specific treatment conditions and knowing which sample belonged to each participant was essential to the analysis process. The consent form document disclosed the purpose for the study and asked participants to type normally. Once the consent form was completed, participants were given directions on how to complete the typing tasks.

Data Capture Procedures

Using the Google Chrome browser, we embedded JavaScript into HTML pages so we could track dwell and transition times for specific keys and key combinations. The data set (i.e., time stamps for when specific keys were pressed and released) was initially stored in JSON files

and later saved on a MongoDB housed on the Amazon Web Services (AWS) cloud. In the database, data was transformed into dwell and transition times. Dwell times were calculated using time stamps of when each key was pressed and released. Transition times were determined using time stamp differences for when the first and second keys in each combination were pressed.

Participants were expected to complete the entire activity in one sitting and the system was set up to not allow stopping the exercises and restarting later. It was believed that allowing this would have created a reliability problem with our data collection due to the fact that we would not know if they were completing the study on a different computer or more importantly using a different keyboard. We anticipate studying this and other variables at a later time. Each of the participants were asked to provide six typing samples (see Table 2). The text participants were asked to type is provided in Appendix B.

The first treatment (T1) was intended as a baseline copy typed exercise to capture each participant's normal typing cadence. Each participant was asked to type the introductory paragraph from the autobiography of Helen Keller. The paragraph consisted of 175 words (964 characters); the number of characters were similar in count to Leggett and Williams' (1988) first baseline character count. After initial data analysis, it was determined that this treatment sample would be suitable for use as the individual's keyprint signature and profile.

The second treatment (T2) was also a copy typing exercise to be used as a similar sample comparison to the first. In this case, however, the participants were provided with the concluding paragraph from the autobiography of Helen Keller--which consisted of 145 words (798 characters); the number of characters gathered were significantly higher (more than two times higher) than that of Leggett and Williams' (1988) second baseline count (see Appendix B).

We determined to use this as the baseline verification treatment sample to both check and verify that the T1 baseline sample was working and to use as the initial comparison treatment for T1 under similar data capture conditions.

The third and fourth treatments (T3 and T4) were free typing tasks. These were intended to simulate situations where the task was different from the baseline task (copy typing) in terms of cognitive effort required to complete the task. In T3 students were provided with the following prompt: "There are over 100 alternative ways to use paper clips from their intended usage, how many you can get?" In T4 participants were asked the following: "In at least 200 words, and without consulting an outside source, type out your answer to the question, what is intelligence?" For the prompt in T3, participants were given instructions that they needed to write at least 150 words, although many did not. In both tasks, participants were able to type their ideas using as much or as little time as needed. Upon completion of the tasks, similar to (Vanette, 2015) participants were asked to fill out a five-point Likert scale survey regarding the difficulty of the typing task. The expectation going into the study was that T4 would be more cognitively demanding than T3, but this assumption proved to be incorrect. Participants rated the typing difficult of sample T3 to be about the same as T4 (T3 = 3.26, T4 = 3.14). T3 did differ from T4 in the amount typed and the variety of dwell and transition times captured; however, based on a chi squared analysis, the response distribution regarding the students' perception of the difficulty for these two tasks was found to be similar ($\chi^2(4)=1.014$, $p = .908$).

The fifth and sixth typing samples (T5 and T6) were intended to mimic situations where a typist might have a temporary mild or moderate impediment when completing a typing task. Participants were asked in T5 to type an assignment with a band-aid on their right index finger. They were then asked to copy type the first two paragraphs of the Gettysburg address which

consisted of ninety-eight words or 533 characters (see Appendix B). For T6, participants typed the last two paragraphs of the Gettysburg address with tape wrapping the middle and ring finger of their left hands together. Instructions were provided, including a picture, on how to apply the tape. The Gettysburg address consisted of 143 words or 791 characters (see Appendix B). A concise breakdown of each treatment and their description is provided in Table 2.

Table 2

Descriptions of the Design Treatments Used for the Data Samples Collected

Treatment Condition	Treatment Description
T1: Baseline sample for Keyprint signature	Participants copy typed the introduction paragraph from the autobiography of Helen Keller which consisted of 175 words (964 characters).
T2: Baseline similar sample comparison	Participants copy typed the concluding paragraph from the Helen Keller's autobiography which consisted of 145 words (798 characters).
T3: Generative list task sample	Participants free typed an answer to the following prompt: "There are over 100 alternative ways to use paper clips from their intended usage, how many you can get?
T4: Explanation composition sample	Participants free typed an answer to the following question: "In at least 200 words, and without consulting an outside source, type out your answer to the question, what is intelligence?"
T5: Mild impediment sample	Participants copy typed the first two paragraphs of the Gettysburg Address which consisted of ninety-eight words (533 characters) with a band-aid on their right index finger.
T6: Moderate impediment sample	Participants copy typed the last two paragraphs of the Gettysburg Address which consisted of 143 words (791 characters) with tape wrapping together the middle and ring fingers of their left hand.

Prescreening Data Process

Before analyzing the data, we needed to clean the data set to identify any unnecessary data and remove it. According to Fawcett (2006), prescreening the data is essential to maximize the performance of the classifiers from the data being analyzed. Prescreening allowed us to remove the non-essential elements of the data, thus maximizing the performance of the algorithm. It was important to identify which keys and key combinations we would keep and

which we would exclude. The criteria for inclusion was that the typed key and key combination occurred at a relatively regular rate and that the dwell and transition time likely represented the individual's typical typing behavior.

The initial data set consisted of 1,630 different transition combinations (see Appendix D). For pre-screening purposes, each combination was tracked for transition time and the number of times it was utilized. The most used transition combination was the "backspace" key followed by the "backspace" key. This combination was typed 11,751 times across all participants. The data set contained 438 different transition combinations that were typed only once. Such limited usage of these transitions warranted their removal from the data set.

In total, we removed 1,587 transition combinations. We kept forty-three transition combinations (see Appendix D) leaving 186,659 transition times for analysis. The decisions to keep the forty-three transitions was informed by the number of times each transition was utilized, how those transitions were employed across treatments, and the similarity of the transitions to everyday typing. For example, the digraph "ea," "th," and "in" were kept because they are commonly occurring digraphs in standard English; however, ", space" was removed because a digraph consisting of punctuation can introduce measurement errors when individuals pause unnaturally after punctuation. That is not to say that punctuation digraphs were completely eliminated. We kept the ". space" digraph, but excluded instances where the transition time was greater than 1,000 milliseconds (or one second) both because the use of a period in typing is a basic skill and because it was utilized enough across treatments to warrant inclusion.

Some key combinations were determined to be less reliable examples of typical typing. The best example of this is keystroke dynamics involving the "shift" key. Data points involving the "shift" key (both for dwell and transition times) were removed because the times obtained

were considered too undependable. Li and Jain (2009), found that using the shift key to modify a character varies based on a person using the left or right hand. More importantly, the amount of time an individual holds the shift key down before typing another key varies dramatically from instance to instance for the same person.

As for the dwell time data, we collected data from roughly eighty unique keys. In the prescreening process this was trimmed to twenty-six (see Appendix D). The decision to keep these twenty-six characters was based on the number of times the characters were used and whether they are commonly used in sentences. We kept characters that had been used at least 2,388 times across all treatments. Any character that was used less than 2,388 times was removed. This was a natural cut point for the data, as the next character in the list occurred only 757 times across the six sample treatments. In addition to infrequently used keys, special characters and non-printable characters were excluded (e.g., the volume key on the keyboard was pressed by several users and was excluded from our analysis). After the initial prescreening analysis for commonly occurring instances of keys and key combinations, we were left with 572,331 data points (i.e., 385,672 dwell times and 186,659 transition times).

The last phase of the prescreening process involved excluding data points found to be unusually long. Based on an initial review of the data, we removed any characters that had a dwell time over one second (1,000 milliseconds). This was done to eliminate extreme outliers in the data set. To complete the prescreening, we removed all participants who did not complete all data capture samples. After final prescreening analysis to exclude unusually long dwell and transition times, as well as data from participants who did not complete each data-gathering task, we were left with 547,725 data points (i.e., 375,173 dwell times and 172,552 transition times).

Keyprint Profiles

Once the list of twenty-six key and forty-three key combinations to be used was completed, the mean times for each transition and dwell time for each individual's baseline sample (T1) was converted into a z-score so we could determine which dwell and transition times were outside the norm for individual typists at each data point.

One of the assumptions when using z-scores and parametric statistical analysis (e.g., mean difference *t* tests) is that the data set is somewhat normal. We initially attempted to run the Shapiro-Wilk statistical test to estimate the degree to which the data set could be considered normal; however, the Shapiro-Wilk test is known to be overly sensitive for large datasets and in R it does not run for data sets over 5,000, making this test unusable.

A visual inspection of the data set suggested the data are somewhat normal shaped; however, it is slightly skewed and has a long tail (see Figure 1). Barnes et al. (2001) suggest that in practice no data set is completely normal and that if the distribution of the sample is "not wildly non-normal,'' standard statistical methods likely work well enough (p. 81). Given the large number of data points we obtained and the somewhat normal shape of the data set, we determined that the use of z-scores to define unusual dwell and transition times was a satisfactory approach.

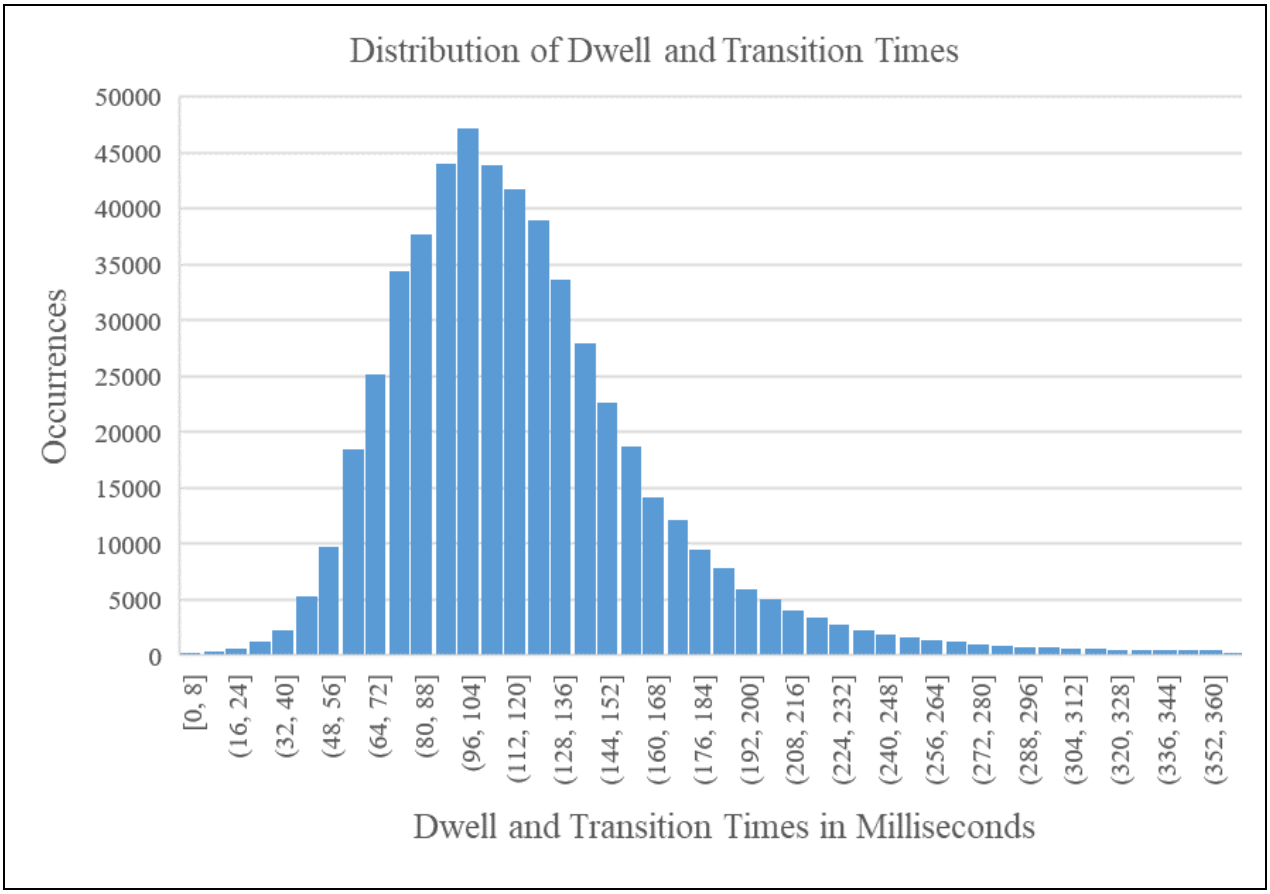

Figure 1. This figure shows the distribution of dwell and transition times of the entire dataset. A visual inspection of the data set suggests the distribution of dwell and transition times is somewhat normal, however the data are slightly skewed with a long tail.

A descriptive analysis of the number of data points in each keyprint was conducted for each possible z-score cut point we might use (see Table 3). The ideal cut-off point identified for this study was 0.5, because anything higher resulted in too few data points in each profile on average. Additional evidence that the data set was normal enough to use z-scores was provided by an analysis of the theoretical normal curve. In theory, it is expected that 38% of the data will fall between the -0.5 and +0.5 standard deviation from the mean of a normally shaped distribution, leaving 62% of the data outside this range.

In our data, using a z-score of +/- 0.5, the average number of data points in each profile was forty-one of sixy-nine possible (i.e., 60%). In theory, we should have had 62% of the data points in the profiles, but we felt the results were adequate for our purposes.

Table 3

Optimal Z-score Cut Points Analysis Data

Z-score cut points	1.00	0.9	0.8	0.7	0.6	0.5	0.4
Min	4	5	9	12	18	23	29
Mean	19	23	27	31	36	41	46
Max	46	52	56	60	66	66	67

Note: The complete keyprint signature included sixty-nine keys and key combinations. The keyprint profile was to include only those keys outside the norm while maintaining a sufficient number of dwell and transition times in each profile to compare. It was determined that 0.5 met this criterion.

Treatment T1 was used to establish keyprint baseline comparison samples for each of the participants. The keyprint signature included the average transition and dwell times (sixty-nine total data points) for each individual. The keyprint profile was established for each individual and included only the atypical or unusually long or short dwell and transition times for each individual. Using a z-cut point of 0.5, the keyprint profiles for participants in this study had between twenty-three and sixty-six unique typing behavioral characteristics.

Data Analysis

With the prescreening complete, the data analysis process consisted of calculating the number of false negative and false positive classifications at each match threshold given that we know the identity of each individual providing each sample. The results were presented using receiver operating characteristic (ROC) charts for continuous output (i.e., depictions of class membership results at different thresholds). This was done to establish optimal threshold points

(i.e., where the number of false negative and false positive is balanced) and critical points for false negatives (i.e., the point at which the probability of incorrectly classifying samples known to match is zero).

Matching samples consisted of comparing the keyprint signature and profiles with samples obtained from each of the treatments separately, all other samples combined, and only those samples obtained under different conditions to the baseline sample (i.e., free typed and typed with an impediment).

A sample match was determined by conducting a mean difference *t* test ($\alpha = 0.05$) for each data point in the samples. The degree to which two samples match was determined by calculating the percentage of data point matches. This was then charted for each potential match threshold. Given that the distribution of the data set is not completely normal, we initially conducted the analysis using a simple match range procedure (i.e., data points were considered a match if they were within +/- 50 milliseconds of each other). We also employed a non-parametric Wilcoxon-Mann-Whitney test and, based on 5,376 comparisons, the *t* test and Wilcoxon had a 92% agreement on matches; the *t* test, however performed better at reducing false negative classifications. Using the match range method, we obtained suboptimal results compared to the other two methods (see Figure 2). As a result, we used the *t* test method to determine matches for each data point comparison.

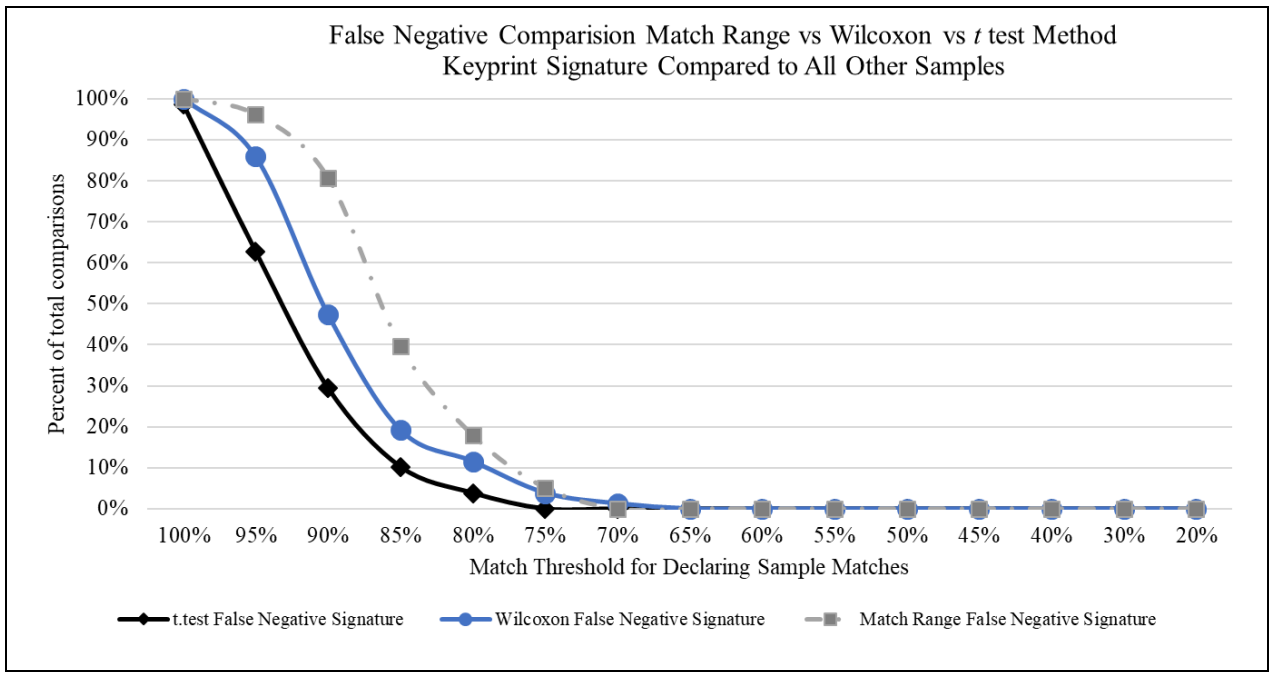

Figure 2. This figure shows the comparison of Match Range Versus Wilcoxon-Mann-Whitney Versus *t* test Method Keyprint Signature Compared to All Other Samples. Among the three methods, the results were somewhat similar but the *t* test method performed better overall. The *t* test performed better between 75% and 100% and hit the critical point for false positive at 75%. Using the non-parametric Wilcoxon method and the match range methods resulted in suboptimal performance compared to the *t* test method.

One additional consideration we needed to make was how to calculate the percentage of data point matches. Two methods were considered. The first method (method 1) consisted of calculating percentages based on the total number of characters in a signature or profile regardless of whether the comparison sample included any instances of that key or key combination being typed. In other words, we treated all missing data as a non-match and divided the number of matched data points by the total number of data points in the baseline signature or profile. Using this method drastically increases the number of false negatives for samples with missing data points. For our data set this only had a major effect on one sample (T3). Most of the data samples contained little missing data.

The second method (method 2) involved excluding instances of missing data and reducing the total number of data points comprised in the percent matched calculation by the number of missing data points. Method 2 considered only available data point comparisons when calculating the percentage of data point matches, which decreased the number of false negative mistakes. We decided to use method 2 as the reporting method in the results section because our study was more concerned with an accurate estimate of false negatives (see Figures F5 and F6 in the appendix). With the exception of Figure F6, the results tables in Appendix E use method 2 when calculating data point matches.

One last issue involving missing data was that of when not to complete a comparison in situations where there were too few data points to compare due to missing data points in the comparison sample. Again, this was only an issue when using the profile baseline for treatment T3. We decided to use a *too few* cut point of ten data points. Comparison that contained fewer than ten data points to compare were excluded from the results, given that there was likely not enough information from which a comparison could be made. The robustness of our matching algorithm in terms of missing data is something we plan to test at a later time.

CHAPTER 4: RESULTS

While analyzing the data, many interesting connections between keyprint signatures, using all characters, and keyprint profiles, using only the unique keys to authenticate identity were found. This section is organized by each research question presenting results pertinent to each issue. A full set of result tables and ROC charts is presented in Appendix E.

Keyprint Accuracy for Baseline Samples

To answer to our first research question, we compared each of the keyprint samples in the baseline treatment T1 to each of the other keyprints obtained. Each of these are known not to match, as they were provided by different individuals. We wanted to determine the degree to which keyprint signatures and profiles were unique to individual students. Figure 2 presents the results for this analysis.

From the information presented in this chart we found that keyprint signatures and keyprint profiles were unique. When match comparisons were conducted using match thresholds for 100% to 80%, no two keyprints were the same (i.e., no false positive matches were found). Once the match threshold got below 80% we did start to get false positives. This means that we started seeing keyprints that were similar enough at that match threshold to be considered a match even though we know they were typed by two different individuals. The lower the match threshold used to determine sample matches, the higher the number of false positives. The use of the keyprint profile performs slightly better at reducing false positive occurrences compared to the keyprint signature at low match thresholds. In general, this finding replicates findings from other studies that show keystroke dynamics are unique for different individuals. The evidence supports our hypothesis that keyprints are unique to some extent and could be used to provide accurate user identification of individuals.

Keyprint Profile Accuracy Question

Our keyprint profile accuracy question focused on whether keystroke dynamics provided accurate user identification of individuals when using a reduced keyprint profile as a baseline comparison. We hypothesized that using a reduced set of keystroke behaviors that included only those keystroke data points that were unusual or somewhat outside the norm for individual typists would provide a more accurate identification of individuals in terms of reduced false positive and false negative results.

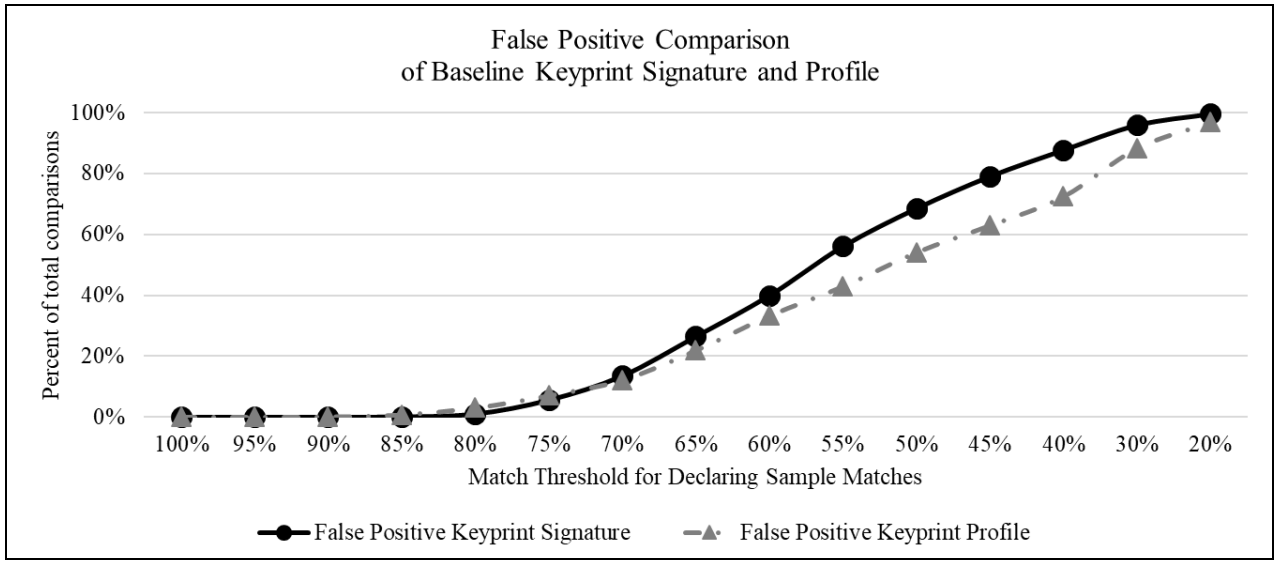

Figure 3. This figure shows the False Positive Occurrences for Baseline Keyprint Signatures and Profiles in Sample T1 at Each Match Threshold**.** Based on this analysis, the critical point for false positive occurrences is between 80% and 85%. This result indicates that at or above an 80% match threshold, each keyprint for the individuals in the data is completely unique.

To check our hypothesis, we compared the keyprint profile along with the keyprint signature to see how each fared. Figure 3 presents false positive and false negative results when comparing keyprint signatures and profiles against all the other typing samples combined. The comparison sample in this case is a composite of copy edit, free typed, and typing with a mild or moderate impediment.

The results of our analysis suggest that using the keyprint profile reduced the number of false positives the algorithm identified compared to the keyprint signature (i.e., matching samples when they were known to have been typed by different individuals). This was especially the case when the match threshold was below the optimal point for false positives. However, using the profile underperformed compared to the keyprint signature in the number of false negatives (i.e., mistakes) the algorithm made when matching samples known to have been typed by the same individual. The keyprint signature was more accurate and contained less error. Because in the context of our study we are more concerned with limiting false negatives (i.e., falsely accusing individuals of not being themselves), our data does not support the hypothesis that using a keyprint profile would be a better method for comparing typing samples. In this case more data is better. Based on this result, the remainder of our analysis will focus on the keyprint signature; however, the keyprint profile is presented alongside the signature for comparison purposes. Figure 4 presents false negative and false positive results when comparing keyprint signatures and profiles against copy typed samples.

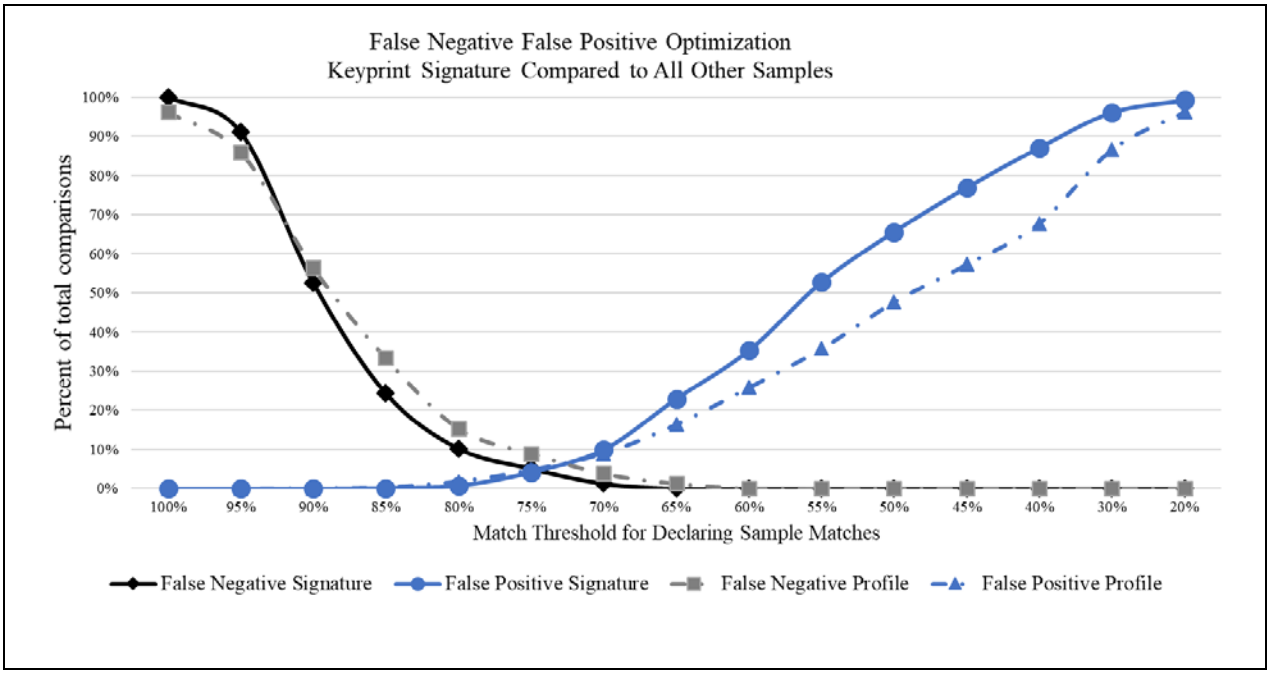

Figure 4. This figure shows the False Negative and False Positive Optimization for Keyprint Signature and Profiles Compared to All Other Typing Samples Combined (T2-T6). Optimization occurs at a match threshold of approximately 75%. This is the point where false positives and false negatives are optimally balanced. However, the critical point for reducing false negative identifications to zero using the keyprint signature is approximately 70%. The critical point for reducing false negative identifications to zero using the keyprint profile is closer to 65%. In this regard using the keyprint signature is better than the keyprint profile.

Comparison in Context

In our analysis, we studied whether different typing conditions affected the algorithm's ability to correctly match samples. We compared copy typed keyprint signatures to samples that were copy typed, free typed, and copy typed with impediments.

Keyprint accuracy with copy typed samples. Our keyprint accuracy context for copy typed samples focused on whether keystroke dynamics provided accurate user identification of individuals who provided a sample under similar typing conditions to that of the baseline keyprint. Figure 5 presents false positive and false negative results when comparing keyprint signatures and profiles against copy typed samples. The analysis in this case is a comparison of a copy typed baseline (T1) with copy typed sample (T2).

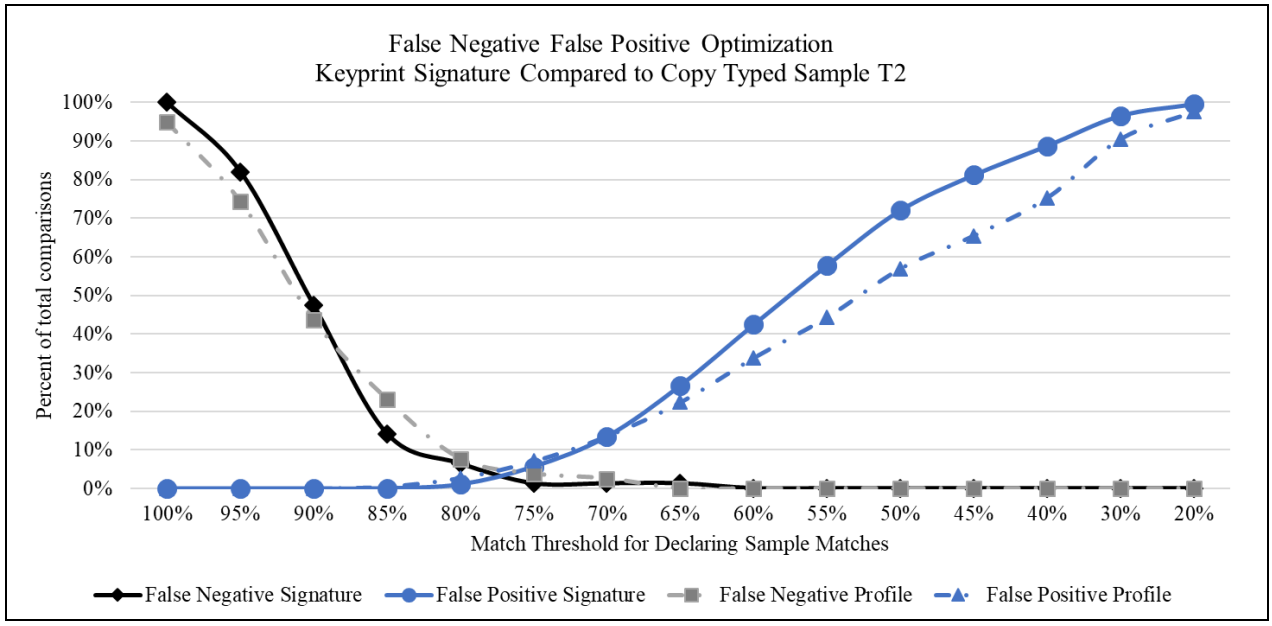

Figure 5. This figure shows the False Negative False Positive Optimization Keyprint Signature Compared to Copy Typed Sample T2. Optimization occurs at a match threshold between 75% and 80%. The critical point for reducing false negative identifications to zero using the keyprint signature is approximately 75%.

The results of our analysis show that when comparing a copy typed sample to the baseline keyprint signature, the algorithm functions fairly well. Clearly individuals are not robots. Unlike a fingerprint, each captured typing sample will never be completely consistent for every data point being compared. However, in practice, if a typing sample (provided under similar conditions to the baseline) does not match the keyprint signature on at least 75% of the data points, based on these results, it would be highly unlikely that the two samples were provided by the same person.

Keyprint accuracy with free typed samples. Our keyprint accuracy context for free typing samples focused on whether keystroke dynamics provided accurate user identification of individuals when the sample was provided in a different context to that of the keyprint. To determine this, we compared free typed samples to the copy typed baseline under two treatment conditions. In the first situation (T3) the sample context involved free typing a generative list task response. In the second situation (T4) we collected a free typed sample of explanatory writing. We hypothesized that there would be a reduction in categorization accuracy when individuals free typed a response as compared to copy typed keyprint signature. Figure 6 presents the results when comparing the baseline sample T1 with the generative list task writing sample T3. Figure 7 presents the results when comparing the baseline sample T1 with the explanatory writing sample T4. Figure 8 presents the results when comparing the baseline sample T1 with the generative list task writing sample T3 and the explanatory writing sample T4 combined.

For the T1 T3 comparison, our analysis compared the free typed generative list task composition sample to the copy typed keyprint signature. The optimal point of comparison occurs between 75% and 80% and the false negative critical point occurs at approximately 60%. Figure 6 presents the false positive and false negative results of this analysis. The results of our analysis show that when comparing a free typed sample to the baseline keyprint signature, as in the previous case, the algorithm also functions well but not as well as it did with samples obtained under similar conditions.

These results support our hypothesis in this regard. In practice, if a free typed sample (provided under different conditions to the baseline) does not match the keyprint signature on at least 60% of the data points, our results indicate that it would be highly unlikely that the two

samples were provided by the same person. One of the challenges with this sample was the limited number of data points captured. Participants' typing samples tended to be smaller than that of other samples captured.

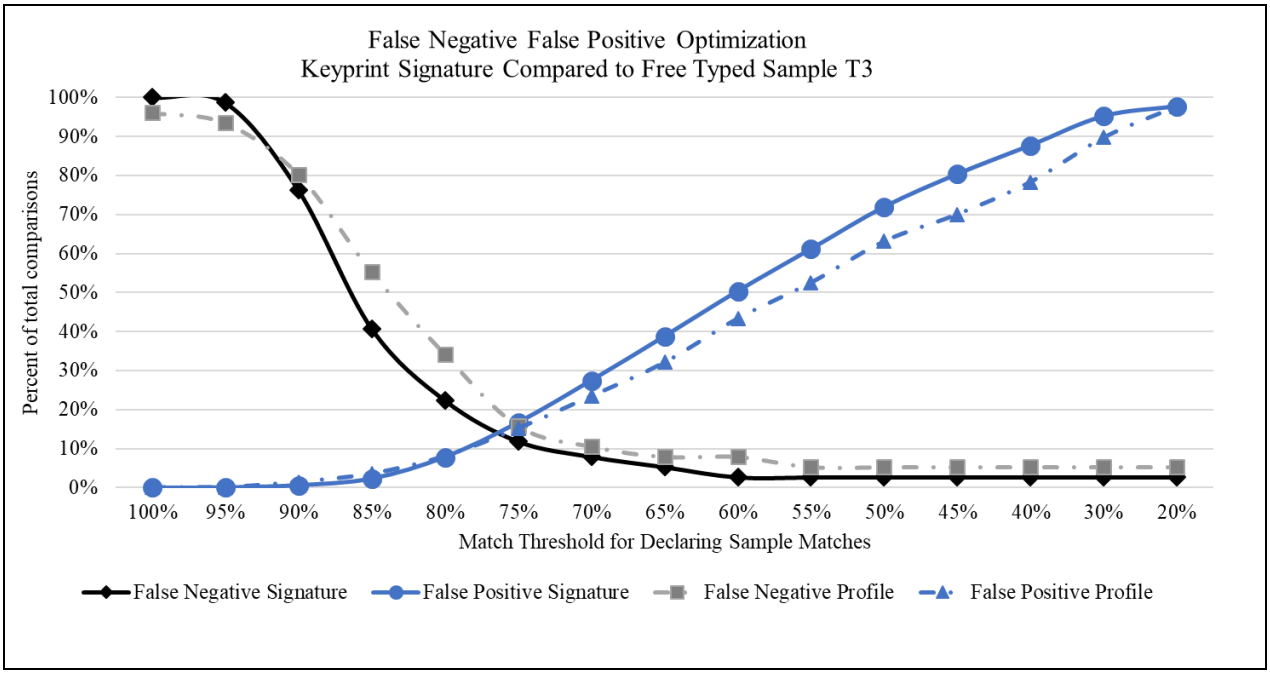

Figure 6. This figure shows the False Negative False Positive Optimization Keyprint Signature Compared to Free Typed Sample (T3). Optimization occurs at a match threshold between 75% and 80%. The critical point for reducing false negative identifications to zero using the keyprint signature is approximately 60%.

In the second free typing situation, T1 T4 comparison, we compared explanatory writing with the keyprint signature. For this situation we had plenty of data as compared to T3. In this case the optimal point occurred between a match threshold of 70% and 75%. The false negative critical point occurs somewhere between 50% and 55%. Figure 7 presents the false positive and false negative results obtained in this treatment condition. The results of our analysis show that when comparing a free typed sample to the baseline keyprint signature, the algorithm functions decently.

For a free typed explanatory writing sample, our results indicate that it would be highly unlikely that the two samples were provided by the same person if the sample did not match the copy typed keyprint on at least 50% of the data points. This result was slightly different from the previous free typed comparison and may indicate that typing patterns vary based on the type of cognitive task elicited by the assignment.

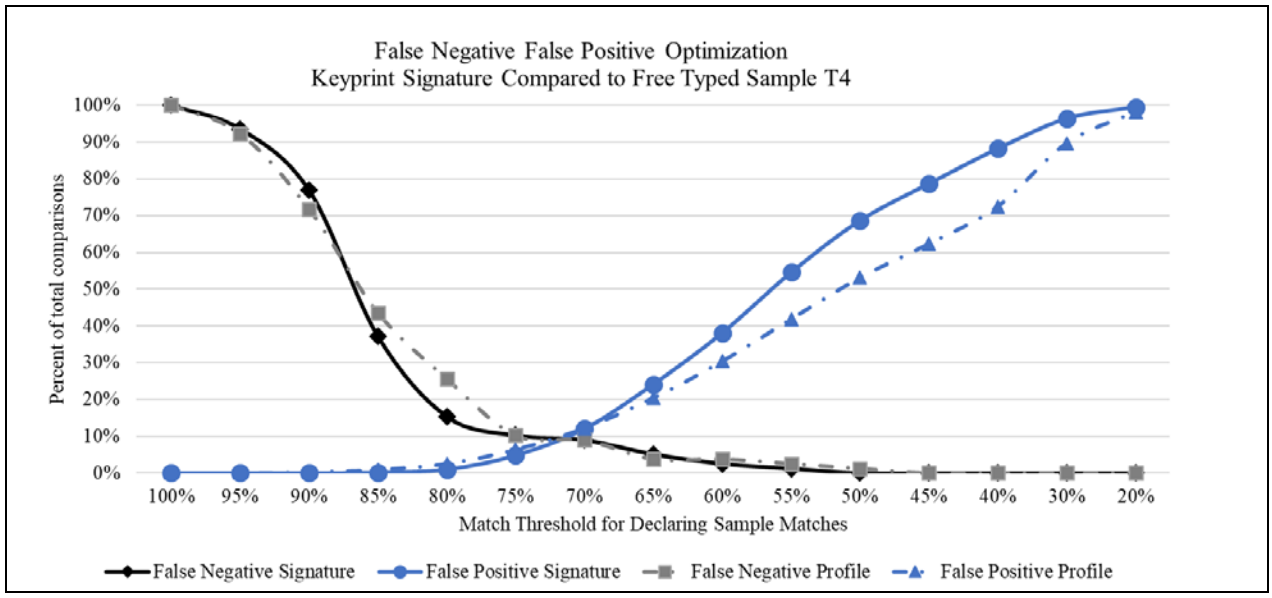

Figure 7. This figure shows the False Negative False Positive Optimization Keyprint Signature Compared to Free Typed Sample (T4). Optimization occurs at a match threshold at about 70%. The critical point using the keyprint signature is somewhere between 50% and 55%.

When comparing samples T3 and T4 combined to T1 (see Figure 8), the optimal point occurs between 70% and 75% match threshold with the false negative critical point occurring somewhere between 55% and 60%. If a free typed sample was compared to the baseline, based on these results, we would expect that the samples must match on at least 55% of the data points if we are to conclude that they were typed by the same person.

As such, our data supports the hypothesis that our matching algorithm would see a reduction in accuracy when comparing free typed samples to the copy typed keyprints; still, we were pleased to see that the algorithm performed sufficiently well to detect potential cheating to some degree.

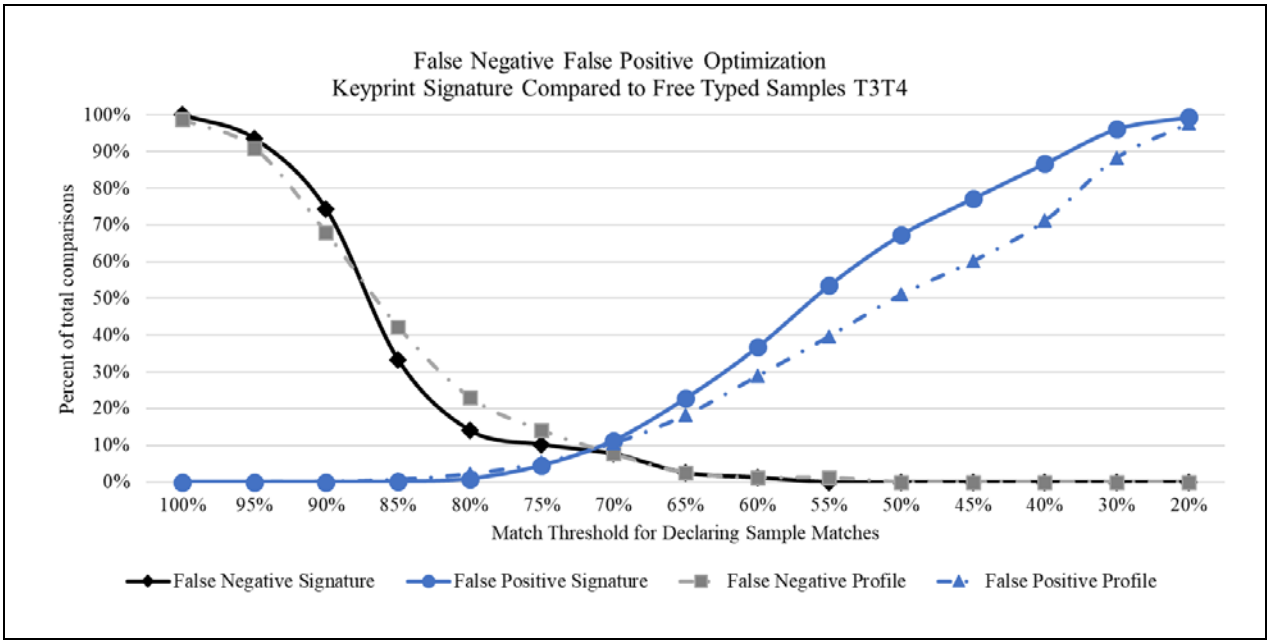

Figure 8. This figure shows the False Negative False Positive Optimization Keyprint Signature Compared to Free Typed Samples (T3 and T4) – Method 2. Optimization occurs at a match threshold at about 70%. The critical point using the keyprint signature is somewhere between 50% and 55%.

Keyprint accuracy comparing samples provided in an impediment context. Our final research question focused on the accuracy of keyprint comparisons in the context of samples involving impediments. We compared two impediment treatments involving copy typed samples. The first treatment (T5) involved copy typing with a band-aid on the right index finger (i.e., a mild impediment). In the second treatment (T6) we collected a sample of copy typing with tape wrapping together the middle and ring fingers on the left hand (i.e., a moderate impediment). We hypothesized that there would be a considerable reduction in matching accuracy when individuals copy typed under such conditions. Figure 9 presents the results when

comparing the baseline sample T1 with the mild band-aid impediment sample T5. Figure 10 presents the results when comparing the baseline sample T1 with the moderate tape-wrapped fingers impediment sample T6. Figure 11 presents the results when comparing the baseline sample T1 with the mild impediment sample T5 and the moderate impediment sample T6 combined.

For the T1 T5, we compared the keyprint signature to mild impediment copy typed samples. Our results show the optimal point for matching occurs between 75% and 80%; the false negative critical point occurs somewhere between 50% and 55%. However, for match thresholds between 55% and 65% the percent of false negative occurrences was only 1%.

The results of our analysis show that when comparing a mild impediment sample to the baseline keyprint signature, the algorithm functions adequately. In practice, if a mild impediment typed sample does not match the keyprint signature on at least 65% of the data points, our results say it would be extremely doubtful that the two typing samples were provided by the same individual. These results support our hypothesis. Typing under this condition is similar to that of free typing without anything impeding one's typing.

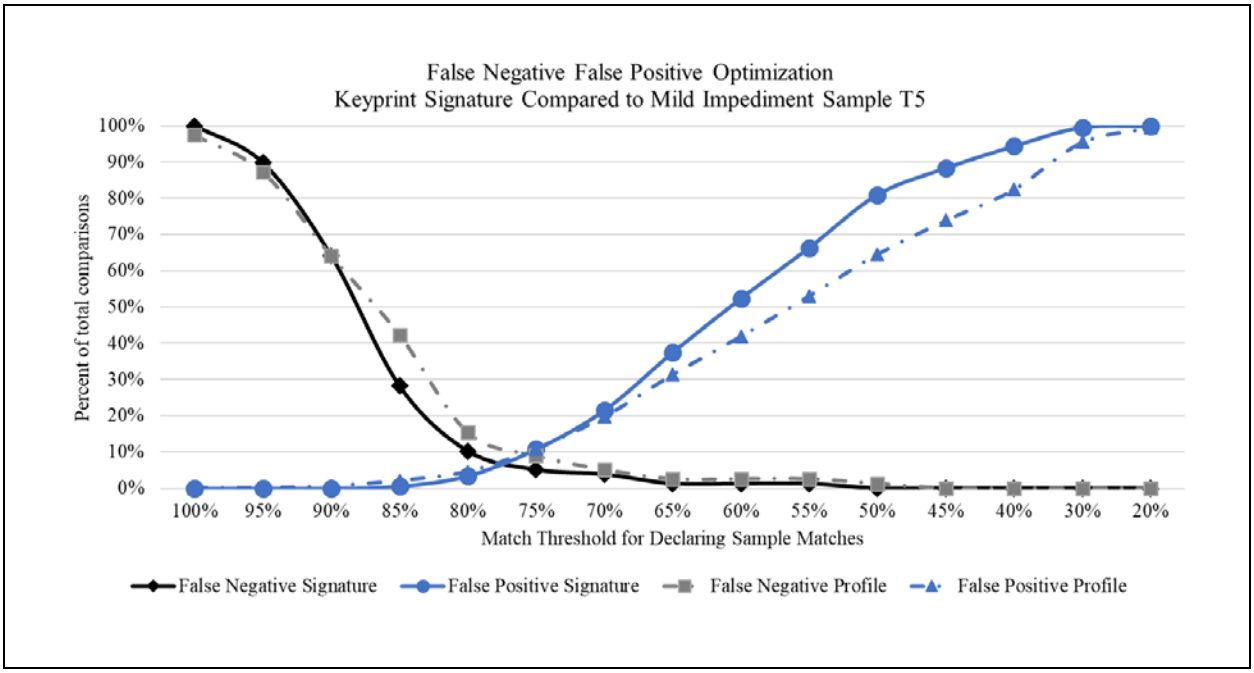

Figure 9. This figure shows the False Negative False Positive Optimization Keyprint Signature Compared to Mild Impediment Sample (T5) – Method 2. Optimization occurs at a match threshold between 75% and 80%. The critical point using the keyprint signature is somewhere between 50% and 55%.

In the second impediment typing situation (the T1 T6 comparison where participants had tape-wrapped fingers) the optimal comparison point occurs between 60% and 65%. The false negative critical point occurs somewhere between 40% and 45%. As expected, when the typing sample is obtained in the condition of a moderate impediment, the accuracy of the matching algorithm is diminished. In this condition, we could be sure that the individuals providing the samples were different people until less than 40% of the data points failed to match. Up until that point we could not be certain the samples were not a match.

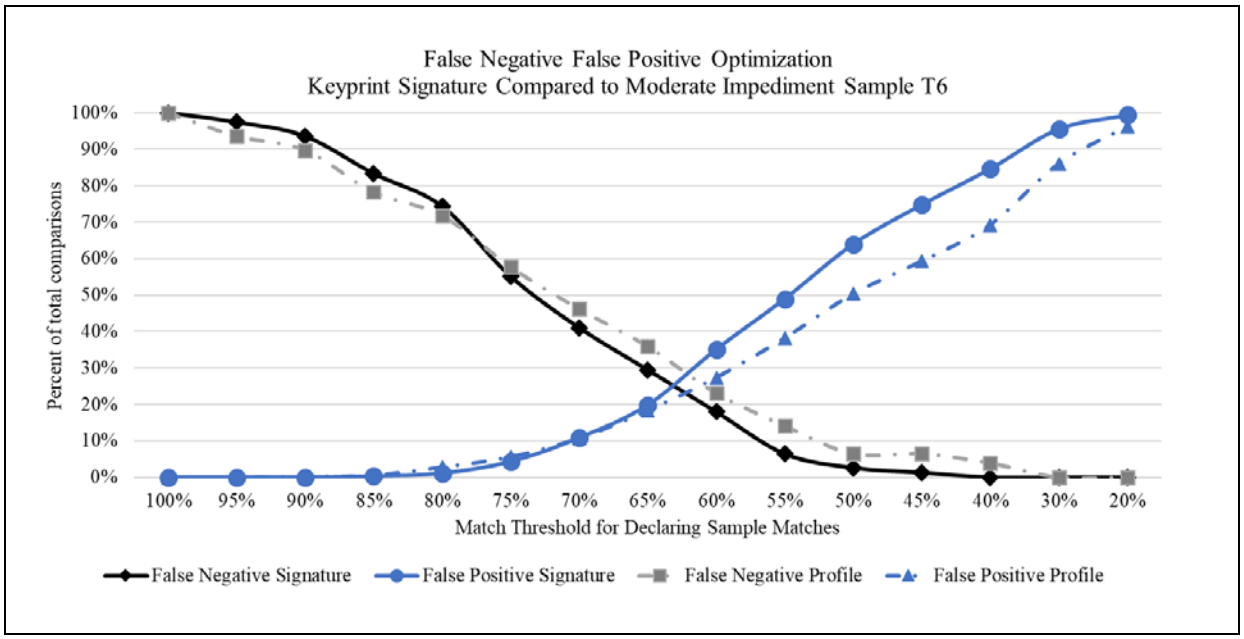

Figure 10. This figure shows the False Negative False Positive Optimization Keyprint Signature Compared to Moderate Impediment Sample (T6) – Method 2. Optimization occurs at a match threshold between 60% and 65%. The critical point using the keyprint signature is somewhere between 40% and 45%.

When comparing both T5 and T6 combined to T1 (see Figure 11) the optimal point occurs close to a 70% match threshold with the false negative critical point occurring somewhere between 45% and 50%. For match thresholds between 50% and 60% the percent of false negative occurrences was only 1%. Clearly a mild or moderate impediment copy typed sample presents challenges to the matching algorithm. But it is also clear that the algorithm performs somewhat well at detecting potential cheating even when the individual might be typing under adverse conditions.

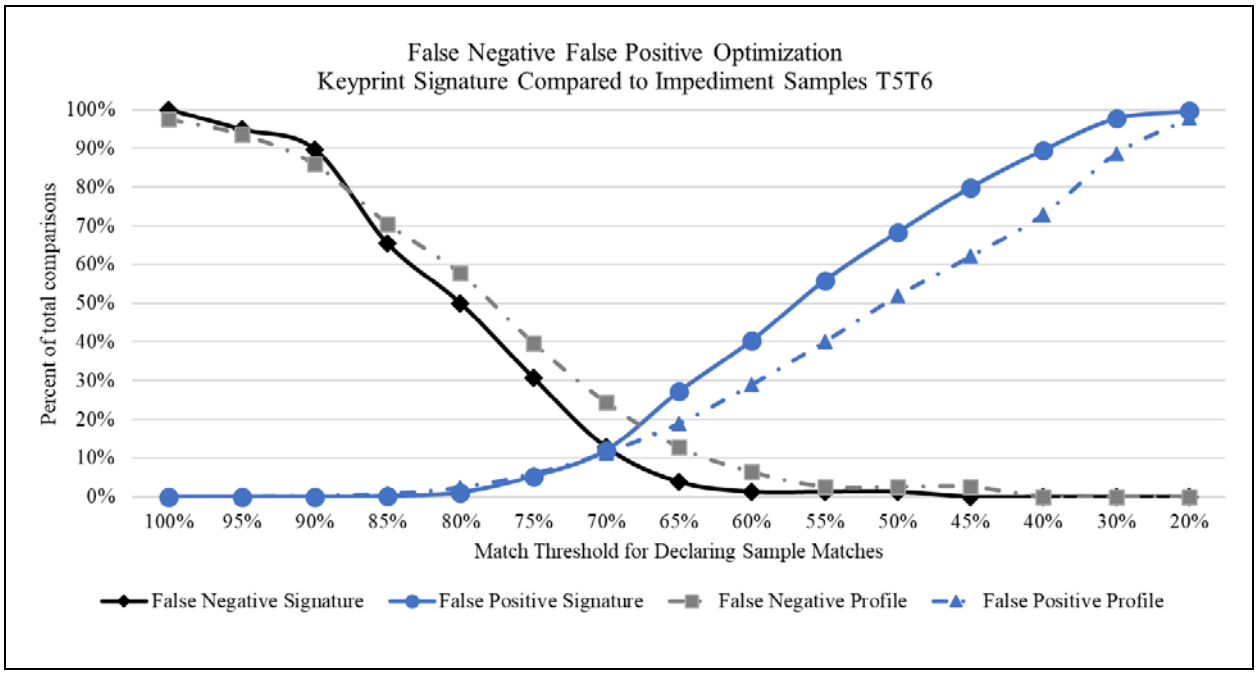

Figure 11. This figure shows the False Negative False Positive Optimization Keyprint Signature Compared to Impediment Samples (T5 and T6). Optimization occurs at a match threshold between 65% and 70%. The critical point using the keyprint signature is somewhere between 50% and 55%.

CHAPTER 5: DISCUSSION AND CONCLUSIONS

This study set out to answer four research questions, each about the ability of keystroke dynamics to accurately identify users in an online assessment context based on distinct treatment scenarios. Each treatment condition studied produced results that we hypothesized would affect the ability of the matching algorithm to correctly match samples. In practice, keystroke dynamics will never be as accurate as a finger print (which, barring disfigurement, is exactly the same all the time) because people do not type exactly the same way every time. The type of task they are completing or typing under the adverse conditions of an impediment will affect their typing patterns. What we hoped to determine with this study was the degree to which keystroke dynamics perform under-less-than ideal conditions. In this regard, the results of our study suggest that keystroke dynamics could be quite valuable.

An analysis of the results from this study positively demonstrated the feasibility of using keystroke dynamics to match typing samples. We found that keyprints are somewhat unique, but it may be best to use a full keyprint signature (75% critical point) rather than a reduced keyprint profile (65% critical point). We found that with a normal copy typed sample, keystroke dynamics can authenticate an individual with a high degree of accuracy (75% - 80% match threshold). With generative list task writing free typed samples, the accuracy rates decreased slightly but were fairly accurate (70% match threshold). With explanatory free typed samples, the accuracy rates decreased marginally (60% match threshold). With a mild impediment, the accuracy slightly decreased, but did not seem to affect the ability of the algorithm to match samples dramatically (75% - 80% match threshold). With a moderate impediment however, the precision rates were somewhat less accurate but still matched samples accurately to some degree (45% match threshold). The results of the study are summarized in Table 4.

Table 4

Results Summary Table

Comparison	Hypothesis	Result
T1 to T1	Keyprints are somewhat unique	Supported. Sample known not to match did not match at or above an 80% match threshold
T1 to T2-T6	Keyprint profiles will work better than keyprint signatures.	Not Supported. The keyprint signature critical point (75%) performed 10% better than the profile critical point (65%)
T1 to T2	Matching will be good for samples obtained under similar conditions	Supported. If samples did not match on at least 75% match threshold, samples were unlikely provided by the same person
T1 to T3/T4	Matching will be diminished for samples obtained under different free typed, cognitive conditions	Supported. If samples did not match on at least 60% match threshold, samples were unlikely provided by the same person
T1 to T5/T6	Matching will be considerably diminished for samples obtained when the typing is done with an impediment	Supported. If samples did not match on at least 45% match threshold, samples were unlikely provided by the same person

Interpretations of Findings, Reflections, and Insights

These findings relate to the practical understanding and application of keystroke dynamics in a number of different ways. Clearly, the optimization point balances the false negatives and the false positives, and the critical point for eliminating false positives are important to establish. These points are valuable to policy makers when determining how to best leverage the technology for their institution as they attempt to comply with government mandates to improve security in online courses. Knowing where the optimal points are will inform decisions on the amount of risk an institution is willing to carry and at what point accusations of cheating should be employed.

Understanding the degree to which the keyprint signature performs in various conditions is extremely important for policy makers. The keyprint signature we used in this study was made up of sixty-nine data points consisting of dwell and transition matches. In practice, and in a normal copy typed context similar to the conditions under which keyprints are obtained, if there was not a match of at least 75% of the data points the probability that the same person typed the two samples being compared is extremely low. However, in addition to the fact that people are not consistent typists and tend to improve with practice, copy typing is unlikely to be the condition under which samples will be obtained when this authentication practice is operationalized.

For practical reasons, copy typing a baseline is necessary in order to obtain all the requisite dwells and transitions needed. Using free typing to obtain a baseline would not guarantee that we would efficiently capture the necessary dwell and transition times needed to establish the keyprint signature as evidenced when we compared the two. It is more likely that comparison samples will be obtained under conditions of cognitive load which is different from that of the baseline keyprint conditions. In addition, students will inevitably experience times when they type with a mild or moderate impediment. This, we found, didn't affect our ability to match samples. Free typed samples did not match copy typed keyprint signatures as well as copy typed samples did. With mild impediments, our results showed that students' typing cadences are not affected too much, but our ability to identify an individual diminished slightly. This was not the case with moderate impediments however. With moderate impediments, accuracy was diminished, but the algorithm still functioned. This was important to understand, because not only can typing ability change over time, typing patterns can also change due to the task being undertaken and circumstances where an injury has been incurred. Using keystroke

dynamics to accurately identify individuals typing in various contexts and with a mild or moderate impediment is still somewhat accurate, but needs to be considered when deciding how best to utilize keystroke dynamics to authenticate individuals.

One possible operational practice that might alleviate some of this would be to periodically recalibrate the keyprint, either adding to the keyprint or completely recapturing the baseline. Doing so would also allow for the most up-to-date keystroke data to be used in the keyprint as well as allow flexibility for typing improvement or degradation.

Limitations

This study was limited in its scope due to multiple factors; some of which we plan to study at a different time. One limitation of this study is that it does not account for the fact that typing ability is not a fixed ability. An individual's typing ability will change over time with practice. In this regard, we anticipate that modifications to the keyprint signature would have to be made as time goes on. Along these lines, we forced individuals to provide samples using a specific keyboard and device. In an authentic online learning situation, this would not be the case.

Another limitation involves implementation implications. In order for keystroke dynamics to be used in authentic online assessment, any typing for the course would need to be done inside the designated assessment tracking system, not outside. Requiring typing to be done in the system environment so keystroke tracking can take place may be difficult to enforce. In reality, most learning management systems (LMS) are not designed as word processors, but keystroke dynamics in an LMS would be worth exploration by LMS designers for future LMS design. As online assignment completion is currently constituted, students will often type their essays and responses in a word processor and then copy their responses into the LMS.

Implementation of keystroke dynamics could be done via partnership with Google or Microsoft online to include their word processing technology in the course. This would allow students to do their work in the browser and allow the technology to track their keystrokes.

A final limitation of the study involves decisions that need to be made about missing data. This again is something we plan to explore at a later time. For this study, we made sure our samples contained a sufficient amount of data to compare. The degree to which it is realistic to assume that samples will contain sufficient data points and whether it is appropriate to combine samples obtained from individuals is unknown.

Implications

Practitioners can benefit from the results of this study in multiple ways. In knowing that a keystroke dynamics system is inexpensive to implement, practitioners can work with their local IT departments to develop and house a similar tool. If these institutions do not have the resources, they could partner with other institutions to work together to fund the project or apply for grant funds.

Once implemented, keystroke dynamics would provide a clearer picture of possible cheaters and where it was occurring in a course. This would allow for a more focused allocation of resources, giving institutions a better understanding of potentially how much effort, time, and money is being spent on academic honesty issues.

Implementation also makes the need for policy development paramount. It would be an opportunity for the institution to develop the necessary administrative checks and balances that need to be in place so that management of the keystroke dynamics system is clear and meaningful.

Students should not be assumed guilty of cheating simply because a sample of typing does not match their keyprint signature; this should only trigger additional identity verification checks. The checks for verifying cheating might involve a number of possible steps. The primary review tier would be a student needing to at least match their false negative critical point signature keyprint at 75%. Should the student not match their false negative keyprint signature at 75%, the next reasonable step might be to trigger the secondary sample comparison involving a reduced false negative critical point of 60%. If the false negative critical point occurs between 60% and 75%, then no further action would be necessary. However, if the false negative critical point were to occur below the 60% false negative critical point, then the next reasonable step might be to trigger an additional review involving a false negative critical point of 45%, checking for a potential impediment situation. Should the false negative critical point fall between 45% and 60%, a responsible approach might be to monitor the student's keyprint moving forward, but no further action may be necessary.

If the false negative critical point were to fall below the 45% threshold, the potential additional step might be to contact the student and let him or her know a potential problem has been identified. Doing this would give the student a chance to let course administrators know something has happened to alter their typing. It would make sense to conduct this interview via video for visual evidence of the student. Only upon verifying cheating has occurred should disciplinary action be taken.

If practitioners were to implement this approach, they would need to consider the institutions response to student cheating. Consequences to students might include giving the student a warning, zeros on assignments, requiring the student to take all their remaining assessments in a face-to-face proctored environment, or possibly removing the student from the

course. Each institution's policies and responses to cheating would be different, yet best practices should govern the overall administration of how student indiscretions are handled.

Keystroke dynamics provide a greater sense of online assessment security as well as closer alignment with federal law. This does not mean that institutions of higher learning should abandon vigilance and oversight once keystroke dynamics are employed. It does mean, however, that there can be a greater sense of confidence that the students completing their courses online are the same ones who are supposed to be doing it. This sense of confidence should bring a stronger commitment to integrity and therefore provide assurance to an accrediting body, of the institution's efforts to uphold the quality of the learning, academic fidelity, and the authenticity of the experience by the individuals receiving credit for the work being completed.

Conclusion

This study examined the potential use of keystroke dynamics to create keyprint signatures (typing fingerprints) to authenticate individuals in online course and assessment situations (Flior & Kowalski, 2010; Gaines et al., 1980; Giot et al., 2015; Killourhy & Maxion, 2009; Killourhy & Maxion, 2008; Monrose & Rubin, 2000; Rouse, 2008; Spillane, 1975; Yu & Cho, 2004). It was set up to determine how well keyprints were able to identify individuals when typing under various treatment conditions (Joyce & Gupta, 1990; Leggett & Williams, 1988; Vanette, 2015). Clearly, it would be very difficult, if not impossible, to establish the actual identity of a person based solely on an unknown sample of typing (Ahmed & Traore, 2007; Giot et al., 2015; Jenkins et al., 2013; Miguel et al., 2015; Sewell et al., 2010). There would be too many false positives to consider. However, the results of this study indicate that keyprints can be utilized effectively for user identification purposes, when determining that an individual may not be who he or she is supposed to be (Flior & Kowalski, 2010; Jenkins et al.; Leggett et al., 1991; Rybnik et al., 2008).

We would not be able to say who the individual is, but we would be able to say with a high degree of certainty that a typing sample was not provided by the individual who was supposed to have provided the sample.

As anticipated, typing with a temporary impediment diminished the algorithm's ability to identify students. This was also the case when user samples were typed under conditions different from those in which the keyprint baseline signature was captured. The ability to identify individuals is also challenging when the number of individual data points captured are limited (i.e., small comparison samples with many missing data points compared to those in the keyprint signature). However, the ability of the system to identify negative cases functions fairly well in each instance. Still, there are always ways to circumvent systems; and there will always be individuals who are unwilling to put in the effort needed to learn what is intended, those who want credit for accomplishing something they did not, and those willing to pay for something they never intend to obtain.

The major contributions of this dissertation come in the form of filling a part of the existing literature gap and beginning the discussion on keystroke dynamics usage in generative list task and explanatory free typing as well as in mild and moderate impediment typing. Overall, keystroke dynamics has not been used extensively in online education, and is still unproven in this arena. That will likely change as this important area of online assessment security is more thoroughly vetted and the value and significance of keystroke dynamics is realized (Giot et al., 2015; Jenkins et al., 2013; Miguel et al., 2015).

Future Research

To further this area of research, additional work needs to focus on other conditions likely to be encountered when capturing typing samples in an online course or assessment situation. Future studies need to consider the degree to which typing on different keyboards affects keyprint matching, the thresholds for matching given missing data (i.e., the minimum number of data points required to satisfactorily perform matches given small comparison samples), and possibly, ways to triangulate match decisions using additional biometric information and typing behaviors unique to individual users (e.g., typing speed, preferred language use, or common syntax and spelling errors made by individuals). Triangulation utilizing mouse dynamics in combination with keystroke dynamics to authenticate user behavior also needs further exploration.

Keystroke dynamics policy development and implementation could use additional study, including the articulation of keystroke dynamics policy best practices. This policy development will mature as authentication thresholds are tested, verified, and applied in real-life situations.

On the system side, to get to the most accurate identification points with our keystroke dynamics system, it is essential to verify the algorithm we developed and used. To do this, machine learning algorithms would be needed to improve the accuracy and precision when considering various data points. These algorithms could potentially train a support vector algorithm on every individual to get a sophisticated prediction and have an improved yes/no authentication accuracy rate. In addition, applications required to capture typing samples in various ways, both in-system and without, might be developed. These are all potential future research studies we intend to explore.

REFERENCES

Ahmed, A. A. E., & Traore, I. (2007). A new biometric technology based on mouse dynamics. *IEEE Transactions on Dependable and Secure Computing*, *4*(3), 165–179. Retrieved from doi.10.1109/TDSC.2007.70207

Alexander, M. W., Bartlett, J. E., Truell, A. D., & Ouwenga, K. (2001). Testing in a computer technology course: An investigation of equivalency in performance between online and paper and pencil methods. *Journal of Career and Technical Education. 18*(1), 69-80. Retrieved from https://ejournals.lib.vt.edu/index.php/JCTE/article/view/378/263

Ali, L., Tappert, C. C., & Qiu, M. (2015, August). Authentication and identification methods used in keystroke biometric systems. In *High Performance Computing and Communications (HPCC), 2015 IEEE 7th International Symposium on Cyberspace Safety and Security (CSS), 2015 IEEE 12th International Conference on Embedded Software and Systems (ICESS),* (pp. 1424-1429). IEEE. Retrieved from doi.10.1109/HPCC-CSS-ICESS.2015.66

Caldarola, R., & MacNeil, T. (2009). Dishonesty deterrence and detection: How technology can ensure distance learning test security and validity. In D. Remenyi (Ed.), *Proceedings of the 8th European Conference on E-Learning* (pp. 108-115). Reading, UK: Academic Publishing Limited. Retrieved from https://books.google.com/books?hl=en&lr=&id=qGw4tvVrKUEC&oi=fnd&pg=PA108&dq=Dishonesty+deterrence+and+detection:+How+technology+can+ensure+distance+learning+test+security+and+validity&ots=rb13EbwUAl&sig=E0HZhpyyCQTSqT1vKhgReLK7QoM#v=onepage&q=Dishonesty%20deterrence%20and%20detection%3A%20How%20techn

ology%20can%20ensure%20distance%20learning%20test%20security%20and%20validity&f=false

Chandrasekar, V., Kumar, S. S., & Maheswari, T. (2016). Authentication based on keystroke dynamics using stochastic diffusion algorithm. *Stochastic Analysis and Applications*, *34*(1), 155–164. Retrieved from doi.10.1080/07362994.2015.1112291

Chang, T. Y., Tsai, C. J., Yang, Y. J., & Cheng, P. C. (2011). User authentication using rhythm click characteristics for non-keyboard devices. In *Proceedings of the 2011 International Conference on Asia Agriculture and Animal IPCBEE* (Vol. 13, pp. 167-171).

EdSurge. (2015, September 8). *Udacity, Coursera and edX now claim over 24 million students*. Retrieved from https://www.edsurge.com/news/2015-09-08-udacity-coursera-and-edx-now-claim-over-24-million-students

Fawcett, T. (2006). An introduction to ROC analysis. *Pattern recognition letters*, 27(8), 861-874. Retrieved from doi.10.1016/j.patrec.2005.10.010

Flior, E., & Kowalski, K. (2010). Continuous biometric user authentication in online examinations. *ITNG2010 - 7th International Conference on Information Technology: New Generations*, 488–492. Retrieved from doi.10.1109/ITNG.2010.250

Freidman, J. (2016, February 9). Study: Enrollment in Online Learning Up, Except at For-Profits. Retrieved from https://www.usnews.com/education/online-education/articles/2016-02-09/study-enrollment-in-online-learning-up-except-at-for-profits

Gaines, R. S., Lisowski, W., Press, S. J., & Shapiro, N. (1980). *Authentication by keystroke timing: Some preliminary results* (No. RAND-R-2526-NSF). Santa Monica, CA: Rand Corporation: Retrieved from http://www.dtic.mil/docs/citations/ADA484022

Gaytan, J., & McEwen, B. C. (2007). Effective online instructional and assessment strategies. *American Journal of Distance Education*, *21*(3), 117–132. doi.10.1080/08923640701341653

Gikandi, J. W., Morrow, D., & Davis, N. E. (2011). Online formative assessment in higher education: A review of the literature. *Computers & Education*, *57*(4), 2333-2351.

Giot, R., Dorizzi, B., & Rosenberger, C. (2015). A review on the public benchmark databases for static keystroke dynamics. *Computers and Security*, *55*, 46–61. Retrieved from doi.10.1016/j.cose.2015.06.008

Giot, R., El-Abed, M., & Rosenberger, C. (2011). Keystroke dynamics authentication. *Biometrics* (chapter 8). Retrieved from https://hal.archives-ouvertes.fr/hal-00990373/document

Giot, R., Hemery, B., & Rosenberger, C. (2010). Low cost and usable multimodal biometric system based on keystroke dynamics and 2D face recognition. *Proceedings - International Conference on Pattern Recognition*, 1128–1131. doi.10.1109/ICPR.2010.282

Graf, F. (2002). Providing security for eLearning. *Computers & Graphics*, *26*(2), 355-365.

Grijalva, T. C., Nowell, C., & Kerkvliet, J. (2006). Academic honesty and online courses. *College Student Journal*, *40*(1), 180-185. Retrieved from https://s3.amazonaws.com/academia.edu.documents/3457387/cheat_online_pap.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1518211925&Signature=uSYWcMvvON2Of49PIC1pwKvOsNU%3D&response-content-disposition=inline%3B%20filename%3DAcademic_Honesty_and_Online_Courses.pdf

Gunetti, D., & Picardi, C. (2005). Keystroke analysis of free text. *ACM Transactions on Information and System Security*, *8*(3), 312–347. Retrieved from doi.10.1145/1085126.1085129

Guven, A., & Sogukpinar, I. (2003). Understanding users' keystroke patterns for computer access security. *Computers and Security*, *22*(8), 695–706. Retrieved from doi.10.1016/S0167-4048(03)00010-5

Hard, S. F., Conway, J. M., & Moran, A. C. (2006). Faculty and college student beliefs about the frequency of student academic misconduct. *The Journal of Higher Education*, *77*(6), 1058-1080.

Hricko, M., & Howell, S. L. (2006). *Online assessment and measurement*. Hershey, PA: IGI Global.

Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2014). Improving password cybersecurity through inexpensive and minimally invasive means: Detecting and deterring password reuse through keystroke-dynamics monitoring and just-in-time fear appeals. *Information Technology for Development*, *20*(2), 1–18. Retrieved from http://www.tandfonline.com/doi/10.1080/02681102.2013.814040

Joyce, R., & Gupta, G. (1990). Identity authentication based on keystroke latencies. *Communications of the ACM*, *33*(2), 168–176. Retrieved from doi.10.1145/75577.75582

Karnan, M., Akila, M., & Krishnaraj, N. (2011). Biometric personal authentication using keystroke dynamics: A review. *Applied Soft Computing Journal*, *11*(2), 1565–1573. Retrieved from doi.10.1016/j.asoc.2010.08.003

Keller, H. (1954). *The story of my life* (Vol. 1). Garden City, New York: Doubleday & Company, Inc.

Keystroke dynamics. (2015). In B*iometric-Solutions.com*. Retrieved from http://www.biometric-solutions.com//solutions/index.php?story=keystroke_dynamics

Keytrac. (2016). *How KeyTrac records your typing behavior*. Retrieved from https://www.keytrac.net/en/technology

Khoury, R., & Drummond, C. (Eds.). (2016). Advances in Artificial Intelligence: *Proceedings of the 29th Canadian Conference on Artificial Intelligence.* Victoria, BC: Springer.

Killourhy, K. S., & Maxion, R. A. (2009, June). Comparing anomaly-detection algorithms for keystroke dynamics. In *Dependable Systems & Networks, 2009. DSN'09. IEEE/IFIP international conference on* (pp. 125-134).

Killourhy, K., & Maxion, R. (2008, September). The effect of clock resolution on keystroke dynamics. In *International Workshop on Recent Advances in Intrusion Detection* (pp. 331-350). Berlin, Heidelberg: Springer.

King, C. G., Guyette Jr, R. W., & Piotrowski, C. (2009). Online exams and cheating: An empirical analysis of business students' views. *Journal of Educators Online*, *6*(1), 1-11.

Lau, E., Liu, X., Xiao, C., & Yu, X. (2004). Enhanced user authentication through keystroke biometrics. *Massachusetts Institute of Technology*, *9,* 1-12. Retrieved from http://people.csail.mit.edu/edmond/projects/keystroke/keystroke-biometrics.pdf

Leggett, J., & Williams, G. (1988). Verifying identity via keystroke characteristics. *International Journal of Man-Machine Studies*, *28*(1), 67-76.

Leggett, J., Williams, G., Usnick, M., & Longnecker, M. (1991). Dynamic identity verification via keystroke characteristics. *International Journal of Man-Machine Studies*, 35(6), 859-870.

Li, C. S., & Irby, B. (2008). An overview of online education: Attractiveness, benefits, challenges, concerns and recommendations. *College Student Journal*, *42*(2), 449-458. Retrieved from http://eds.b.ebscohost.com/eds/detail/detail?vid=0&sid=2bd31246-8bbd-4cb7-98d9-d55ad27456aa%40sessionmgr120&bdata=JnNpdGU9ZWRzLWxpdmUmc2NvcGU9c2l0ZQ%3d%3d#AN=32544879&db=aph

Li, S. Z., & Jain, A. K. (Eds.). (2009). Keystroke Dynamics. *Encyclopedia of Biometrics*. East Lansing, MI: Springer.

Marsters, J. D. (2009). *Keystroke dynamics as a biometric* (Doctoral dissertation). Retrieved from https://eprints.soton.ac.uk/66795/

McMurtry, K. (2001). E-Cheating: Combating a 21st Century Challenge. *THE Journal*, *29*(4), 36-41. Retrieved from https://www.questia.com/library/journal/1G1-80634264/e-cheating-combating-a-21st-century-challenge

Meng, M., & Agarwal, R. (2007). Through a glass darkly: Information technology design, identity verification, and knowledge contribution in online communities. *Information Systems Research*, *18*(1), 42–67. Retrieved from doi.10.1287/isre.1070.0113

Moini, A., & Madni, A. M. (2009). Leveraging biometrics for user authentication in online learning: A systems perspective. *Systems Journal, IEEE*, *3*(4), 469-476.

Monaco, J. V., Stewart, J. C., Cha, S. H., & Tappert, C. C. (2013, September). Behavioral biometric verification of student identity in online course assessment and authentication of authors in literary works. In *Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on* (pp. 1-8). Retrieved from doi.10.1109/BTAS.2013.6712743

Monrose, F., & Rubin, A. (1997, April). Authentication via keystroke dynamics. In *Proceedings of the 4th ACM Conference on Computer and Communications Security* (pp. 48-56). Retrieved from doi.10.1145/266420.266434

Monrose, F., & Rubin, A. D. (2000). Keystroke dynamics as a biometric for authentication. *Elsevier Future Generation Computer Systems*, *16*, 351–359. Retrieved from doi.10.1016/S0167-739X(99)00059-X

Newton, D. (2015). Cheating in online classes is now big business. Atlantic Website. Retrieved from https://www.theatlantic.com/education/archive/2015/11/cheating-through-online-courses/413770/

Panchumarthy, R., Subramanian, R., & Sarkar, S. (2012, November). Biometric evaluation on the cloud: A case study with humanid gait challenge. In *Proceedings of the 2012 IEEE/ACM Fifth International Conference on Utility and Cloud Computing* (pp. 219-222). IEEE Computer Society. Retrieved from https://dl.acm.org/citation.cfm?id=2415728

University Testing Services (n.d.). *UGA Student Affairs: Online Course Exams.* Retrieved from the University of Georgia website https://testing.uga.edu/students-customers/online-course-exams

O'Shaughnessy, L. (2009, September 11). The latest ways that kids cheat on exams. Retrieved from http://www.cbsnews.com/news/the-latest-ways-that-kids-cheat-on-exams/

Pérez-Peña, R. (2012, August 31). Harvard students in cheating scandal say collaboration was accepted. Retrieved from http://www.nytimes.com/2012/09/01/education/students-of-harvard-cheating-scandal-say-group-work-was-accepted.html

Pfost, J. (2007). The science behind keystroke dynamics. *Biometric Technology Today*, *15*(2), 7. Retrieved from doi.10.1016/S0969-4765(07)70057-7

Robles, M., & Braathen, S. (2002). Online assessment techniques. *Delta Pi Epsilon Journal*, *44*(1), 39–49. Retrieved from http://www.acousticslab.org/dots_sample/module2/RoblesAndBraathen2002.pdf

Rouse, M. (2008). Keystroke dynamics. Retrieved from http://searchsecurity.techtarget.com/definition/keystroke-dynamics

Rybnik, M., Tabedzki, M., & Saeed, K. (2008). A keystroke dynamics based system for user identification. *2008 7th Computer Information Systems and Industrial Management Applications*, 225–230. Retrieved from doi.10.1109/CISIM.2008.8

Saevanee, H. (2014). Continuous user authentication using multi-modal biometrics. *Computers & Security*, *53*, 1–13. Retrieved from doi.10.1016/j.cose.2015.06.001

Sewell, J. P., Frith, K. H., & Colvin, M. M. (2010). Online assessment strategies: A primer. *Journal of Online Learning and Teaching*, *6*(1), 297–305.

Simkin, M. G., & McLeod, A. (2010). Why do college students cheat? *Journal of Business Ethics*, *94*(3), 441–453. Retrieved from doi.10.1007/s10551-009-0275-x

Spillane, R. (1975). Keyboard apparatus for personal identification. *IBM Technical Disclosure Bulletin*, 17(3346), 3346.

Tamilarasi, M., Rajasekhar Reddy, P., & Palanivelu, T. G. (2008). Adaptive route timeout for on-demand routing protocols in MANETs. *Proceedings - International Conference on Computational Intelligence and Multimedia Applications, ICCIMA 2007*, *4*, 293–297. Retrieved from doi.10.1109/ICCIMA.2007.51

Talavera-Franco, R. (2014, April 23). Facial biometrics: A solution or a problem for MOOCs assessments? MOOCstream. Retrieved from

http://moocstream.blogspot.com/2014/04/facial-biometrics-solution-or-problem.html#.VxKyPDArI2w

U.S. Higher Education System. 2016. In the *National Science Foundation*. Retrieved October 12, 2017, from https://www.nsf.gov/statistics/2016/nsb20161/#/report/chapter-2/the-u-s-higher-education-system

Vrankuli, A. (2013, January 16). Coursera looks to verify online student identity with photo, keystroke dynamics. BiometricUpdate.com. Retrieved from http://www.biometricupdate.com/201301/coursera-looks-to-verify-online-student-identity-with-photo-keystroke-dynamics

Yu, E., & Cho, S. (2004). Keystroke dynamics identity verification—its problems and practical solutions. *Computers and Security*, *23*(5), 428–440. Retrieved from doi.10.1016/j.cose.2004.02.004

APPENDIX A

EMAIL INSTRUCTIONS TO ACCESS KEYSTROKE COLLECTION SYSTEM

Everyone,

Thanks for participating in our keystroke data collection. Just wanted to remind you of what we are asking as well as some important details. We are collecting keystroke data for Jay Young's Dissertation study and are hoping that you will participate. For this to be successful, you should be aware:

- Participating in this study will take about 15-30 minutes of your time
- Please Use **Chrome**, that will provide the best results, go to the website, http://keystroke.webdrawnsilk.com/
- Log in and use the tools you were given in class today to complete the extra credit assignment
- Please complete it in one sitting
- At the end of the keystroke activity, your name will be added to the list of those who participated and you will receive the extra credit.

Thanks for contributing to the study.

APPENDIX B

TREATMENT TEXT PARTICIPANTS WERE ASKED TO TYPE

T1 - Baseline check #1	Text
Introductory paragraph to the autobiography of Helen Keller.	"It is with a kind of fear that I begin to write the history of my life. I have, as it were, as superstitious hesitation in lifting the veil that clings about my childhood like a golden mist. The task of writing an autobiography is a difficult one. When I try to classify my earliest impressions, I find that fact and fancy look alike across the years that link the past with the present. The woman paints the child's experiences in her own fantasy. A few impressions stand out vividly from the first years of my life; but "the shadows of the prison-house are on the rest." Besides, many of the joys and sorrows of childhood have lost their poignancy; and many incidents of vital importance in my early education have been forgotten in the excitement of great discoveries. In order, therefore, not to be tedious I shall try to present in a series of sketches only the episodes that seem to me to be the most interesting and important. (Keller, 1904, p. 3)"

Figure C1. T1 - Baseline Check #1. Each participant typed the introductory paragraph to Helen Keller's autobiography, the Story of my Life.

T2 - Baseline check #2	Text
Conclusion paragraph to the autobiography of Helen Keller.	"Often when I dream, thoughts pass through my mind like cowled shadows, silent and remote, and disappear. Perhaps they are the ghosts of thoughts that once inhabited the mind of an ancestor. At other times, the things I have learned and the things I have been taught, drop away, as the lizard sheds its skin, and I see my soul as God sees it. There are also rare and beautiful moments when I see and hear in Dreamland. What if in my waking hours a sound should ring through the silent halls of hearing? What if a ray of light should flash through the darkened chambers of my soul? What would happen, I ask many and many a time. Would the bow-and-string tension of life snap? Would the heart, overweighted with sudden joy, stop beating for very excess of happiness? (Keller, 1904, p. 431)"

Figure C2. T2- Baseline check #2. Each participant typed the conclusion paragraph to Helen Keller's autobiography, the Story of my Life.

T5 – Impediment Check #1:	Text
Introduction paragraph of the Gettysburg Address.	“Four score and seven years ago our fathers brought forth, upon this continent, a new nation, conceived in liberty, and dedicated to the proposition that “all men are created equal.” Now we are engaged in a great civil war, testing whether that nation, or any nation so conceived, and so dedicated, can long endure. We are met on a great battle field of that war. We come to dedicate a portion of it, as a final resting place for those who died here, that the nation might live. This we may, in all propriety do” (Lincoln, 1863).

Figure C4. T3 Hand Impediment Check #1. Each participant typed the introduction paragraph to the Gettysburg Address, by Abraham Lincoln

T6 – Impediment Check #2	Text
Conclusion paragraph of the Gettysburg Address.	"But, in a larger sense, we cannot dedicate – we cannot consecrate – we cannot hallow, this ground – The brave men, living and dead, who struggled here, have hallowed it, far above our poor power to add or detract. The world will little note, nor long remember what we say here; while it can never forget what they did here. It is rather for us, the living, we here be dedicated to the great task remaining before us – that, from these honored dead we take increased devotion to that cause for which they here, gave the last full measure of devotion – that we here highly resolve these dead shall not have died in vain; that the nation, shall have a new birth of freedom, and that government of the people, by the people, for the people, shall not perish from the earth" (Lincoln, 1863).

Figure C5. T4 Hand Impediment Check #2. Each participant typed the conclusion paragraph to the Gettysburg Address, by Abraham Lincoln.

APPENDIX C

R CODE USED TO ANALYZE DATA

The dataset used is available upon request by contacting Jay Young at jillow@gmail.com

R code used for analyzing the data:

```
---
title: "Keystroke Dynamics Analysis"
author: "RSD"
date: "10/20/2017"
output: html_document
---

```{r get data, echo=FALSE}
# Get data from its location on the computer and name it, need to set working dir to where the file is located
DatasetV1 <- read.csv("DatasetV1 92217final.csv")
tolower(DatasetV1)
TooFew <- 9 # how few is too few in the sample to make comparison
zcut <- 0.5 # cut point to include data points in profile
library(dplyr)
library(reshape)
```
```{r index chlable, echo=FALSE}
# Index the names of the keys/combos to get a list of their names, then convert them to numbers.  Create a table that lets you compare the number to the name if needed called "namnum"
DatasetV1 <- DatasetV1[order(DatasetV1$chLabel),] # sort
names <- unique(DatasetV1$chLabel) # get unique labels
x <- as.factor(DatasetV1$chLabel) # get index for lables
DatasetV1$chLabel <- as.numeric(x) # replace labels with index number
numbers <- unique(DatasetV1$chLabel) # get unique indexes
namnum <- data.frame(names, numbers) # create a numbered list of characters and transition combos
```
```{r Create Signature Profiles, echo=FALSE}
DataTempX <- DatasetV1[DatasetV1$Treatment==1,] #get treatment sample 1
# reshape baseline treatment data T1,
DataT1means <- cast(DataTempX, ID~chLabel, mean, value = 'Time')
# Get the Zscore, note uses mean of means not all user data for SD
ZscoreT1 <- data.frame(apply(DataT1means, 2, scale)) # used mean and SD of means to reduce influence of outliers
# create signature profiles based on unusually large z scores
ProfileT1 <- data.frame(abs(ZscoreT1)>zcut) # keyprint profile
ProfileT1[is.na(ProfileT1)] <- FALSE # flag empty profiles cells
profileCount <- data.frame(rowSums(ProfileT1)) # count number of keys in each profile
```

```{r false negatives for treatment 1 vs other samples, echo=TRUE}
# function to calculate t values at each data point when comparing keyprint signature vs comparison sample
MeanDifference.t <- function(m2,sd2,n2) {
 meanDiff <- (Keyprint.mean[,-1] - m2[,-1]) # calculate mean differences
 # se, scaled by the sample sizes used to calculate t
 se <- sqrt( ((1/Keyprint.n[,-1]) + (1/n2[,-1])) * ( ( ((Keyprint.n[,-1]-1) * (Keyprint.sd[,-1]^2)) + ((n2[,-1]-1)*(sd2[,-1]^2)) ) / (Keyprint.n[,-1]+n2[,-1]-2) ) )
 t <- meanDiff / se # calculate t values
return(t) # return t values
}
DataTempX <- DatasetV1[DatasetV1$Treatment==1,] #get treatment sample 1
# get the descriptives for each key/combo for each person, one line per person/ID
Keyprint.mean <- cast(DataTempX, ID~chLabel, mean, value = 'Time') # average time of Keyprint signature
Keyprint.sd <- cast(DataTempX, ID~chLabel, sd, value = 'Time') # Standard deviation of Keyprint signature
Keyprint.n <- cast(DataTempX, ID~chLabel, length , value = 'Time') # count of Keyprint signature


# get Treatment sample to compare
DataTempX <- DatasetV1[DatasetV1$Treatment!=1,] # select all but T1
#DataTempX <- DatasetV1[DatasetV1$Treatment>4,] # select only T5 T6
```
```

```
#DataTempX <- DatasetV1[(DatasetV1$Treatment==3)|(DatasetV1$Treatment==4) ,] # select only two treatments
#DataTempX <- DatasetV1[DatasetV1$Treatment==3,] # select Treatment sample to compare

# get the descriptives for sample to be compared
Tcompare.mean <- cast(DataTempX, ID~chLabel, mean, value = 'Time') # get sample means to compare
Tcompare.sd <- cast(DataTempX, ID~chLabel, sd, value = 'Time') # get sample SDs to compare
Tcompare.n <- cast(DataTempX, ID~chLabel, length , value = 'Time') # get Ns of comparison sample

t.scores <- abs(MeanDifference.t(Tcompare.mean,Tcompare.sd,Tcompare.n)) # get t values from comparison
NAcount.t <- data.frame(rowSums(is.na(t.scores))) # Count number of NA
df.table <- data.frame((Keyprint.n[,-1]+Tcompare.n[,-1])-2) # calculate Degree of Freedom

# calculate p values for each t value excluding NA
p.values <- t.scores # create data frame for p.values matching t.scores
for (j in 1:nrow(t.scores)) {
 for (k in 1:ncol(t.scores)) {
 if(!is.na(t.scores[j,k])) {
 p.values[j,k] <- 2*pt(-abs(t.scores[j,k]),df=df.table[j,k]) # calc p values 2 tailed for each data point
}}}

# determine how often sample matched Keyprint
matchTemp <- data.frame(matrix(ncol = ncol(t.scores), nrow = nrow(t.scores))) # setup results table
excludeTooFew <- data.frame(ncol(matchTemp)-NAcount.t <= TooFew ) # exclude if toofew
matchTemp[is.na(p.values)] <- FALSE # replace NA with FALSE
matchTemp[p.values <= 0.05] <- FALSE # flag non matches at each data point
matchTemp[p.values > 0.05] <- TRUE # flag matches at each data point
matchResult.t <- data.frame(rowSums(matchTemp)/ncol(matchTemp)) # get % matches treat NA as non-match
matchResult.t2 <- data.frame(rowSums(matchTemp)/(ncol(matchTemp)-NAcount.t)) # get % matches exclude NA
matchResult.t[excludeTooFew==TRUE] <- FALSE # exclude too few
matchResult.t2[ excludeTooFew==TRUE] <- FALSE # exclude too few
# matches based on ProfileT1
NApro <- data.frame(rowSums((is.na(t.scores)&(ProfileT1==TRUE)))) # Number NA in profile
excludeTooFewPro <- data.frame(profileCount-NApro <= TooFew ) #exclude if toofew
matchTemp[(ProfileT1==FALSE)] <- FALSE # flag data points not in the profile
matchResult.tpro <- data.frame(rowSums(matchTemp)/(profileCount)) # get % matches based on profile treat NA as non-match
matchResult.tpro2 <- data.frame(rowSums(matchTemp)/(profileCount-NApro)) # get % matches exclude NA from total
matchResult.tpro[excludeTooFewPro==TRUE] <- FALSE # exclude too few
matchResult.tpro2[ excludeTooFewPro==TRUE] <- FALSE # exclude too few

# determine false negatives at each match thresholds for ROC chart
MT.values <- c(1,0.95,0.9,0.85,0.8,0.75,0.7,0.65,0.6,0.55,0.5,0.45,0.4,0.3,0.2) # set Match thresholds to compare
FNFPT1T <- data.frame(matrix(ncol = length(MT.values), nrow = 4)) # setup results Table ncol = num thresholds indicated
FNFPT1Tm2 <- data.frame(matrix(ncol = length(MT.values), nrow = 4)) # setup results Table for method 2
colnames(FNFPT1T) <- MT.values # add column lables
rownames(FNFPT1T) <- c("FNsignature","FPsignature","FNprofile","FPprofile") # add row labels
colnames(FNFPT1Tm2) <- MT.values # add column lables
rownames(FNFPT1Tm2) <- c("FNsignature","FPsignature","FNprofile","FPprofile") # add row labels

# Compare each Users against know match in comparison samples, Calc % false negative matched
matched <- matchResult.t # setup temp results variable
matched2 <- matchResult.t2 # setup temp results variable for method 2
for (mt in as.numeric(MT.values)) {
 matched[matchResult.t >= mt] <- FALSE # flag True Matches for sample vs keyprint signature
 matched[matchResult.t < mt] <- TRUE # flag False Negatives for sample vs keyprint signature
 FNFPT1T[1,as.character(mt)] <- sum(matched)/(nrow(matched)-colSums(excludeTooFew)) # place value in Results table at mt
 matched2[matchResult.t2 >= mt] <- FALSE # flag True Matches for sample vs keyprint signature
 matched2[matchResult.t2 < mt] <- TRUE # flag False Negatives for sample vs keyprint signature
 FNFPT1Tm2[1,as.character(mt)] <- sum(matched2)/(nrow(matched2)-colSums(excludeTooFew)) # place value in Results table at mt

 # check matches in profile at each Match Threshold
 EmptyProfiles <- length(profileCount[profileCount==0]) # count number of empty profiles
 matched[(matchResult.tpro >= mt)] <- FALSE # flag True Matches
 matched[(matchResult.tpro < mt)] <- TRUE # flag False Negatives
 FNFPT1T[3,as.character(mt)] <- sum(matched)/(nrow(matched)-colSums(excludeTooFew)-EmptyProfiles) # place value
 matched2[(matchResult.tpro2 >= mt)] <- FALSE # flag True Matches method 2
 matched2[(matchResult.tpro2 < mt)] <- TRUE # flag False Negatives method 2
 FNFPT1Tm2[3,as.character(mt)] <- sum(matched2)/(nrow(matched2)-colSums(excludeTooFew)-EmptyProfiles) # place value
}
```

```{r false positives for treatment 1 vs another sample, echo=TRUE}
```

```
 # function to calculate t values at each data point when comparing keyprint signature vs comparison sample
SampleCompare.t <- function(KeyRow,CompRow, npro=TRUE, m2=FALSE) {
 mDiff <- (Keyprint.mean[as.numeric(KeyRow),-1] - Tcompare.mean[as.numeric(CompRow),-1]) # mean differences
 se <- sqrt( ((1/Keyprint.n[as.numeric(KeyRow),-1]) + (1/Tcompare.n[as.numeric(CompRow),-1])) * ( ( ((Keyprint.n[as.numeric(KeyRow),-1]-1)
* (Keyprint.sd[as.numeric(KeyRow),-1]^2)) + ((Tcompare.n[as.numeric(CompRow),-1]-1)*(Tcompare.sd[as.numeric(CompRow),-1]^2)) ) /
(Keyprint.n[as.numeric(KeyRow),-1]+Tcompare.n[as.numeric(CompRow),-1]-2) ) ) #Calc standard Error
 t <- mDiff / se # calculate t values
 # calculate % match for these two rows
 NAcount <- data.frame(rowSums(is.na(t))) # Count number of NA
 NApro <- data.frame(rowSums((is.na(t.scores)&(ProfileT1==TRUE)))) # Number NA in profile
 # calculate Degrees of Freedom
 df.tab <- data.frame((Keyprint.n[as.numeric(KeyRow),-1]+Tcompare.n[as.numeric(CompRow),-1])-2)
 p.vals <- t # create data frame for p.values matching t.scores
 # calculate p values for each t value excluding NA
 for (k in 1:ncol(t)) {
 if(!is.na(t[1,k])) {
 p.vals[1,k] <- 2*pt(-abs(t[1,k]),df=df.tab[1,k]) # calc p values 2 tailed at each data point
 }
 }
 matchT <- data.frame(matrix(ncol = ncol(t), nrow = 1)) # setup results table
 matchT[is.na(p.vals)] <- FALSE # replace NA with FALSE
 if (npro) {
 # determine how often data points in sample matched Keyprint signature
 matchT[p.vals <= 0.05] <- FALSE # flag non matches at each data point
 matchT[p.vals > 0.05] <- TRUE # flag matches at each data point
 if ((rowSums(matchT)-NAcount)<=TooFew) {
 PercentMatch <- 0 # no matches
 PercentMatch2 <- 0 # no matches
 } else {
 PercentMatch <- rowSums(matchT)/ncol(matchT) # Calculate % matches
 PercentMatch2 <- rowSums(matchT)/(ncol(matchT)-NAcount) # Calculate % matches Exclude NA
 }
 } else {
 # determine how often data points in sample matched Keyprint profile
 matchT[(p.vals <= 0.05)|(ProfileT1[as.numeric(KeyRow),]==FALSE)] <- FALSE # non matches at each data point
 matchT[(p.vals > 0.05)&(ProfileT1[as.numeric(KeyRow),]==TRUE)] <- TRUE # matches at each data point
 # Calculate % matches
 if ((profileCount[as.numeric(KeyRow),]-NApro[as.numeric(KeyRow),])<=TooFew) {
 PercentMatch <- 0
 PercentMatch2 <- 0
 } else {
 PercentMatch <- rowSums(matchT)/(profileCount[as.numeric(KeyRow),]) # % matches of data points in profile
 PercentMatch2 <- rowSums(matchT)/(profileCount[as.numeric(KeyRow),]-NApro[as.numeric(KeyRow),]) #excludes NA
 }
 }
 # return % match for these two samples, known to not match, using matching method specified
 if (m2) {return(PercentMatch2)} else {return(PercentMatch)}
} #end function

# determine number of false positives in the sample
k <- 1 # initialize index
TotalFPcompared <- 0 # initialize total comparisons counter
FNFPT1T[2,] <- 0 # initialize false positive counts
FNFPT1T[4,] <- 0 # initialize false positive counts
FNFPT1Tm2[2,] <- 0 # initialize false positive counts for method 2
FNFPT1Tm2[4,] <- 0 # initialize false positive counts for method 2

# nested for loop to compare all samples against all other samples known not to be matches, counts false positives
 for (row in 2:nrow(Keyprint.mean)) {
 # add FP counts in second row of Results table at each match threshold
 FP <- SampleCompare.t(1,row, TRUE, FALSE) # determine if false positive for two full samples using method 1
 FPpro <- SampleCompare.t(1,row, FALSE, FALSE) # determine if false positive for two samples using Profile + method 1
 FP2 <- SampleCompare.t(1,row, TRUE, TRUE) # determine if false positive for two full samples using method 2
 FPpro2 <- SampleCompare.t(1,row, FALSE, TRUE) # determine if false positive for two samples using Profile + method 2
 TotalFPcompared <- TotalFPcompared+1 # comparisons counter
 # increment false positive counter for each method and keyprint type at each match threshold
 for (mt in as.numeric(MT.values)) {
 if (FP >= mt) { FNFPT1T[2,as.character(mt)] <- FNFPT1T[2,as.character(mt)] +1 }
 if (FPpro >= mt) { FNFPT1T[4,as.character(mt)] <- FNFPT1T[4,as.character(mt)] +1 }
 if (FP2 >= mt) { FNFPT1Tm2[2,as.character(mt)] <- FNFPT1Tm2[2,as.character(mt)] +1 }
```

```
if (FPpro2 >= mt) { FNFPT1Tm2[4,as.character(mt)] <- FNFPT1Tm2[4,as.character(mt)] +1 }
}
for (r in (row+1):nrow(Keyprint.mean)) {
j<-k+1
if (r <= nrow(Keyprint.mean)) {
FP <- SampleCompare.t(j,r, TRUE, FALSE) # determine if false positive for two full samples using method 1
FPpro <- SampleCompare.t(j,r, FALSE, FALSE) # determine if false positive for two samples using Profile + method 1
FP2 <- SampleCompare.t(j,r, TRUE, TRUE) # determine if false positive for two full samples using method 2
FPpro2 <- SampleCompare.t(j,r, FALSE, TRUE) # determine if false positive for two samples using Profile + method 2
TotalFPcompared <- TotalFPcompared+1 # comparisons counter
# increment false positive counter for each method and keyprint type at each match threshold
for (mt in as.numeric(MT.values)) {
if (FP >= mt) { FNFPT1T[2,as.character(mt)] <- FNFPT1T[2,as.character(mt)] +1 }
if (FPpro >= mt) { FNFPT1T[4,as.character(mt)] <- FNFPT1T[4,as.character(mt)] +1 }
if (FP2 >= mt) { FNFPT1Tm2[2,as.character(mt)] <- FNFPT1Tm2[2,as.character(mt)] +1 }
if (FPpro2 >= mt) { FNFPT1Tm2[4,as.character(mt)] <- FNFPT1Tm2[4,as.character(mt)] +1 }
} } }
k <- k+1
} # end forloop that counts false positives

# place false positive counts in results tables for both match methods
FNFPT1T[2,] <- FNFPT1T[2,]/ TotalFPcompared # calc % false positives at each Match Threshold
FNFPT1T[4,] <- FNFPT1T[4,]/ TotalFPcompared # calc % false positives using profile at each Match Threshold
FNFPT1Tm2[2,] <- FNFPT1Tm2[2,]/ TotalFPcompared # calc % false positives at each Match Threshold method 2
FNFPT1Tm2[4,] <- FNFPT1Tm2[4,]/ TotalFPcompared # calc % false positives using profile using method 2

```
```
```

APPENDIX D

TRANSITION AND DWELL CHARACTER USAGE TABLES

Table D1

Transition Characters Used to Develop the Keyprint Signatures and Profiles Organized Alphabetically

	Transition Characters	Average Time	Character Count		Transition Characters	Average Time	Character Count
1.	. space	340.9	2369	23.	n t	150.4	2262
2.	a n	125.8	4354	24.	o n	81.3	3180
3.	a s	157.3	1717	25.	o r	97.7	2739
4.	a t	123.5	4298	26.	o u	102.6	2640
5.	backspace backspace	189.4	11751	27.	r e	162.9	4486
6.	d space	171.8	5591	28.	s e	189.1	1949
7.	e a	141.8	2557	29.	s space	159.6	5598
8.	e d	193.5	2628	30.	s t	126.0	2028
9.	e n	145.3	3514	31.	space a	186.6	6885
10.	e r	138.5	3957	32.	space f	290.9	2382
11.	e s	178.5	2651	33.	space h	175.0	2858
12.	e space	125.4	11546	34.	space i	238.7	4324
13.	f space	97.2	2390	35.	space o	203.0	3938
14.	h a	111.6	4079	36.	space s	315.7	3568
15.	h e	126.3	6610	37.	space t	189.3	9505
16.	h i	80.1	1456	38.	space w	201.4	3275
17.	i n	99.5	6216	39.	t e	160.1	2708
18.	i s	114.0	1849	40.	t h	87.8	8639
19.	i t	196.2	2400	41.	t i	117.8	2415
20.	l i	88.0	2525	42.	t o	106.7	2281
21.	n d	129.1	2980	43.	t space	151.8	6349
22.	n space	142.1	4913				

Table D2

Dwell Characters Used to Develop the Keyprint Signatures and Profiles

Number	Dwell Character	Average Time	Character Count	Number	Dwell Character	Average Time	Character Count
1.	,	97.7	4792	14.	l	133.3	12440
2.	.	108.4	2897	15.	m	121.2	5921
3.	a	151.7	23223	16.	n	108.8	21035
4.	b	88.0	2509	17.	o	115.3	21777
5.	backspace	95.1	22894	18.	p	139.5	5663
6.	c	116.0	7274	19.	r	127.6	16030
7.	d	108.8	11435	20.	s	144.2	16791
8.	e	121.7	37226	21.	t	116.3	27940
9.	f	112.3	6531	22.	u	123.5	5940
10.	g	103.6	6499	23.	v	105.5	3375
11.	h	95.8	16922	24.	w	138.1	6154
12.	i	128.9	21713	25.	y	100.6	4963
13.	k	81.1	2388	26.	space	114.1	65087

Table D3

Dwell Characters Excluded from the Keyprint Signature and Profiles

Number	Dwell Character	Times Used	Number	Dwell Character	Times Used
1.	-	757	31.	5	28
2.	"	590	32.	\	25
3.	'	566	33.	CapsLock	15
4.	Enter	503	34.	[	14
5.	x	466	35.	Meta	12
6.	1	410	36.	AudioVolumeDown	10
7.	;	357	37.	7	9
8.	j	350	38.	NumLock	8
9.	3	324	39.	End	8
10.	)	296	40.	AudioVolumeUp	8
11.	0	276	41.	+	7
12.	ArrowRight	268	42.	!	7
13.	9	266	43.	_	7
14.	(	251	44.	<	6
15.	4	227	45.	]	6
16.	q	203	46.	Home	4
17.	?	197	47.	*	4
18.	ArrowLeft	178	48.	&	3
19.	/	177	49.	#	3
20.	z	162	50.	@	2
21.	8	160	51.	%	2
22.	6	158	52.	Tab	2
23.	Control	126	53.	ContextMenu	1
24.	Delete	76	54.	Insert	1
25.	ArrowDown	71	55.	{	1
26.	=	70	56.	PageDown	1
27.	ArrowUp	68	57.	PageUp	1
28.	>	39			
29.	2	33			
30.	:	30			

Table D4

Transition Characters Excluded from Developing Keyprint Signatures or Profiles. All Other Key Combinations Were Used Fewer Times and Were Excluded from the Table

Number	Transition Characters	Times Used	Number	Transition characters	Times Used	Number	Transition characters	Times Used
1	, Space	4603	35	Space n	1316	69	k e	890
2	Space Shift	3958	36	h Space	1311	70	i f	879
3	y Space	3478	37	o t	1279	71	Backspace e	862
4	r Space	2912	38	w h	1273	72	u s	845
5	a r	2641	39	n o	1231	73	r t	845
6	o Space	2622	40	s o	1212	74	u t	835
7	Space Backspace	2581	41	o w	1203	75	n a	832
8	Space m	2522	42	e l	1197	76	e t	829
9	n g	2327	43	p e	1195	77	Backspace Space	820
10	Space c	2310	44	f o	1188	78	p r	820
11	v e	2297	45	d i	1175	79	e e	811
12	o f	2255	46	r i	1170	80	o p	796
13	Space p	2083	47	n e	1168	81	p o	792
14	Space d	2065	48	I Space	1163	82	u r	790
15	Space l	2064	49	i g	1157	83	r a	785
16	Space b	2034	50	c o	1146	84	Backspace t	771
17	l l	1993	51	g e	1136	85	s s	751
18	a Space	1930	52	g h	1132	86	h t	746
19	l e	1888	53	l d	1120	87	c h	743
20	d e	1719	54	Space r	1082	88	Backspace Shift	733
21	i o	1717	55	t a	1075	89	m y	732
22	a l	1680	56	m a	1022	90	a p	716
23	Shift i	1616	57	s i	989	91	e m	714
24	g Space	1613	58	e ,	974	92	t s	712
25	b e	1583	59	i l	966	93	l o	710
26	n c	1566	60	s h	962	94	u g	702
27	l Space	1530	61	u l	952	95	l a	674
28	w e	1515	62	a v	943	96	i v	671
29	h o	1491	63	o m	943	97	a c	660
30	c e	1450	64	e Backspace	935	98	Backspace ,	659
31	Space e	1424	65	r s	925	99	Shift t	656
32	m e	1395	66	Space g	917	100	p l	655
33	r o	1381	67	i e	910	101	Backspace a	652
34	c a	1376	68	i c	899	102	e .	646

APPENDIX E

ROC CHARTS WITH DATA ATTACHED

Table E1

False Positive Occurrences for Baseline Keyprint Signatures and Profiles in Sample T1

	Match Thresholds														
	100%	95%	90%	85%	80%	75%	70%	65%	60%	55%	50%	45%	40%	30%	20%
% False Positives Keyprint Signature	0.00	0.00	0.00	0.00	0.01	0.06	0.14	0.26	0.40	0.56	0.69	0.79	0.88	0.96	1.00
% False Positives Keyprint Profile	0.00	0.00	0.00	0.01	0.03	0.07	0.12	0.22	0.33	0.43	0.54	0.63	0.73	0.88	0.97

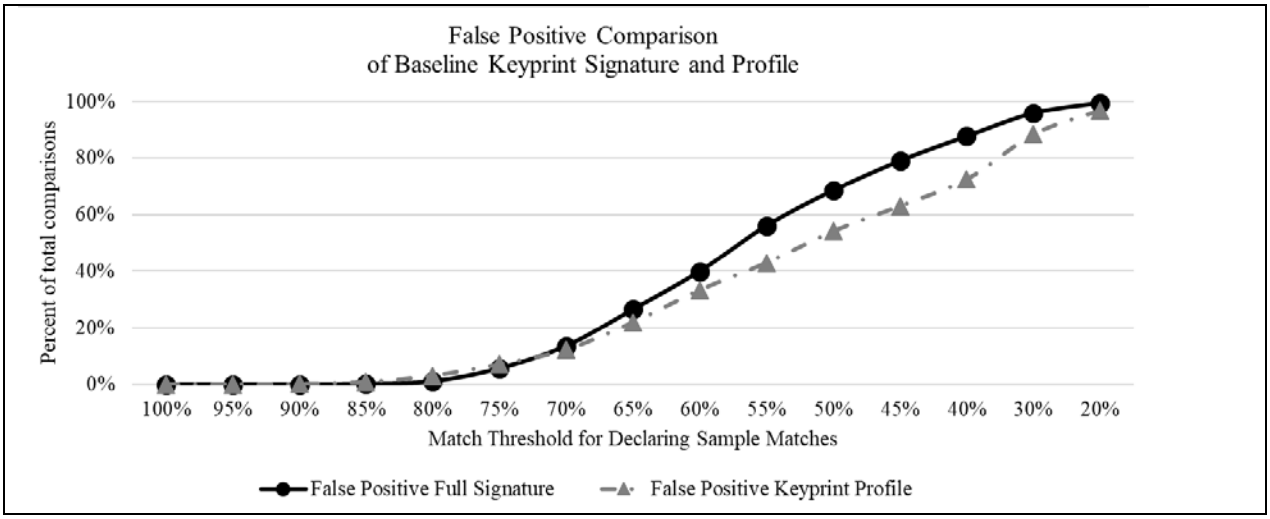

Figure E1. False positive occurrences for baseline keyprint signatures and profiles in sample T1 at each match threshold. Based on this analysis, the critical point for false positive occurrences is between 80% and 85%. This result indicates that at or above an 80% match threshold, each keyprint for the individuals in the data is completely unique.

Table E2

False Negative Comparing Match Range versus Wilcoxon Versus t test Method Keyprint Signature Compared to All Other Samples

	Match Thresholds														
	100%	95%	90%	85%	80%	75%	70%	65%	60%	55%	50%	45%	40%	30%	20%
t.test False Negative Signature	0.99	0.63	0.29	0.10	0.04	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Wilcoxon False Negative Signature	1.00	0.86	0.47	0.19	0.12	0.04	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
Match Range False Negative Signature	1.00	0.96	0.81	0.40	0.18	0.05	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

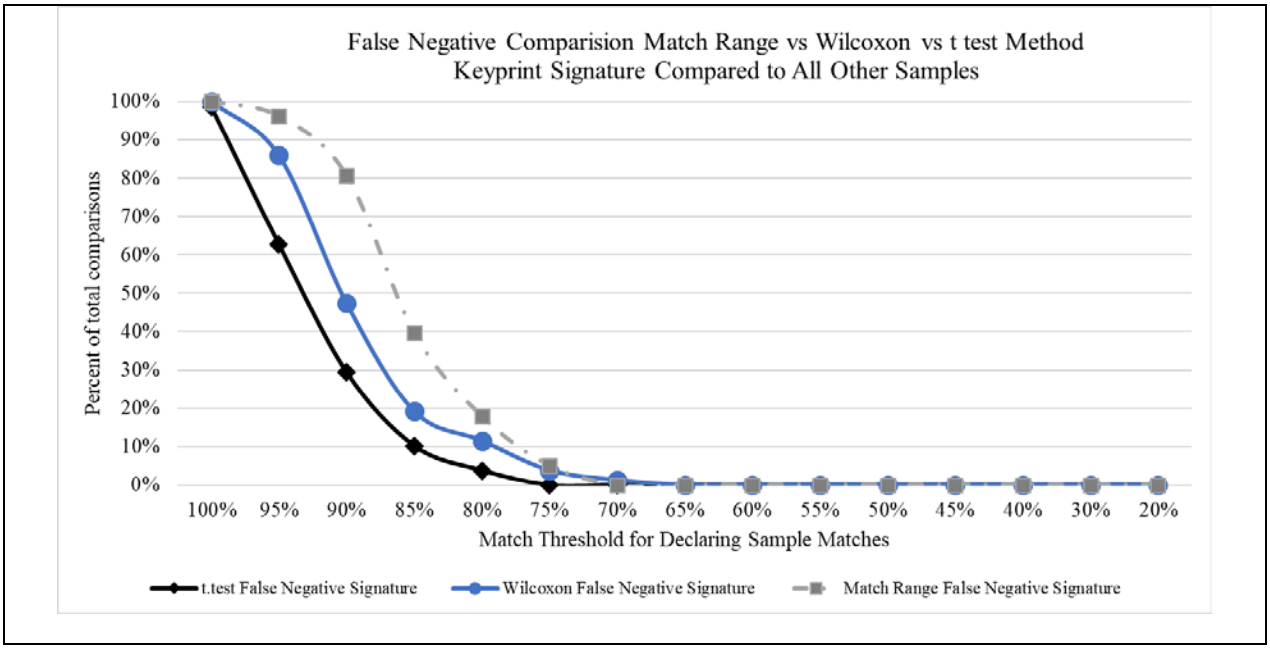

Figure E2. Comparison of match range versus Wilcoxon-Mann-Whitney versus *t* test method keyprint signature compared to all other samples. Among the three methods, the results were somewhat similar but the *t* test method performed better overall.

The ***t*** test performed better between 75% and 100% and hit the critical point for false positive at 75%. Using the non-parametric Wilcoxon method and the match range methods resulted in suboptimal performance compared to the ***t*** test method.

Table E3

False Negative False Positive Optimization for Keyprint Signature and Profile (T1) Compared to All Other Samples (T2-T6)

	Match Thresholds														
	100%	95%	90%	85%	80%	75%	70%	65%	60%	55%	50%	45%	40%	30%	20%
% False Negative Keyprint Signature	1.00	0.91	0.53	0.24	0.10	0.05	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
% False Positives Keyprint Signature	0.00	0.00	0.00	0.00	0.01	0.04	0.10	0.23	0.35	0.53	0.66	0.77	0.87	0.96	0.99
% False Negative Keyprint Profile	0.96	0.86	0.56	0.33	0.15	0.09	0.04	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00
% False Positives Keyprint Profile	0.00	0.00	0.00	0.00	0.02	0.05	0.09	0.16	0.26	0.36	0.48	0.57	0.68	0.87	0.96

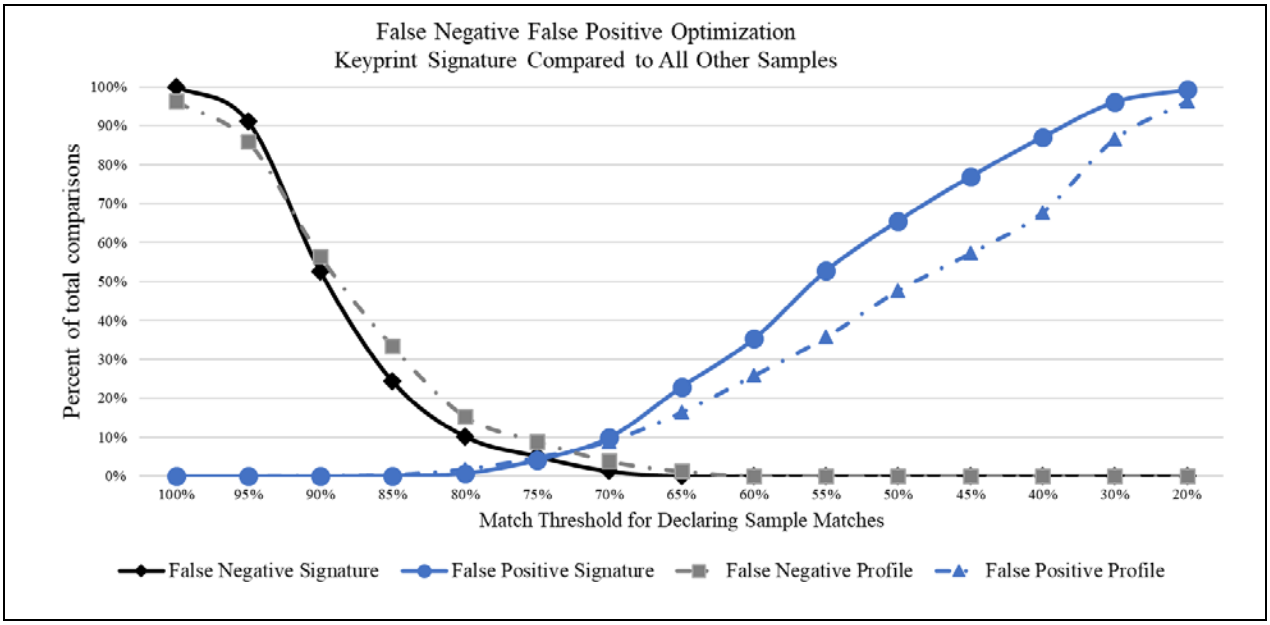

Figure E3. False negative and false positive optimization for keyprint signature and profiles compared to all other typing samples combined (T2-T6). Optimization occurs at a match threshold of approximately 75%. This is the point where false positives and false negatives are optimally balanced. However, the critical point for reducing false negative identifications to zero using the keyprint signature is approximately 70%. The critical point for reducing false negative identifications to zero using the keyprint profile is closer to 65%. In this regard, using the keyprint signature is better than the keyprint profile.

Table E4

False Negative False Positive Optimization for Keyprint Signature and Profile (T1) Compared to Copy Typed Sample (T2)

	Match Thresholds														
	100%	95%	90%	85%	80%	75%	70%	65%	60%	55%	50%	45%	40%	30%	20%
% False Positives Keyprint Signature	1.00	0.82	0.47	0.14	0.06	0.01	0.01	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.00
% False Positives Keyprint Profile	0.00	0.00	0.00	0.00	0.01	0.06	0.13	0.27	0.42	0.58	0.72	0.81	0.89	0.97	1.00
% False Negative Keyprint Signature	0.95	0.74	0.44	0.23	0.08	0.04	0.03	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
% False Positives Keyprint Profile	0.00	0.00	0.00	0.01	0.03	0.07	0.14	0.22	0.34	0.44	0.57	0.65	0.75	0.91	0.98

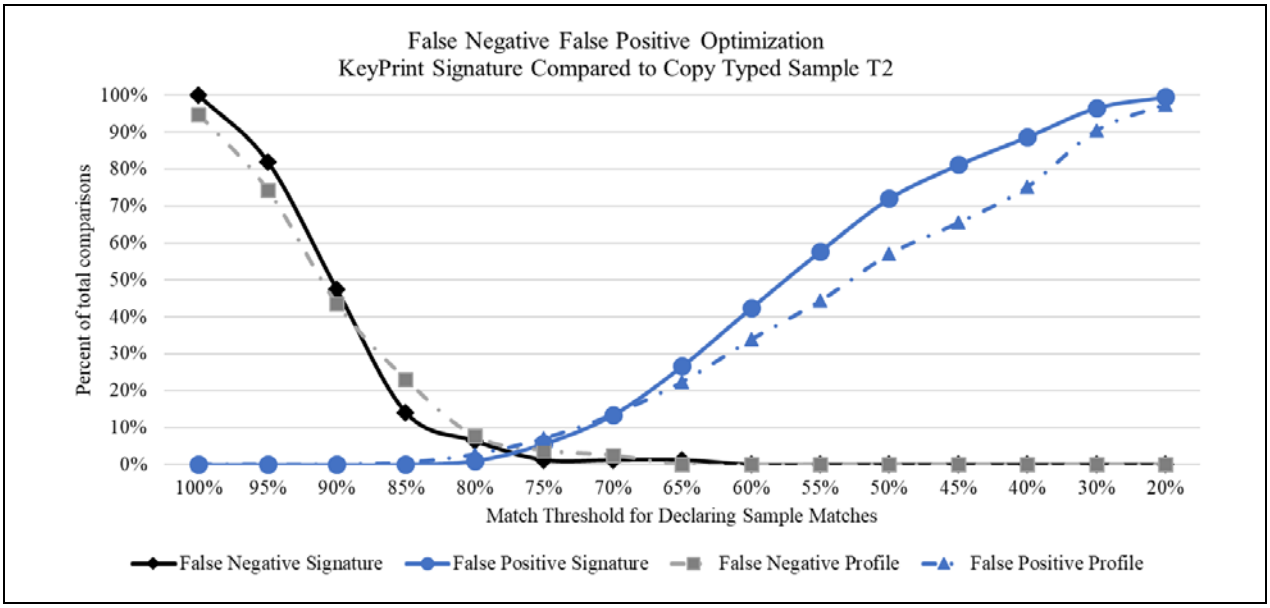

Figure E4. False Negative False Positive Optimization Keyprint Signature Compared to Copy Typed Sample T2. Optimization occurs at a match threshold between 75% and 80%. The critical point for reducing false negative identifications to zero using the keyprint signature is approximately 75%. The critical point for reducing false negative identifications to zero using the keyprint profile is closer to 65%. In this regard, using the keyprint signature is slightly better than the keyprint profile.

Table E5

False Negative False Positive Optimization for Keyprint Signature and Profile (T1) Compared to Free Typed Sample (T3) – Method 2

	Match Thresholds														
	100%	95%	90%	85%	80%	75%	70%	65%	60%	55%	50%	45%	40%	30%	20%
% False Positives Keyprint Signature	1.00	0.99	0.76	0.41	0.22	0.12	0.08	0.05	0.03	0.03	0.03	0.03	0.03	0.03	0.03
% False Positives Keyprint Profile	0.00	0.00	0.01	0.02	0.08	0.17	0.27	0.39	0.50	0.61	0.72	0.80	0.88	0.95	0.98
% False Negative Keyprint Signature	0.96	0.93	0.80	0.55	0.34	0.16	0.11	0.08	0.08	0.05	0.05	0.05	0.05	0.05	0.05
% False Positives Keyprint Profile	0.00	0.00	0.01	0.04	0.08	0.15	0.23	0.32	0.43	0.53	0.63	0.70	0.78	0.90	0.98

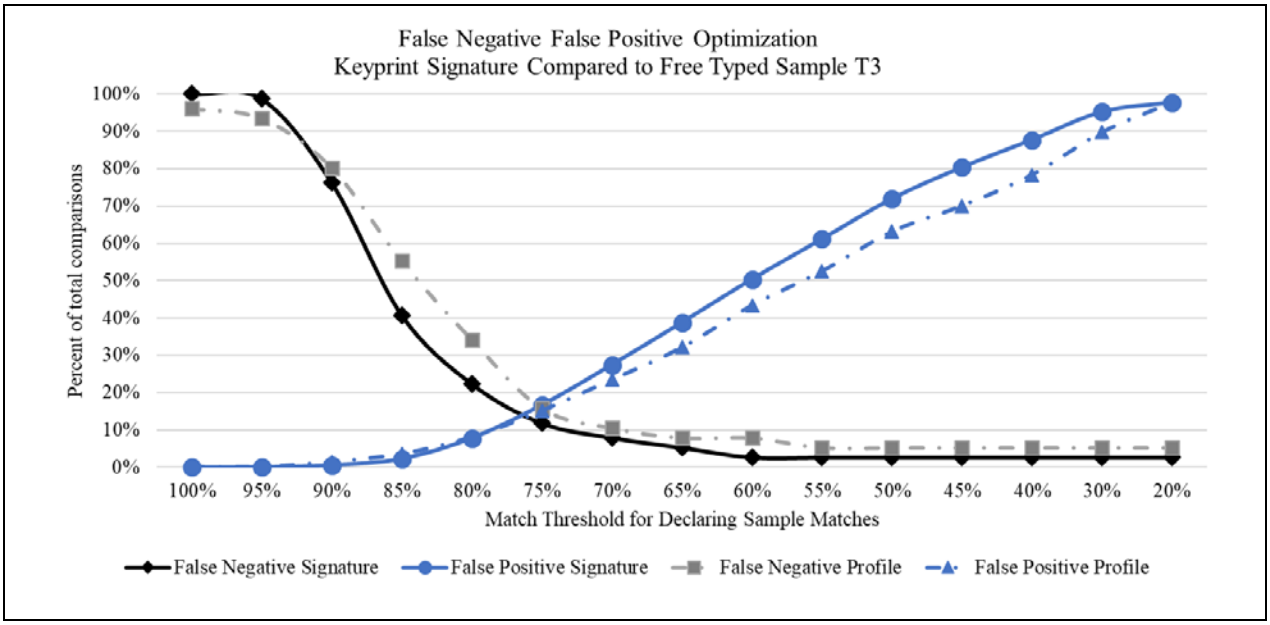

Figure E5. False Negative False Positive Optimization Keyprint Signature Compared to Free Typed Sample (T3) – Method 2. Optimization occurs at a match threshold between 75% and 80%. The critical point for reducing false negative identifications to zero using the keyprint signature is approximately 60%. The critical point for reducing false negative identifications to zero using the keyprint profile is closer to 55%. In this regard, using the keyprint signature is slightly better than the keyprint profile.

Table E6

False Negative False Positive Optimization for Keyprint Signature and Profile (T1) Compared to Free Typed Sample (T3) – Method 1

	Match Thresholds														
	100%	95%	90%	85%	80%	75%	70%	65%	60%	55%	50%	45%	40%	30%	20%
% False Positives Keyprint Signature	1.00	1.00	0.99	0.96	0.95	0.92	0.88	0.79	0.71	0.56	0.53	0.41	0.28	0.10	0.05
% False Positives Keyprint Profile	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.03	0.05	0.09	0.14	0.21	0.36	0.64	0.87
% False Negative Keyprint Signature	1.00	1.00	1.00	0.97	0.94	0.92	0.88	0.83	0.69	0.62	0.50	0.45	0.35	0.13	0.06
% False Positives Keyprint Profile	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.02	0.04	0.08	0.13	0.20	0.30	0.56	0.82

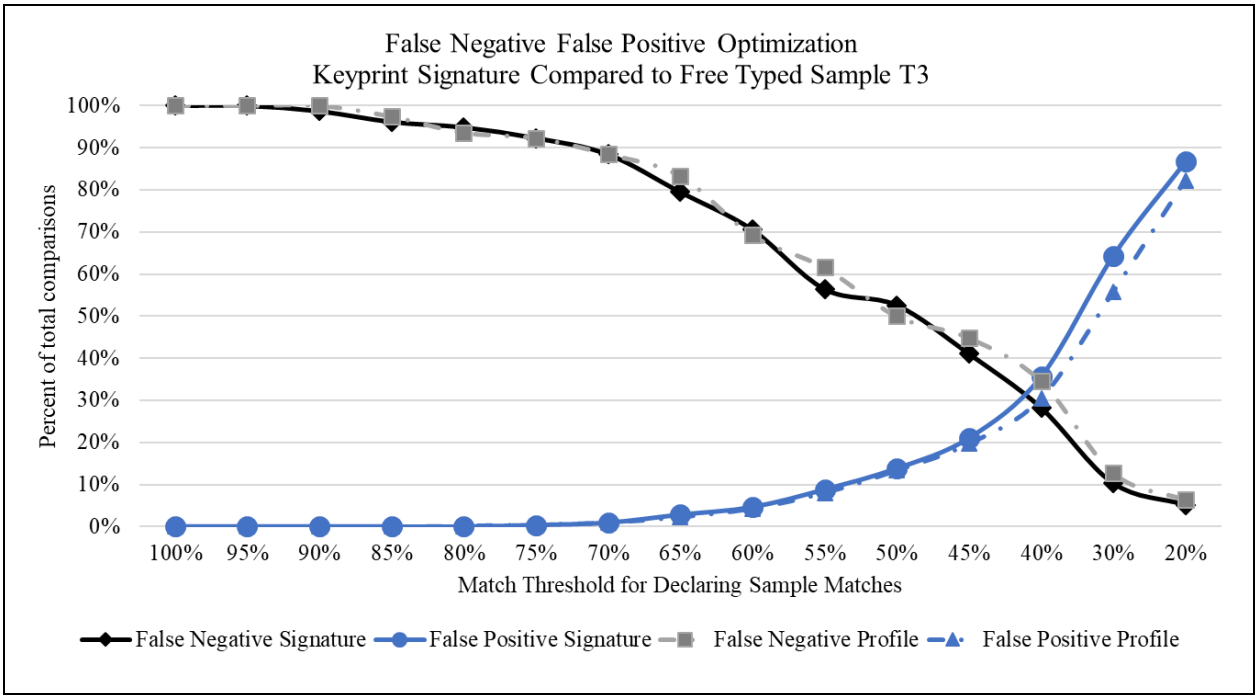

Figure E6. Method 1 - False Negative False Positive Optimization Keyprint Signature Compared to Free Typed Sample (T3) – Method 1. Optimization occurs at a match threshold at about 40%. No critical point is reached for either the keyprint signature or the keyprint profile. In this respect, using the keyprint signature is slightly better than the keyprint profile but there is still a large margin for error.

Table E7

False Negative False Positive Optimization for Keyprint Signature and Profile (T1) Compared to Free Typed Sample (T4)

	Match Thresholds														
	100%	95%	90%	85%	80%	75%	70%	65%	60%	55%	50%	45%	40%	30%	20%
% False Positives Keyprint Signature	1.00	0.94	0.77	0.37	0.15	0.10	0.09	0.05	0.03	0.01	0.00	0.00	0.00	0.00	0.00
% False Positives Keyprint Profile	0.00	0.00	0.00	0.00	0.01	0.05	0.12	0.24	0.38	0.55	0.69	0.79	0.88	0.96	1.00
% False Negative Keyprint Signature	1.00	0.92	0.72	0.44	0.26	0.10	0.09	0.04	0.04	0.03	0.01	0.00	0.00	0.00	0.00
% False Positives Keyprint Profile	0.00	0.00	0.00	0.01	0.03	0.06	0.12	0.20	0.30	0.42	0.53	0.62	0.72	0.90	0.98

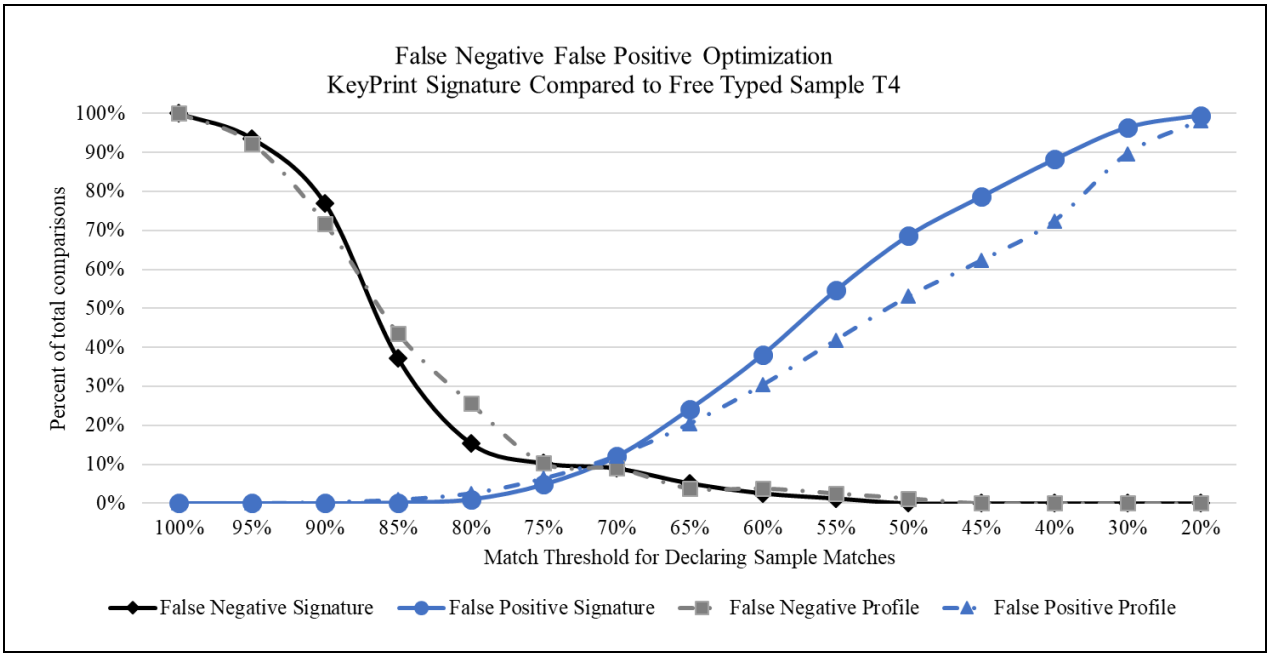

Figure E7. False Negative False Positive Optimization Keyprint Signature Compared to Free Typed Sample (T4). Optimization occurs at a match threshold at about 70%. The critical point using the keyprint signature is somewhere between 50% and 55%. The critical point for the keyprint profile is somewhere between 45% and 50%. In this regard, the keyprint signature is better than the keyprint profile.

Table E8

False Negative False Positive Optimization for Keyprint Signature and Profile (T1) Compared to Free Typed Samples (T3 and T4)

	Match Thresholds														
	100%	95%	90%	85%	80%	75%	70%	65%	60%	55%	50%	45%	40%	30%	20%
% False Positives Keyprint Signature	1.00	0.94	0.74	0.33	0.14	0.10	0.08	0.03	0.01	0.00	0.00	0.00	0.00	0.00	0.00
% False Positives Keyprint Profile	0.00	0.00	0.00	0.00	0.01	0.05	0.11	0.23	0.37	0.54	0.67	0.77	0.87	0.96	0.99
% False Negative Keyprint Signature	0.99	0.91	0.68	0.42	0.23	0.14	0.08	0.03	0.01	0.01	0.00	0.00	0.00	0.00	0.00
% False Positives Keyprint Profile	0.00	0.00	0.00	0.01	0.02	0.05	0.11	0.18	0.29	0.40	0.51	0.60	0.71	0.88	0.98

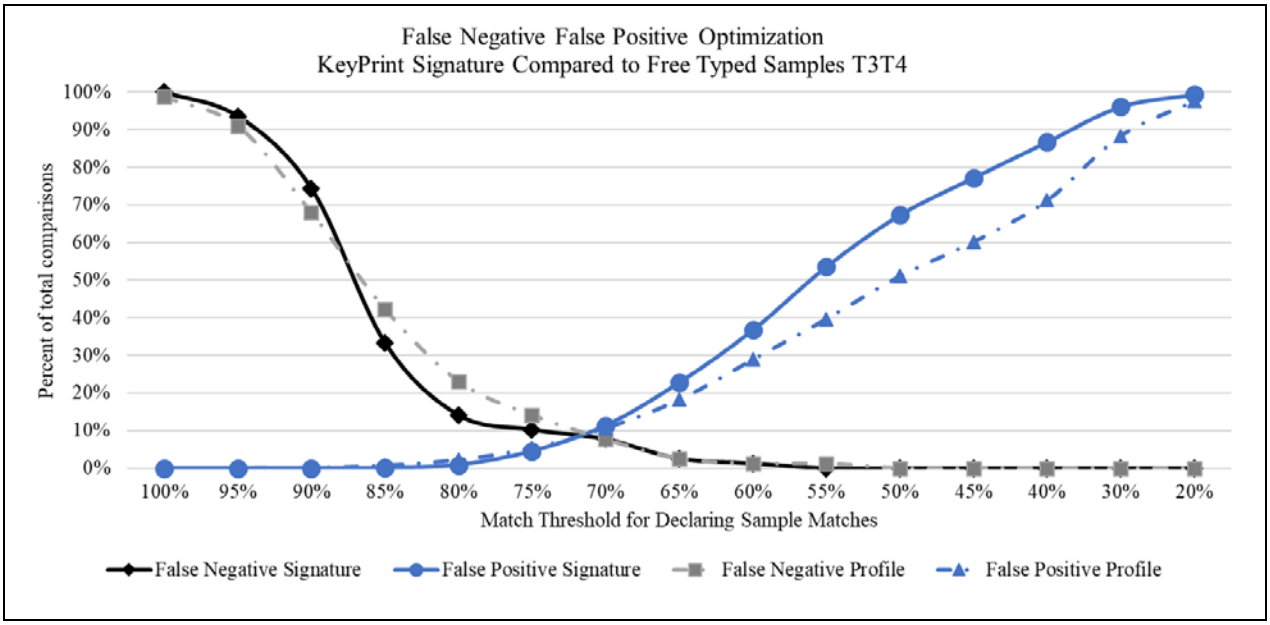

Figure E8. False Negative False Positive Optimization Keyprint Signature Compared to Free Typed Samples (T3 and T4) – Method 2. Optimization occurs at a match threshold at about 70%. The critical point using the keyprint signature is somewhere between 50% and 55%. The critical point for the keyprint profile is somewhere between 45% and 50%. In this regard, the keyprint signature is better than the keyprint profile.

Table E9

False Negative False Positive Optimization for Keyprint Signature and Profile (T1) Compared to Mild Impediment Sample (T5)

	Match Thresholds														
	100%	95%	90%	85%	80%	75%	70%	65%	60%	55%	50%	45%	40%	30%	20%
% False Positives Keyprint Signature	1.00	0.90	0.64	0.28	0.10	0.05	0.04	0.01	0.01	0.01	0.00	0.00	0.00	0.00	0.00
% False Positives Keyprint Profile	0.00	0.00	0.00	0.01	0.03	0.11	0.22	0.37	0.52	0.66	0.81	0.88	0.94	1.00	1.00
% False Negative Keyprint Signature	0.97	0.87	0.64	0.42	0.15	0.09	0.05	0.03	0.03	0.03	0.01	0.00	0.00	0.00	0.00
% False Positives Keyprint Profile	0.00	0.00	0.01	0.02	0.05	0.11	0.20	0.31	0.42	0.53	0.65	0.74	0.82	0.95	0.99

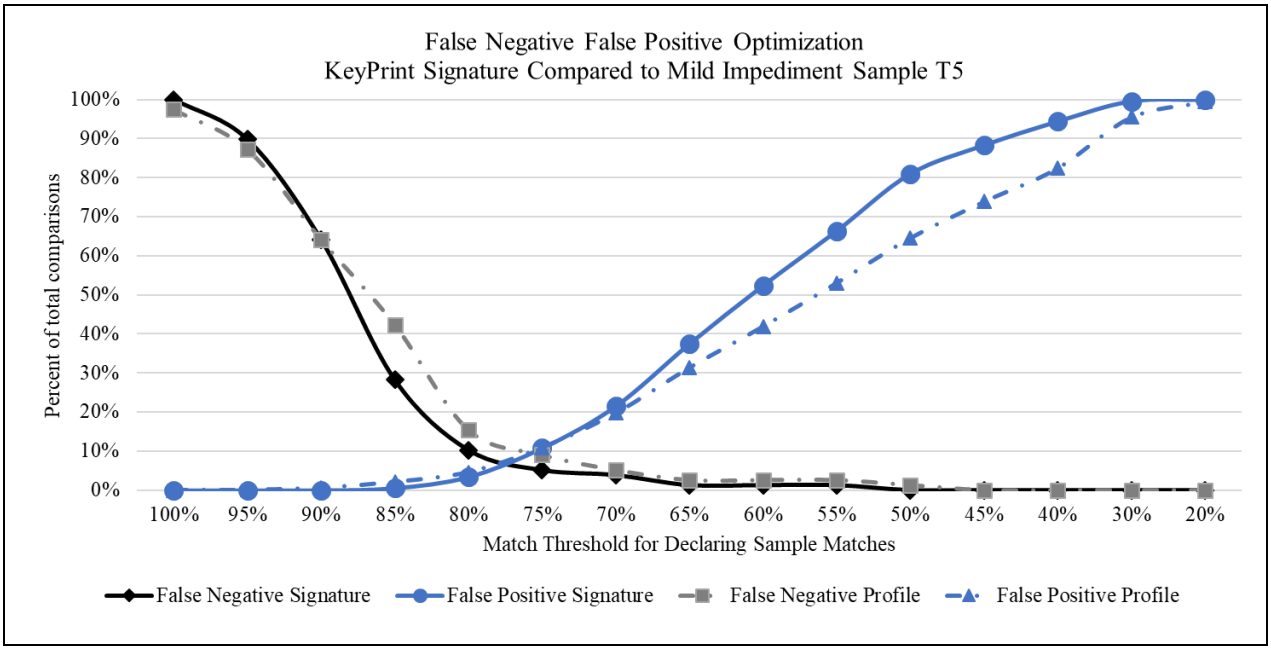

Figure E9. False Negative False Positive Optimization Keyprint Signature Compared to Mild Impediment Sample (T5) – Method 2. Optimization occurs at a match threshold between 75% and 80%. The critical point using the keyprint signature is somewhere between 50% and 55%. The critical point for the keyprint profile is somewhere between 45% and 50%. In this regard, the keyprint signature is better than the keyprint profile.

Table E10

False Negative False Positive Optimization for Keyprint Signature and Profile (T1) Compared to Moderate Impediment Sample (T6)

	Match Thresholds														
	100%	95%	90%	85%	80%	75%	70%	65%	60%	55%	50%	45%	40%	30%	20%
% False Positives Keyprint Signature	1.00	0.97	0.94	0.83	0.74	0.55	0.41	0.29	0.18	0.06	0.03	0.01	0.00	0.00	0.00
% False Positives Keyprint Profile	0.00	0.00	0.00	0.00	0.01	0.04	0.11	0.20	0.35	0.49	0.64	0.75	0.85	0.96	0.99
% False Negative Keyprint Signature	1.00	0.94	0.90	0.78	0.72	0.58	0.46	0.36	0.23	0.14	0.06	0.06	0.04	0.00	0.00
% False Positives Keyprint Profile	0.00	0.00	0.00	0.01	0.03	0.06	0.11	0.18	0.27	0.38	0.50	0.59	0.69	0.86	0.96

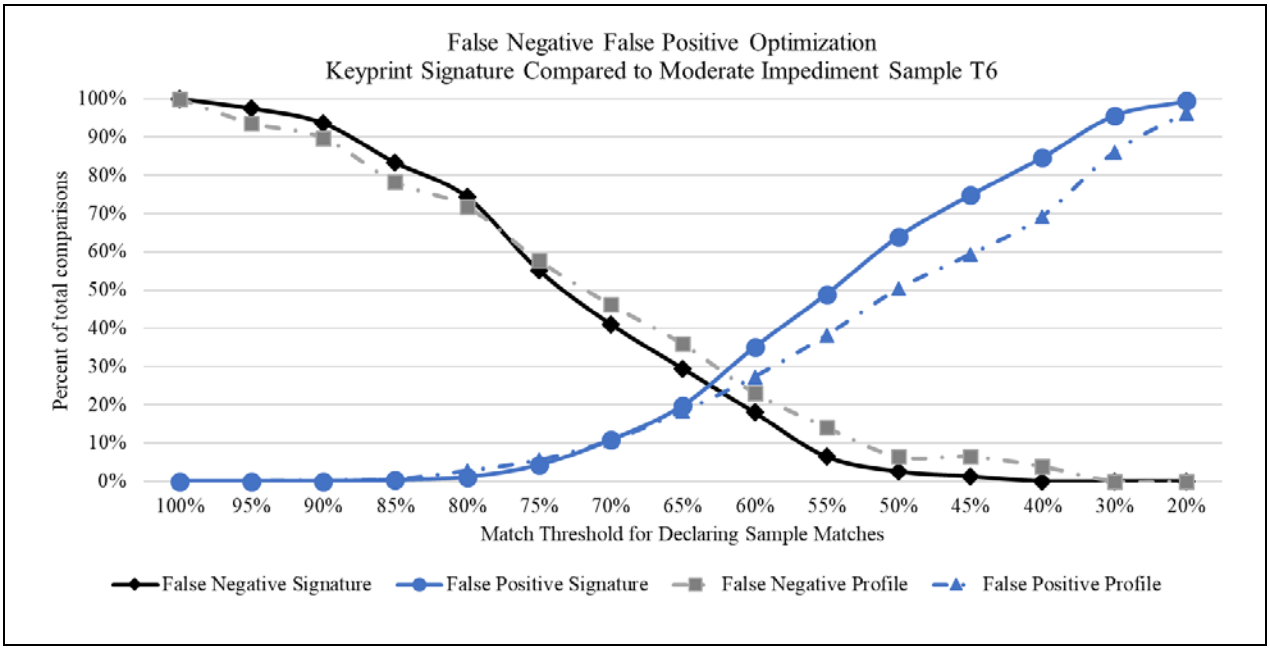

Figure E10. False Negative False Positive Optimization Keyprint Signature Compared to Moderate Impediment Sample (T6) – Method 2. Optimization occurs at a match threshold between 60% and 65%. The critical point using the keyprint signature is somewhere between 40% and 45%. The critical point for the keyprint profile is somewhere between 30% and 40%. In this regard, the keyprint signature is better than the keyprint profile.

Table E11

False Negative False Positive Optimization for Keyprint Signature and Profile (T1) Compared to Impediment Samples (T5 and T6)

	Match Thresholds														
	100%	95%	90%	85%	80%	75%	70%	65%	60%	55%	50%	45%	40%	30%	20%
% False Positives Keyprint Signature	1.00	0.95	0.90	0.65	0.50	0.31	0.13	0.04	0.01	0.01	0.01	0.00	0.00	0.00	0.00
% False Positives Keyprint Profile	0.00	0.00	0.00	0.00	0.01	0.05	0.12	0.27	0.40	0.56	0.68	0.80	0.90	0.98	1.00
% False Negative Keyprint Signature	0.97	0.94	0.86	0.71	0.58	0.40	0.24	0.13	0.06	0.03	0.03	0.03	0.00	0.00	0.00
% False Positives Keyprint Profile	0.00	0.00	0.00	0.01	0.02	0.06	0.11	0.19	0.29	0.40	0.52	0.62	0.73	0.89	0.98

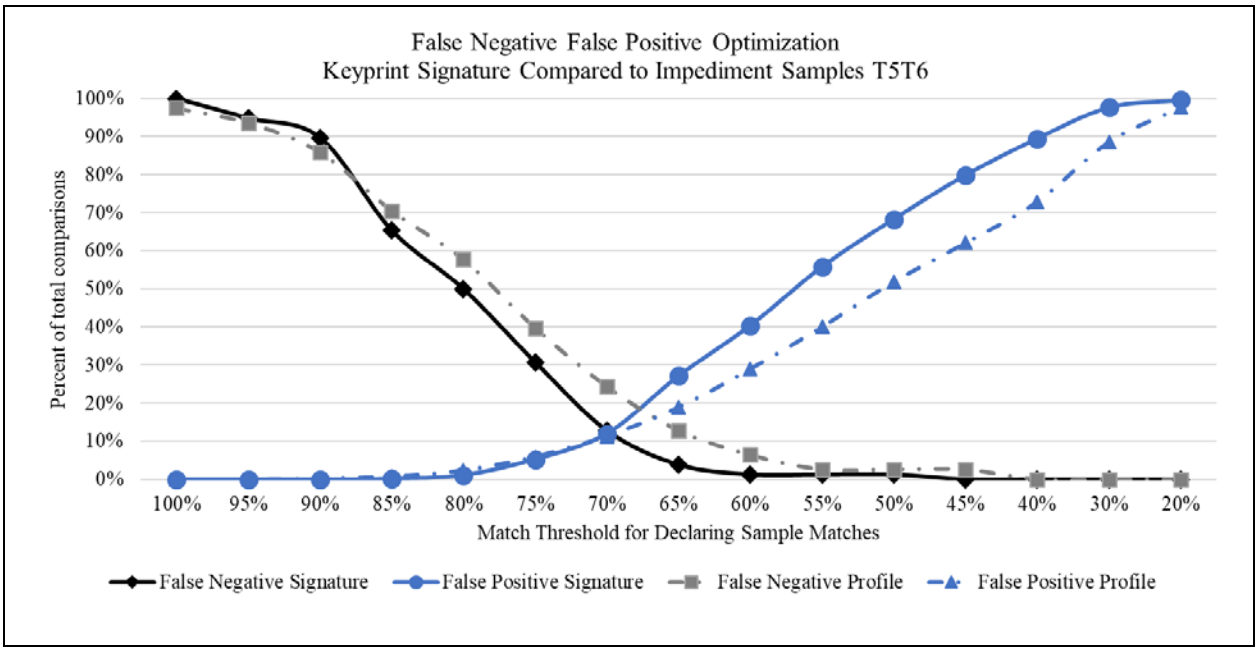

Figure E11. False Negative False Positive Optimization Keyprint Signature Compared to Impediment Samples (T5 and T6) – Method 2. Optimization occurs at a match threshold between 75% and 80%. The critical point using the keyprint signature is somewhere between 50% and 55%. The critical point for the keyprint profile is somewhere between 45% and 50%. In this regard, the keyprint signature is better than the keyprint profile.

Table E12

Number of Keyprint Signature Characters identified for T3 and deleted for T3 Method 2 – Participants 1-26

Participant	T3 Profile Characters	T3 Profile Characters Missing Data	Actual Data Points Used in T3 Method 2	Too Few (9 or fewer) Removed From Data for Method 2 (41 total)
1	24	11	13	
2	10	5	5	X
3	44	22	22	
4	39	27	12	
5	18	14	4	X
6	40	35	5	X
7	15	8	7	X
8	21	19	2	X
9	30	22	8	X
10	33	28	5	X
11	51	46	5	X
12	19	11	8	X
13	39	22	17	
14	59	27	32	
15	18	14	4	X
16	22	13	9	X
17	32	12	20	
18	32	13	19	
19	21	15	6	X
20	10	5	5	X
21	32	18	14	
22	60	25	35	
23	15	14	1	X
24	35	18	17	
25	4	3	1	X
26	34	17	17	

Table E13

Number of Keyprint Signature Characters identified for T3 and deleted for T3 Method 2 – Continued; Participants 27-54

Participant	T3 Profile Characters	T3 Profile Characters Missing Data	Actual Data Points Used in T3 Method 2	Too Few (9 or fewer) Removed From Data for Method 2 (41 total)
27	31	19	12	
28	32	15	17	
29	17	10	7	X
30	3	2	1	X
31	14	9	5	X
32	26	13	13	
33	18	13	5	X
34	39	23	16	
35	25	18	7	X
36	23	18	5	X
37	55	24	31	
38	24	20	4	X
39	61	42	19	
40	17	12	5	X
41	0	0	0	X
42	2	1	1	X
43	18	10	8	X
44	31	9	22	
45	16	8	8	X
46	40	26	14	
47	39	25	14	
48	11	8	3	X
49	35	24	11	
50	42	17	25	
51	20	9	11	
52	31	22	9	X
53	11	6	5	X
54	18	8	10	

Table E14

Number of Keyprint Signature Characters identified for T3 and deleted for T3 Method 2 – Continued: Participants 55-78

Participant	T3 Profile Characters	T3 Profile Characters Missing Data	Actual Data Points Used in T3 Method 2	Too Few (9 or fewer) Removed From Data for Method 2 (41 total)
55	47	29	18	
56	22	15	7	X
57	39	25	14	
58	34	21	13	
59	45	23	22	
60	30	14	16	
61	34	20	14	
62	38	18	20	
63	33	19	14	
64	33	22	11	
65	4	3	1	X
66	23	15	8	X
67	38	13	25	
68	33	21	12	
69	30	22	8	X
70	32	14	18	
71	50	36	14	
72	9	6	3	X
73	23	15	8	X
74	32	23	9	X
75	27	23	4	X
76	37	23	14	
77	19	10	9	X
78	26	20	6	X