SECURING UNFAMILAR SYSTEM ENTRY POINTS

AGAINST FAULTY USER AUTHENTICATION VIA

ELECTROMAGNETIC SIDE CHANNEL ATTACKS

Approved by:

_____

Dr. Mitchell A. Thornton, Advisor

_____

Dr. Sukumaran Nair

_____

Dr. Stephen Szygenda

SECURING UNFAMILAR SYSTEM ENTRY POINTS AGAINST FAULTY USER AUTHENTICATION VIA ELECTROMAGNETIC SIDE CHANNEL ATTACKS

A Thesis Presented to the Graduate Faculty of the

Bobby B. Lyle School of Engineering

Southern Methodist University

in

Partial Fulfillment of the Requirements

for the degree of

Master of Science in Computer Engineering

with a

Major in Computer Engineering

by

John J. Howard

(B.S.Cp.E, Southern Methodist University)

May 15, 2010

Howard, John J. B.S.Cp.E., Southern Methodist University, 2010

Securing Unfamiliar System Entry Points
Against Faulty User Authentication Via
Electromagnetic Side Channel Attacks

Advisor: Professor Mitchell A. Thornton

Master of Science conferred May 15, 2010

Thesis completed April 9, 2010

This research presents concepts intended to reduce a system's vulnerability to a password sniffing technique that exploits differential current usage in hardware, known as an electromagnetic side channel attack. The first countermeasure discussed is an augmentation to the standard register design that significantly reduces the amount of electromagnetic interference produced by these circuits. Furthermore, this paper outlines a novel approach to user authentication based on keystroke dynamics that, in the event a user's password is compromised by this kind of attack, renders this information insufficient as a standalone credential for system login.

One well documented security concern when using a keyboard as an input device to a system is the capability of an individual to measure electromagnetic emanations produced by the changes in current and register states associated with a user's keystroke activity. By capturing and analyzing these signals an attacker can discover the user's exact keystroke pattern, possibly revealing a password or other sensitive information. Background research was conducted into this form of computer system attack and causes

as well as potential countermeasures identified. Techniques known as signal strength reduction and signal information reduction are described as traditional corrective methods. However, because of limited commercial interest, these approaches have not been applied to vulnerable system entry point devices such as the standard keyboard. To address this potential security concern a new model of register was created with an emphasis on equalizing current flow to the various nets within a device. Using this design significantly reduces the electromagnetic interference produced by the keyboard device, making it considerably harder to isolate the information bearing signal from standard atmospheric noise, thus hardening the system against this type of a side channel attack.

Despite significantly reducing the possibility of an electromagnetic side channel attack, the use of these secure registers does not entirely eliminate the potential for hardware signal interception. Consequently, an improved keystroke dynamics algorithm is also presented which when used in combination with interference reducing registers provides near total protection from hardware password sniffing techniques. Keystroke dynamics is a field of study that leverages an individual's consistently demonstrated tendencies when typing commonly used words as a means of behavioral biometric identification. Prior to the presentation of a novel augmentation to this concept, an investigation into traditional methods for identifying and isolating the unique characteristics of user's typing pattern was performed. Concepts of "flight" and "down" time were recognized as established means for these purposes and the outcome of research implementing these mechanisms produced and analyzed. Close examination of

these results showed inconsistencies in the ability of such routines to consistently and accurately determine user identification based on these two heuristics alone. Consequently, new capabilities which incorporated the concept of pressure were modeled and added to expand upon the original timing based characteristics of this biometric technique. These enhancements resulted in substantial increases in the accuracy of the overall authentication routine such that this method of user recognition now displays the potential for deployment as a standalone system that further could diminish the threat posed to keyboard entry devices by electromagnetic side channel attacks.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

First and foremost I would like to recognize and express my unwavering gratitude and love to my family for their constant support throughout this process. Furthermore I must thank Dr. Thornton, my adviser, as well as Dr. Nair, and Dr. Szygenda for their guidance and intellectual encouragement. Lastly, I would like to acknowledge my friends and colleagues, especially Jeff Allen for his partnership, insight, and tireless work on developing the biometric keyboard application. Without his vision this project never would have become a reality much less experienced the level of success it has up to this point.

Chapter 1

INTRODUCTION

The keyboard is one of the most common devices used to input information into a computer system. While extended work has been done in the area of computer security as it relates to information already contained within a software or network system, little emphasis has been placed on the authentication and integrity of data at this initial system entry point. Despite its under-researched nature, significant security concerns exist at this crucial junction in the overall information assurance process. These concerns include, but are not limited to, data interception and user authentication. Data interception is the act of a third party recording the signals produced by a system. This information can then be used for a variety of purposes such as discovering compromising information about the system's operation or to gain unauthorized access at some point in the future. In the field of network security the latter case is commonly referred to as a replay attack and has received considerable attention. However, the monitoring of computer signals can occur at any level within the system including software and hardware. User authentication involves evaluating credentials submitted by an individual with the intent of allowing or denying system access. These materials can be knowledge, token, or biometric based or some combination therein. Moreover, there is generally a direct relationship between the number of authentication classes required by a system and the

perceived security of that system. The focus of this research is to address these two security issues by proposing design enhancements to prevent the capture of electromagnetic signals produced at the circuit level and to introduce a novel augmentation to the user authentication process based on behavioral biometrics.

Data interception at the hardware level receives relatively little attention as compared to the emphasis this security concern enjoys in the networking field. The majority of attention in this field of study has been given to countering side channel cryptanalysis, which is the process of obtaining and then analyzing information, such as power consumption and produced electromagnetic interference, leaked from the operation of a hardware system. It has been proven that using this information and differential analysis the encryption primitives of several smart cards can be obtained [8]. More relevant to this research however is the possibility that an attacker could record the electromagnetic signatures produced by changes in current and internal register state of a standard keyboard and then use this information to discover a person's password or other sensitive information.

Efforts to reduce the possibility of this type of side channel attack have largely focused on two key areas. Firstly, reducing the possibility of an attacker obtaining such information, called signal strength reduction, and secondly, reducing the possibility that if obtained these signals contain any usable information, called signal information reduction. Signal strength reduction uses electromagnetic shielding to ensure that emanations omitted by device components are weakened and therefore undetectable by modern antennas [6]. This is the approach adopted by most government agencies,

explaining why secure devices, rooms, and even entire buildings employ expensive metallic shielding. The second common means of preventing side channel attacks, signal information reduction, attempts to adapt standard circuit elements to ensure that a minimal amount of constructive interference is generated. One method to acheive this desirable quality is signal balancing, which involves offsetting events that produce electromagnetic interference with a set of events that are electromagnetically neutral, essentially balancing the interference generated by the circuit component as a whole. Another approach involves randomizing the produced electromagnetic interference for a single execution sequence [7]. This ensures that attackers are unable to reliably interpret the magnetic signature of hardware events and therefore cannot statistically determine what input stimuli affect different parts of the system.

Behavioral biometric identification attempts to distinguish individuals based on the measurement of some learned routine. This subset of the larger biometric identification class is generally viewed as far less accurate than physiological biometrics, which measure innate features such as fingerprints or DNA samples. This is because physiological characteristics are largely invariant over time, whereas behaviors can be modified or even unlearned completely. Despite this fact several reliable methods for behavioral biometric identification have been developed including gait recognition, handwritten signature analysis, and keystroke dynamics.

Keystroke Dynamics involves measuring and analyzing certain distinguishable aspects of a person's typing habits in real time as they enter information into a terminal. This information can then be compared to a standard template of a user's keystroke

tendencies and used to either confirm or repudiate identity. Previous work in this field has largely focused on timing the period between the keystrokes and other timing based measurements such as total time to type a given word [1]. More commonly this timing can be broken down into “flight” and “dwell” time, which are defined as the time a user is in transition between two keys and the time a user holds down a specific key, respectively. Despite noticeable effort by the research community [1, 4, 5], this field of research has largely failed to produce results comparable to those obtained using conventional biometric authentication.

Our approach to counteracting the electromagnetic side channel attack involves implementing a register that uses signal balancing to significantly reduce current differential within keyboard registers. We will show the design theoretically leads to vast reductions in electromagnetic signal production thereby providing increased security against attacks that capture and analyze these signals. We also seek to further secure user authentication systems against this form of attack by augmenting current timing based models of keystroke dynamics with pressure sensitive heuristics. Adding both a measure of maximum pressure and matching a pressure curve to the pattern in which the user depresses any particular key greatly increases the degrees of freedom associated with this biometric. By employing both of these two methodologies, the vulnerability of keyboard input systems to electromagnetic side channel attacks and unauthorized use is significantly reduced.

Chapter 2

BACKGROUND

This section discusses the background topics that support this research. First, a discussion of key principles related to user authentication is presented to provide a framework for understanding the proposed security enhancements outlined by this paper. Secondly, key motivations for the research into entry point security and its place in the spectrum of the information assurance process are explained. Next, we discuss the theory surrounding the electromagnetic side channel attack, present research detailing the severity of this form of password sniffing, and describe approaches designed to counteract its threat. Concepts surrounding the field of keystroke dynamics are also presented and previous work in this area discussed. Finally, this chapter presents a description of our methods for eliminating the possibility of faulty user authentication due to an electromagnetic side channel attack.

2.1 User Authentication

The ultimate goal of computer security, whether it is at the hardware, software, or network level, is to prevent the unauthorized access of sensitive data. The first step in the user authentication process is to accurately identify the individual attempting the access the system. Any one of the dozens of common identification schemes generally fall into one of three primary categories: what you have, what you know, and who you are [9].

The more categories implemented by a security system, for example using a password (what you know) and a key card (what you have), the more secure that system is thought to be. "What you have" is the category used to delineate measures that operate via the possession of a physical device, such as a badge card. "What you know" has been the traditional means of computer access and relies on some unique and secretive knowledge that only an authorized user is thought to possess, such as user name and password schemes. "Who you are" is most commonly thought of as biometrically identifying an individual using some unchanging and unique physical detail, such as a fingerprint or retinal scan. However, more behavioral details, such as a written signature or the way someone walks, can also be thought of as biometrically relevant although typically less accurate than physiological measurements. This topic will be discussed in detail in later sections.

2.2 Entry Point Security and the Information Assurance Process

As society becomes increasingly mobile the access of information over networks has become more common. As a consequence, much research and effort has been put into securing network systems from malicious observation and manipulation. However, another largely overlooked consequence of this tremendous increase in human mobility has been the corresponding rise in the manner of ways and number of locations from which legitimate users access their data. Public workstations are used every day to view sensitive personal and corporate information at locations ranging from coffee shops to hotel lobbies.

These *unfamiliar systems* are just a few examples of entry points that are vastly more susceptible to manipulation by outside parties than the traditional desktop that remains safely locked inside a home or place of business. The principle goal of user authentication as it relates to network security is to ensure that the digital signals which represent identifying attributes cannot be manipulated or forged. However, another equally important aspect is that these attributes cannot be forged or stolen before they have been digitized for transmission to an authentication service. This is the concept of entry point security and as the use of unfamiliar systems increases it must receive additional attention in order to ensure an unbroken chain of security from legitimate user to remote data.

2.3 Electromagnetic Side Channel Attacks on Unfamiliar Systems

One of the greatest entry point security concerns related to the knowledge (What you know) based systems which dominate the modern computer landscape is the possibility that the information required for authentication has been intercepted and is now being used by an illegitimate party. One of the particularly well documented [21] techniques used by attackers to achieve these goals is password sniffing via the capture of electromagnetic emanations or interference that radiate from keyboards. These physical anomalies arise because of changing current flows within the various channels of a device. In modern CMOS circuits current is required to change the state of any continuous section of wire, also called a net, while holding these fields constant uses little to no current flow. Because at some level all hardware components can be modeled as a series of interconnected nets, any device which switches several different nets at one time

will require a surge in electrical power. This often sudden change in current flow and consequently netlist state is usually modeled as a short burst of square waves with sharp rising and falling edges and emits electromagnetic signals with a frequency related to the duration of the rise or fall time and the pulse frequency. These emanations carry information about the current flow, netlist state, and consequently the device's operation. If these waves are intercepted and properly interpreted they can reveal the events that are occurring on a piece of hardware at any given clock cycle.

Electromagnetic interference can be divided into two general categories: direct and unintentional, or indirect emanations. Direct interference results from intentional current flows from one system component to another. These generally coincide with a sharp burst of current at the rising edge of a square wave clock cycle and can be observed over a wide range of frequencies, depending on the state transition time. Unintentional emanations results from interactions between device components that exist at close proximity. These are often easier to detect than direct signals because they propagate as modulations of carrier signals, which can be picked up at greater distances away from a device than direct radiation. However, discerning the exact cause of this type of interference is much harder even for circuit designers and usually only becomes evident during compliance testing [8]. Consequently, information retrieval from this variety of radiation is generally harder, although not impossible.

The emanations generated by increased current flows propagate through space by a combination of radiation and conduction. Generally the presence of these signals can be observed through the use of a wide range receiver set to scan its entire frequency range.

The recorded output is then demodulated based on its Amplitude Modulation or Frequency Modulation in an attempt to isolate signals of interest. Once any such signal is identified, filtering and narrow band antennas can be used to decrease the signal to noise ratio to extract useful information [8, 21].

The first recorded use of these signals to perform an attack on a computer signal occurred in the 1960s when British MI5 scientists, after several unsuccessful attempts at breaking a French diplomatic cipher, noticed a faint electromagnetic phenomenon in the enciphered traffic. This signal turned out to be the plain text which had leaked through the cipher machine as a result of electromagnetic emanations [19].

More recently, Agrawal et al. in [6] demonstrate this manner of attack by placing a simple near-field probe on the back of a smart card and an employing an Amplitude Modulation (AM) receiver. Using only this simple equipment, they are able to successfully isolate a 13 instruction loop and identify the conditions within the device's registers that caused the processor to begin this series of execution. Once these conditions were discovered, by simply modifying the perceived values coming from the register file their team was able to infinitely lock the card's operation inside this loop.

In terms of user authorization and entry point security these same EM emanations utilized in [6] and [19] can easily be monitored to determine a user's password. Most modern keyboards operate on the basic principle that a grid of broken circuits, called the key matrix, lies underneath the physical keys. When a user presses, a key a switch is depressed that completes the circuit causing current to flow. Since EM emanations are the consequence of differential current flow it naturally follows that keystrokes cause

distinctive patterns of electromagnetic interference to be produced from a keyboard. If these signals were intercepted by an attached probe or, perhaps more concerning, a remote antenna they could be easily filtered to reveal a user's typing history and potentially a password or other sensitive information. Vuagnoux and Pasini [21] definitively demonstrated the catastrophic nature of this security weakness with their 2009 study in which they were able to recover nearly 95% of keystrokes typed on a several varieties of both wired and wireless keyboard at distanced of up to 20 meters and through walls. The extent of this problem has been recognized by various government and intelligence organizations since the 1960s and is one of the main reasons secure buildings employ expensive shielding materials against these electromagnetic emanations, or Tempest radiation, so named after a U.S. government program to counteract their affect [20].

Unfortunately, the modern computer user cannot rely on electromagnetic shielding when accessing sensitive information on unfamiliar work stations. Moreover, it has been argued that this form of signal strength reduction alone will never fully solve the problems associated with Tempest radiation because shielding never entirely eliminates electromagnetic signals coming from a device [7]. Shielding can only reduce and obscure these signals but even at the most elementary physical level, the interaction of an electromagnetic wave with another atomic structure (such as shielding material) induces oscillations within that structure, which in turn produce more electromagnetic waves. Granted, shielding does provide a prohibitive factor in an attacker's attempts to analyze

tempest radiation. However as knowledge of a shielding scheme and antenna sensitivity increases, this factor is markedly reduced.

2.4 Signal Information Reduction

For reasons discussed above, the only truly effective long term solution to electromagnetic emanations, especially as they relate to unfamiliar entry points, is signal information reduction. This methodology attempts to ensure that while tempest radiation might emanate from a device, the information contained within its frequencies is minimal harmful at best. Several designs to accomplish this goal have been suggested. However, because of prohibitive costs, littler commercial interest in either signal strength or signal information reduction has ever been achieved.

Two general approaches have been proposed, namely the randomization of general operations' execution sequence over time and electromagnetic balancing. Randomization involves executing particular portions of an algorithm in different orders with the goal of confusing attempts to reliably interpret the electromagnetic emanations that are produced as a result. This can be as simple as initializing variables or recalling them from memory in different permutations for each iteration of a particular loop. However, because of the vast interdependencies of the various modules of most modern algorithms, Chari et al. [7] suggest this approach will never achieve true randomness and a "casual order" will always be discernable as the device executes its various stages. The alternative, load balancing, requires that any event producing a significant electromagnetic signal, i.e. consuming current, be offset by a complementary event which causes some other portion of the device to significantly reduce its current dissipation.

Again, Chari et al., point out evident faults in this approach by noting that balancing attempts will be ineffective at high resolutions because they never achieve perfect symmetry between the offsetting sequences.

Kuhn in his Cambridge doctoral dissertation [22] did extensive work on the feasibility of remotely obtaining information from electronic devices, specifically monitors. While only limited countermeasures are suggested or tested, one promising solution seemed to be adding a significant source of background radiation that is of a similar frequency to the electromagnetic emanations in order to mask the information carrying signal. Having several independent sources generating such a signal also significantly interrupted the team's ability to isolate and analyze the emanation coming from their control device because the multiple background producers were out of phase with each other. However, this notion proves impractical for use on unfamiliar systems because it requires individuals to transport and employ external equipment for effective implementation.

Despite the best efforts of security engineers, the total elimination of electromagnetic emanations from hardware will more than likely never be achieved. This has little to do with circuit design but is instead a property of the physical laws governing the creation and containment of these waves. While significant progress is undoubtedly possible, as we hope to demonstrate in this paper, other measures such as using biometrics must be taken to harden authentication processes against malicious intentions.

2.5 Biometric Identification on Unfamiliar Systems

Of the three previously discussed primary classes for user identification, biometrics (who you are) hold a distinctive advantage over both knowledge based (what you know) and token based (what you have) methods [10]. This is a consequence of the obvious fact that the former scheme is based on inherent attributes of a given individual while the latter two are based on aspects that can be lost, stolen, or simply forgotten. Generally, biometric identification is divided into two general categories which have already been briefly touched on: physiological and behavioral [3]. Physiological biometrics deals with innate features of an individual's identity while the measurement of learned routines falls into the behavioral category. In most cases, physiological features are extensively more accurate because they are invariant over time. However, biometric identification of this type typically requires external and often expensive equipment to record, such as iris scanners or fingerprint readers. Behavioral features are generally less accurate but certain extensively repeated and therefore muscularly ingrained operations such as an individual's written signature have been shown to be reliable means of confirming identity.

Because of the external equipment needed to measure physiological biometrics, their implementation is generally not practical on unfamiliar systems. Keystroke dynamics however is a means of behavioral biometric identification that requires only a keyboard, a device almost universally found on modern computer systems.

2.6 Identification based on Keystroke Characteristics

Gains et al. [12] were the first to study the timing information between keystrokes as a means of individual identification. They attempted to create a matrix of *digraph latency times* or flight times between any given key and every other letter of the alphabet. Only lower case letters were used resulting in a 26x26 matrix or 676 possible two letter combinations. Their experiment asked ten RAND corporation secretaries to type a 300-400 word passage and used only digraph information for which the two letter combination appeared more than ten times. This resulted in 87 statistically significant letter combinations. To test their findings, Gains et al. developed a model for statistical comparison of each digraph latency time. This model essentially compared each individual digraph entry to the mean for that digraph of either the same secretary or a different secretary depending on whether false acceptance or false rejection rates were being produced. In this manner the team determined how often a given user is not able to consistently reproduce flight times between letters and the probability that someone else could reproduce similar flight times and thus gain faulty access to the system. Using this model and eliminating redundant tests, 55 comparisons were carried out on the data. The results show a combined false acceptance rate of zero and a false rejection rate of 4%. Moreover, Gains was able to run his analysis on individual two key combinations and found that if only a select subset were used, namely **`in`**, **`io`**, **`no`**, **`on`**, and **`ul`**, that both the false acceptance and false rejection rates dropped to zero.

Because of the extremely small test pool in this study, minimal importance can be given to the accuracy results obtained. However, this work did show the feasibility of

keystroke dynamics (although the name had not been coined at the time) as a possibility for obtaining identifying credentials from a user.

The next major set of experiments conducted on Keystroke dynamics were conducted by Leggett, Williams, and Umphress and presented in a series of papers [13, 14, 15]. This team's first effort [15] had 17 programmers type a control paragraph of 1400 characters and a second test paragraph of 300 characters. This test expanded on Gains' original idea by comparing the overall mean of the users keystroke latencies in addition to statistically significant digraph flight times. The team considered a test signature to be verified if more than 60% of the test latencies were deemed valid. The requirement for a test latency to be deemed valid was that it fell within 0.5 of a standard deviation of the mean digraph latencies for the control signature. The results from this study show that the mean latency time, which basically measured the user's average typing speed, did not improve the accuracy results as obtained by [12].

The team's next study [13] expanded the test pool to 36 participants which typed a 537 character paragraph on two separate occasions. The measure of mean keystroke latency was dropped and the space bar was added to the digraph latency matrix, causing its size to increase from 676 to 729. A number of different tests were performed on the digraph latency times, including generating false acceptance and rejection rates if only right hand or only left hand digraphs are used, as well as only using the subset identified by [12] and the 15 most frequently typed digraphs. These tests produced interesting results, such as that using the subset of digraphs that produced zero percent false acceptances and false rejections in [12] resulted in false acceptance and rejection rates of

17% and 30% in [15], respectively. Ultimately however, it was discovered that the best accuracy results were obtained from using the set of digraphs that had maximum latencies under 500 milliseconds. Using these heuristics, the team obtained false rejection rates of 5.5% and false acceptance rates of 5.0% by again using the same comparison method described in their first experiment.

Further research conducted by Joyce and Gupta [2] explored the possibility of augmenting login credentials with additional information, in this case a first and last name, and performing keystroke analysis on these fields. Their research involved thirty-three users going through a reference session in which they are asked to type their username, password, as well as first and last name eight times. The flight times for each letter in these fields were calculated and those that were three standard deviations from the mean discarded. Joyce and Gupta rejected the comparison technique used in [15, 13] because the 60% validity rule allowed a test vector to pass even if up to 40% of the some of the test signature latencies to differed substantially from the control signature. Their team instead opted to view the comparison as a measurement of the difference between a test vector T and a control vector M where:

$$M = \{m_{username}, m_{password}, m_{firstname}, m_{lastname}\}$$
$$T = \{t_{username}, t_{password}, t_{firstname}, t_{password}\}$$

Such that each *m* is a vector consisting of the mean digraph times observed in the reference sessions and each *t* is a vector consisting of the digraph times observed in a subsequent login attempt. In this manner the difference between M and T can simply be viewed as the L_1 or Manhattan norm of the difference between M and T. Their

approach also used the novel concept of adapting the threshold for acceptance based on the variance of the eight reference signatures. In this manner, a user who had little variability in how they type would be expected to meet a much more stringent condition for verification than a user who demonstrated a large degree of inconsistency in their typing habits.

Their research reported two separate results. The first requires test signatures to fall within a threshold of the mean plus 1.5 standard deviations for verification and has a false rejection rate of 16.36% and a false acceptance rate of 0.25%. The second modifies this condition to allow verification if a test signature is within the mean plus 2.0 standard deviations and modifies the false rejection and acceptance rates to 6.67% and 0.8%, respectively.

Several other important contributions to the field of keystroke dynamic have been made since these original experiments. These include a patent by Garcia [4] which introduced the idea of using Mahalanobis distance when comparing a test and control signature. This essentially considered the variance of the control signature latency times when calculating the difference between them and a test signature latency time. The implementation of the Mahalanobis distance had the effect of automatically skewing the data to account for inconsistencies in typing habits and of further encouraging research into alternative comparisons techniques, despite the fact that no results are actually presented in the patient literature.

Brown and Rogers [16] were the first to implement the concept of down time as well as flight time in their work. By measuring and comparing the average time a single key

is held down in a 26 element vector, they substantially increased the amount of information their algorithm was able to leverage for its final verification decisions. Mahar et al. [17] showed using this two interval system was vastly more reliable than the original metrics based solely on latency time. This idea has been expanded by [3] to suggest that down time is affected by the preceding keystroke and possibly the following keystroke as well. This leads to the possibility of constructing a *digraph down time* matrix in addition to the previously described digraph latency matrix and possibly expanding both of these matrices into *trigraphs* as well, although no research has been done to support this concept.

Lv and Wang [18] were the first to present initial work using pressure as a third heuristic on which to base their verification algorithm. However their results gave only marginal improvements of less than a percent increase in accuracy over the results they saw when ignoring the pressure sensitive aspect.

2.7 Securing Unfamiliar Entry Points against Faulty User Authentication and Electromagnetic Side Channel Attacks

Our approach to the problem of user authentication and the electromagnetic side channel attack on unfamiliar entry points as outlined in the preceding sections is twofold. The first aspect seeks to prevent the possibility that a user's password can be hijacked by employing a current neutral register to significantly reduce the electromagnetic differential associated with depressing various keys on a standard keyboard. This design employs the load balancing technique of signal information reduction by attaching a secondary register which operates in the inverse mode of the primary register as well as

electromagnetically neutral control circuitry. Because of the relatively small scale of a keyboard's internal circuitry this load balancing attempt is feasible despite claims by [7] that such an approach is impractical. The second portion of this paper outlines a methodology for ensuring that even in a scenario where a password is compromised, an attacker will be unable to maliciously employ this information because of a sophisticated keystroke dynamic algorithm. This approach augments standard timing based keystroke analysis routines with a pressure sensitive aspect that monitors and compares not only absolute pressure as suggested by [18] but also the novel concept of a *pressure curve.* This curve attempts to increase the overall amount of information that can be obtained from a user's typing patterns by leveraging the affect that tiny muscles in the fingers have on the manner in which a user presses and releases a key. These same muscles are a critical factor in handwritten signature verification as researched by [23]. When an individual signs their name or performs any act of handwriting that has been repeatedly ingrained in their finger's muscle memory, the action is smooth and clean. However if this particular action is relatively new to the user the muscles in the fingers work in a disjoint manner, resulting in a significant amount of jitter or variability in the signature. This research intends to demonstrate this same general concept applies to the field of keystroke dynamics and to employ these findings in developing a superior algorithm for biometric identification based on observed typing tendencies.

Chapter 3

DESIGN OF ELECTROMAGNETICALLY NEUTRAL REGISTER

In order to reduce the electromagnetic emanations from a standard keyboard we must first look at the design of such a device and understand what operations cause these signals to be produced. This chapter starts with a discussion of the basic design concepts employed by modern keyboards. Next, we analyze the current flow through these devices when various input transitions are made and isolate components where differential power requirements could produce Tempest radiation. After identifying the electromagnetically compromising elements we present one possible solution to equalize current dissipation throughout the design.

3.1 Standard Keyboard Design

While the exact keyboard circuitry varies for different manufacturers, the basic concepts remain the same across most modern devices. Generally, keyboards operate as a layer of *keyswitches* placed over a grid of broken circuits. Depressing a particular keyswitch connects the circuit and generates a signal which is subsequenyly processed by the keyboard controller and communicated via some interface to a system's operating software. Instead of having one signal for each keyswitch, which would require over one hundred keyswitches and therefore over one hundred input pins on the controller, keyswitch sensors are arranged in a grid like pattern. Thus when a particular key is pressed, it simply communicates a row and column number to the controller, requiring far

fewer pins. The concepts of keyswitches, keygrids, and the keyboard controller are shown for a simplified 4x4 keyboard in Figure 3.1. This basic design can easily be expanded to accommodate any arbitrary *N x M* keyboard layout.

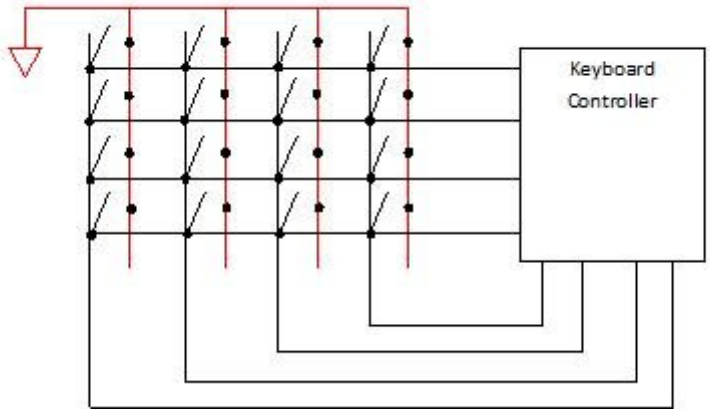

Figure 3.1 - Simple 4x4 Keyboard Diagram

However, this simplified design fails to account for one crucial aspect, which if left unaddressed results in extremely unpredictable transmissions from the keygrid to the keyboard controller. Switch bounce, or contact bounce, is a physical side effect experienced by any mechanical switch. These components are made of spring like materials that are forced into contact by an actuator, in this case a human finger. However, after this transition from open to close and then back to open these switches experience some degree of bounce. Physically, this contact bounce is a function of both the momentum with which the switch is depressed and the elasticity of the metals that make up this circuit component.

In terms of our keyboard design, switch bounce will cause the controller to record several rapid key events for each actual depression of a key. This will obviously need to

be accounted for in order for the perceived input from the user to match the electronic signals interpreted by the keyboard controller. The simplest, and therefore the most widely used approach to "debouncing" is to use a double throw SR Latch (Figure 3.2) to remove the bounce from the signal and then a D Flip-Flop to capture the steady state output. The SR Latch has the property that even if the switch bounces in the neutral region between the two contacts, the output will remain constant because of the feedback loop between the NAND gates.

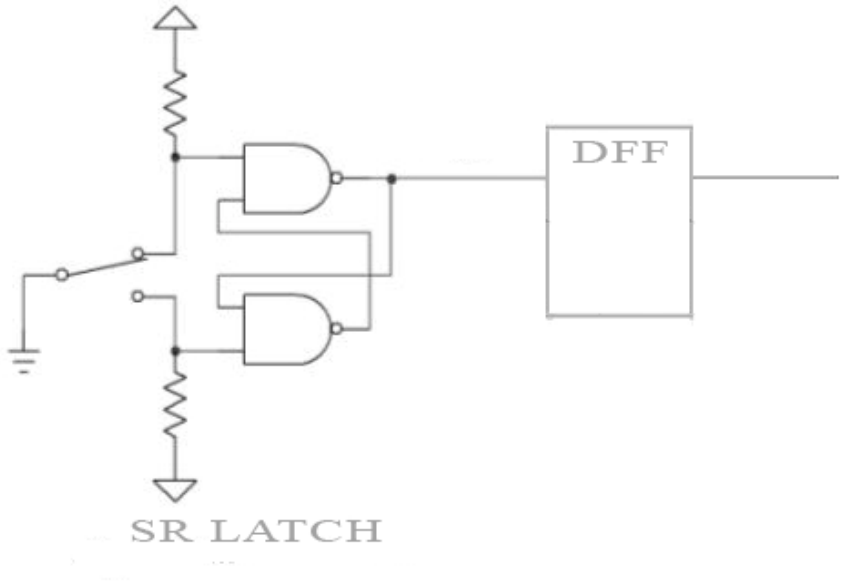

Figure 3.2 - "Debounce" Circuit [26]

In order to prevent multiple instances of a single letter being processed for a single keystroke event these circuits must be placed in between the keyswitches and the keyboard controller for every row and column.

3.2 Analysis of Current Flow within Keyboard Design

In order to isolate parts of this design which generate compromising electromagnetic signals, we must examine how current flows through the various components for different keystroke events. As mentioned, tempest radiation is the result of sudden changes in the overall current needs of a circuit. Thus, any state transition that causes varying numbers of nets to switch will have a distinctive electromagnetic signature.

Surprisingly, the gird of wires and keyswitches is relatively electromagnetically neutral. We can see this by picturing what happens across the grid as a user enters information. Only two lines, one corresponding to the row and the other to the column of the pressed key, are active during any given keystroke[1]. Consequently two nets will begin drawing current while two other will have their power needs drop to zero, resulting in constant current flow over time to this particular component. This is demonstrated by Figures 3.3 and 3.4.

[1] We recognize the possibility that users can hold down two keys simultaneously, such as when entering a capital letter. However, for the purpose of this research we will consider the possibility that an attacker could identify the number of capital letters in a password as minimally important relative to the possibility that an attack could identify an entire password string.

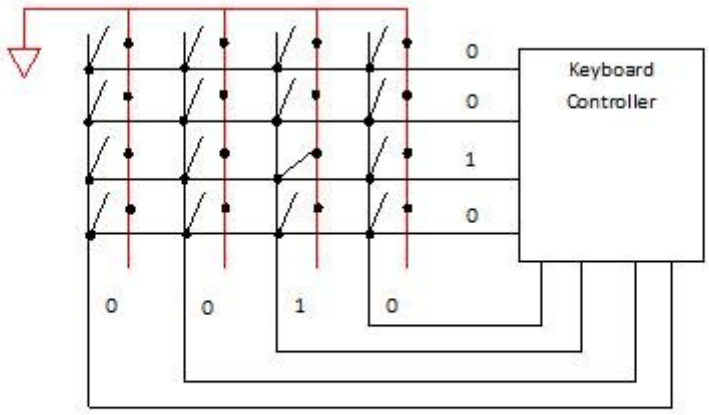

Figure 3.3 - Active Lines with Key 3,3 pressed

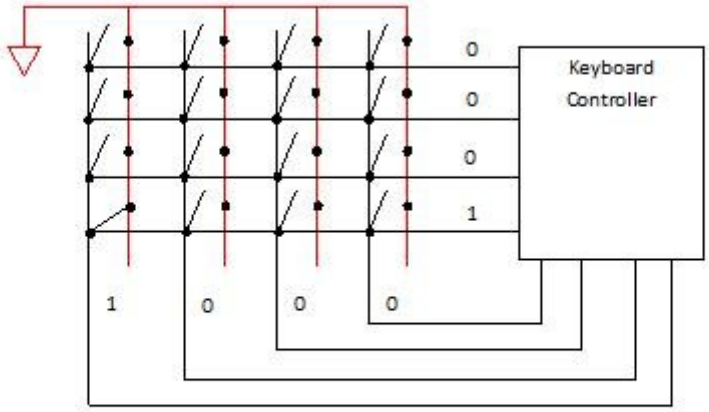

Figure 3.4 - Active Lines with Key 4,1 Pressed

This successfully eliminates the keyswitch grid as the source of the keyboard's electromagnetic emanations. The next component to look at is the debouncing circuitry we discussed earlier. First, we will examine the operation of the SR Latch as its input

changes. This proves relatively easy to do by hand because there is only one input pin and four nets, which for the purposes of this discussion have been numbered in a clockwise order as outlined by Figure 3.5.

We will define the time quanta $t = 0$ as a point in time when the switch is in the up position. At this instant the grounded switch pin establishes connection to one input of the upper NAND gate causing its output to become 1 and the entire netlists state to be (0, 1, 0, 1)[2]. As stated we must examine the effect on consumption as a result of all possible transitions. First we look at the number of net transitions when the switch moves from this initial state to the down position at time $t = 1$. This action causes an input of the lower NAND to become connected to the ground signal forcing Net 3 to transition from 0 to 1, which in turn switches Net 2 to 0 resulting in the stable state configuration of (1, 0, 1, 0) for the switch in the lower position. Lastly, we must examine the internal netlist states as the switch moves from the lower to the higher position. At time $t = 2$ we force the switch to make this state transition and again observe the total net configuration of (0, 1, 0, 1). This entire sequence can be seen in Table 3.1.

[2] (Net 1, Net 2, Net 3, Net 4)

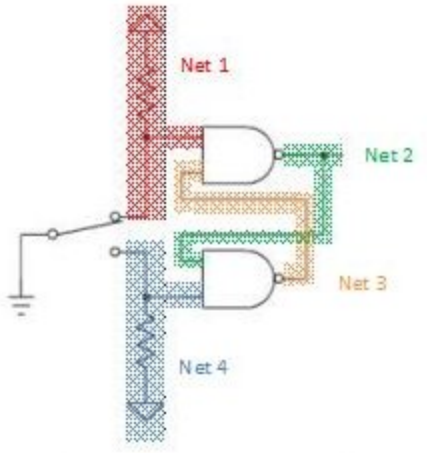

Figure 3.5 - Netlists of SR Latch

Notice that for either the up-to-down or down-to-up transition the total number of nets transitioning from 0 to 1 equals the total number of nets transitions from 1 to 0. Mathematically, this corresponds to the Corrected Hamming distance between any netlist configuration and the configuration of the circuit at the previous time interval being equal to 0. Corrected Hamming distance is a term used throughout this paper to denote a special case of the Hamming distance measurement[3] in which a substitution of two complementary digits cancels out. In the SR Latch example, 1 and 0 are complementary binary units and therefore since each transition requires the substitution of exactly two 1s and two 0s, the Corrected Hamming distance cancels out to 0.

Electronically, we can see then that as the SR Latch operates, the number of switches and therefore the total component current usage is constant and therefore a static amount

[3] A Hamming Distance is the number of positions by which two equal length strings differ. For example HD(1110, 1010) = 1 because the first and second strings only differ in the second digit [25].

of electromagnetic interference is produced. Because the amount of electromagnetic interference produced is unchanging, it cannot be used by an attacker to learn sensitive information about the devices operation. Consequently, the SR Latch component is electromagnetically neutral and not the source of the keyboard's tempest radiation emanations.

Table 3.0.1 - Condition of SR Latch Nets as Component Operates

	Net 1	Net 2	Net 3	Net 4	CHD
t = 0	0	1	0	1	NA
t = 1	1	0	1	0	0
t = 2	0	1	0	1	0

The next component of the keyboard design we need to look at is the D Flip-Flop that registers keystroke information before it is passed to the keyboard controller. Because these components are larger and have multiple inputs, we will not be able to examine them by hand as we did the SR Latch. Instead, we modeled the gate level design of a DFF circuit, which is shown in Figure 3.6, using the hardware description language Verilog[4]. We also created a test bench to transition this design through all possible state changes. For the SR Latch circuit there were only two possible state changes: up to down and down to up. However for a three input DFF circuit there are 64 possible state

[4] IEEE 1364 Standard Verilog code, compiled using Icarus Verilog software on Windows Vista environment

transitions. After each change in input, all nine of the internal nets must be checked and compared to their previous state to compute the current differential associated with that transition.

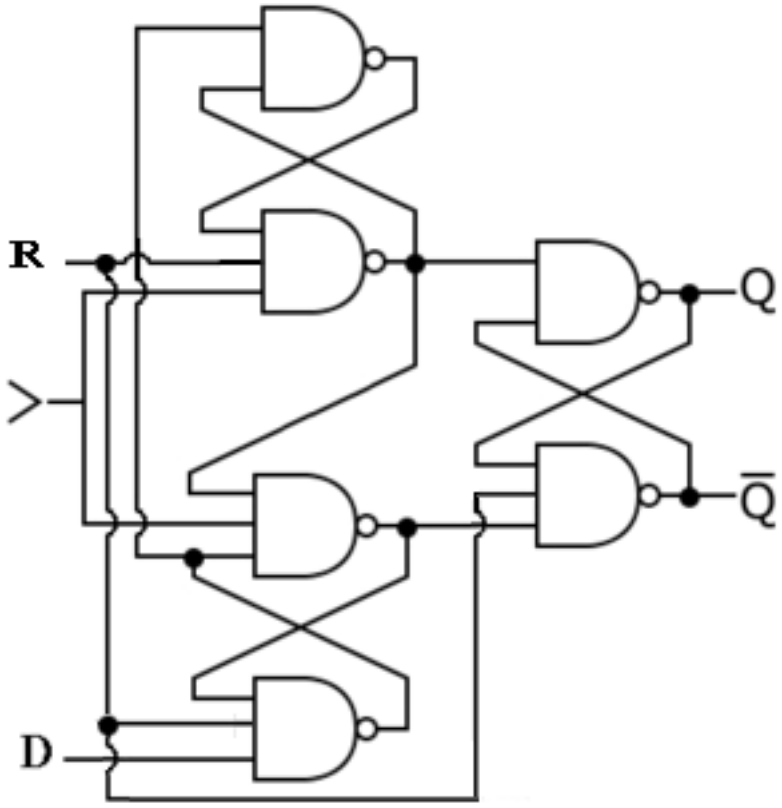

Figure 3.6 - Gate Model of D Flip Flop

By analyzing the results of this test, which are presented in Table 3.2, we can see that the D Flip-Flop circuit is not electromagnetically neutral. As the inputs to the component change, the corrected Hamming distance does not equal 0 and thus the total change in netlist state is not constant, meaning that the circuit draws differential amounts of current and therefore puts off distinct electromagnetic waves. These signals can be recorded and analyzed to determine what transition the device has just performed, which on a keyboard equates to the row and column number of the key that was just entered by the user.

Table 3.0.2 - Hamming Distance Results for DFF Input Transitions

Input	Output	Corrected HD	Input	Output	Corrected HD
001	001011101	NA	111	111101010	2
000	000011101	-1	001	001011101	-1
000	000011101	0	111	111101010	1
001	001011101	1	010	010010101	-2
001	001011101	0	011	011010101	1
010	010010101	-1	010	010010101	-1
010	010010101	0	100	100011101	1
000	000011101	0	010	010010101	-1
010	010010101	0	101	101111001	2
001	001011101	1	010	010010101	-2
011	011010101	0	110	110010101	1
011	011010101	0	010	010010101	-1
000	000011101	-1	111	111010101	2
011	011010101	1	011	011010101	-1
001	001011101	0	100	100011101	0
100	100011101	0	011	011010101	0
100	100011101	0	101	101111001	1
000	000011101	-1	011	011101110	0
100	100011101	1	110	110010101	-1
001	001011101	0	011	011010101	0
101	101111001	1	111	111010101	1
101	101111001	0	100	100011101	-1
000	000011101	-2	101	101111001	1
101	101111001	2	100	100011101	-1
001	001011101	-1	110	110010101	0
110	110010101	0	100	100011101	0
110	110010101	0	111	111101010	1
000	000011101	-1	101	101111010	0
110	110010101	1	110	110010101	-1
001	001011101	0	101	101111001	1
111	111101010	1	111	111101010	0
111	111101010	0	110	110010101	-1
000	000011101	-2	111	111010101	1

3.3 Design of Electromagnetically Neutral Register

Our goal is to design augmentations to the standard D Flip Flop design that cause each of the nine nets in the circuit to be counterbalanced by another net. This means that when a net switches state from 0 to 1, its counter net switches from 1 to 0 and vice versa. Furthermore, when a series of nets is in a steady state or does not change from time $t=x$ to time $t=x+1$ we want its series of counter nets to also stay steady in its inverted state. Lastly, these augmentations should be not affect the overall function of the primary D Flip Flop circuit and should be limited to a minimal amount of complexity so as not to significantly increase the cost of manufacturing the circuit.

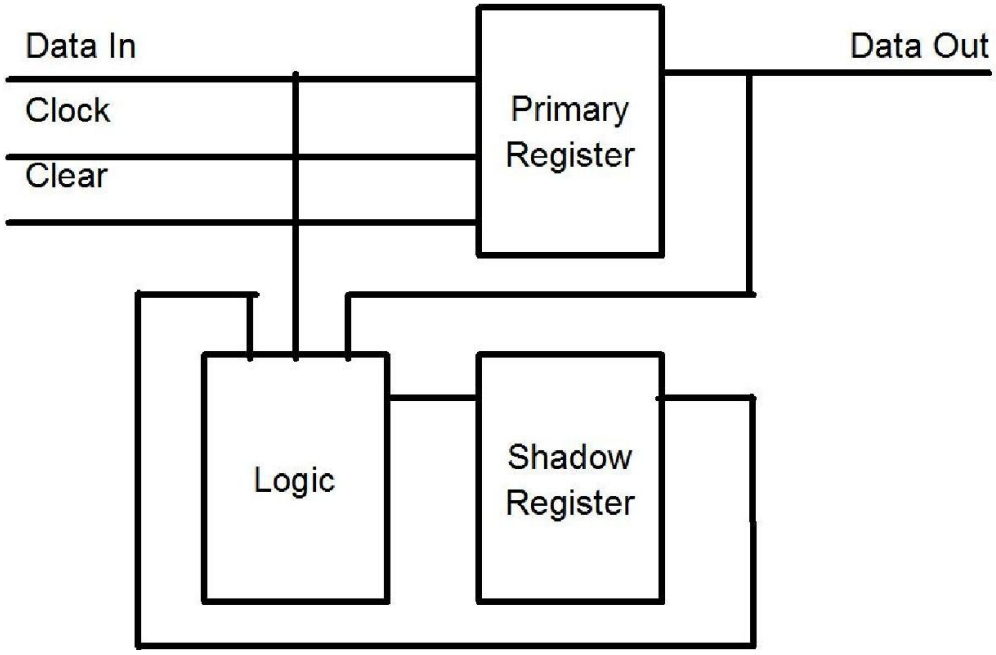

Figure 3.7 - High Level Design of Electromagnetically Neutral Register

An obvious starting point for designing a circuit that meets these criteria is to add a secondary register whose function is directed by some amount of control logic (as shown in Figure 3.7) because we now have two sets of identical netlists whose operation we can

manipulate. However our manipulation of the nets inside the secondary register is still governed by basic Boolean algebra. In order to ensure that we will be able to direct the netlists of this *shadow register* into the exact inverse operations of the primary register we need to closely examine the power consumption affects that different input stimuli had on the flip flop device by groups in search of distinct patterns, which we attempt to demonstrate in Tables 3.3 and 3.4.

Table 3.0.3 - Current Differential Table I

$Input_t$	$Input_{t+1}$							
	000	001	010	011	100	101	110	111
000	0	1	0	1	1	2	1	2
001	-1	0	-1	0	0	1	0	1
010	0	1	0	1	1	2	1	2
011	-1	0	-1	0	0	1	-1	1
100	-1	0	-1	0	0	1	0	1
101	-2	-1	-2	0	-1	0	-1	0
110	-1	0	-1	0	0	1	0	1
111	-2	-1	-2	-1	-1	0	-1	0

While it might not be immediately obvious, this table is almost a perfectly represented symmetrically negated matrix. Because of the manner in which we set up its layout, this distinct pattern provides valuable insight into the input stimuli that will cause the netlists of the shadow register to display the inverse behavior of the primary flip flop. With few exceptions these findings indicate that by inverting the three input stimuli to the

shadow register we should obtain the desired inverse switching behavior in the netlists. The few deviations from this rule correspond to locations where the matrix is not exactly symmetric, such as the transition from 101 to 011 and 100 to 001. However these anomalies should produce far less current differential than the results we saw in Table 3.2. The relationship and its significance are more easily recognized if we color code the Corrected Hamming Distances and black out the identity transition, as shown in Table 3.4.

Table 3.0.4 - Differential Current Table II

$Input_t$	$Input_{t+1}$							
	000	001	010	011	100	101	110	111
000		1		1	1	2	1	2
001	-1		-1			1		1
010		1		1	1	2	1	2
011	-1		-1			1	-1	1
100	-1		-1			1		1
101	-2	-1	-2		-1		-1	
110	-1		-1			1		1
111	-2	-1	-2	-1	-1		-1	

Chapter 4

DESIGN OF AUGMENTED KEYSTROKE DYNAMIC ALGORITHM

Chapter 5 demonstrates that the use of the electromagnetically neutral register has the potential to significantly reduce tempest radiation produced by a keyboard as a result of differential current requirements. While this design makes significant progress in reducing the likelihood that electromagnetic signals could be used to discover a keyboard's textual input, it does not entirely eliminate the possibility of such an attack occurring. Consequently, additional augmentations are needed to further strengthen the user authentication process against electromagnetic side channel attacks on password based systems. This section will describe pressure based additions to standard keystroke dynamics approach that substantially increase the amount of information leveraged by the procedures and thus noticeable increase correctly matched signatures. These algorithmic refinements elevate the accuracy of this behavioral biometric to a degree where it becomes a workable option to harden passwords against sniffing techniques.

4.1 Pressure Based Keystroke Attributes

As discussed, the use of keystroke dynamics has the potential to be an easily deployed and user transparent extension to the traditional login process. One major road block to the application of this technology in the real world has been its well documented struggle to obtain consistently reliable accuracy results. This is largely because standard methods for measuring individuals' typing habits have been primarily based on the

evaluation of only two characteristics per keystroke, namely down time and flight time. To make an analogy to the comparison of handwritten signatures, this approach would be like measuring only the length of and space between each written letter. Not only is this insufficient information to make accurate correlations between handwritten signatures, but these characteristics are the easiest to forge by illegitimate users. Consequently, in traditional handwriting comparison, letter length and letter gap are the least significant contributing factors to the verification or repudiation of two signatures [25]. Unfortunately, the equivalents of these two characteristics are the only measurements available to the vast majority of keystroke dynamics algorithms. The most meaningful characteristics in handwriting analysis are those that relate to curve smoothness and jitter. Obviously, there is no direct correlation between these characteristics and those that can be measured by a keyboard. However, pressure curves, or the exact depression pattern with which a user strikes a key, draw noticeable comparisons with measurements of curve smoothness in the sense that are much more sensitive to finger vibration and extremely difficult to reproduce. We will demonstrate that the addition of this measurement, along with normalized maximum pressure, significantly increases the accuracy of a keystroke dynamic algorithm to the point where it is a viable approach to strengthening password based log in systems against electromagnetic side channel attacks.

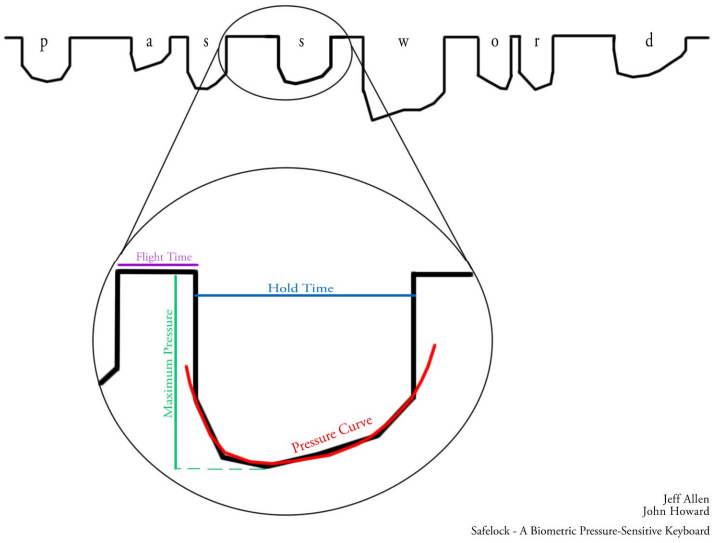

Figure 4.1 - Visual Description of Keystroke Measurements

Figure 3.7 attempts to visually describe the four attributes that our keystroke dynamic algorithm will take into affect. This diagram also shows a variety of pressure curves observed for a sample user typing the word “password”. As we can, see the nature and shape of these curves vary greatly depending on the users exact finger movement as they type a given word. Furthermore, because they are intricately tied to reflex mussel coordination that is ingrained through the process of repetition in a user’s typing habits, they are exponentially harder for illegitimate users to reproduce than characteristics such as down and flight time.

There are two distinct aspects of any keystroke dynamics algorithm: signature construction and signature scoring. Signature construction is the process of observing a user’s typing patterns and then employing that information to generate what we will refer

to as a *legitimate keystroke template*[5]. Signature scoring is umbrella term for the algorithms we use to compare any other *claimant keystroke template* to a user's legitimate template with the ultimate goal of confirming or repudiating identity. For the purpose of this research we will define a *keystroke signature* as the set individual *letter signatures* for a typed log in credential. Presumably, this credential is a standard textual password however, as demonstrated by [2], these same concepts can be applied to other frequently typed words such as first and last name. Letter signatures contain the measurements of flight time[6], down time, maximum pressure, and a pressure curve for an individual key depression.

4.2 Signature Construction

Figure 3.7 is a visual representation of a keystroke signature but for comparison purposes these attributes must be described mathematically. Down time, flight time, and maximum pressure are fairly straightforward to model numerically. When constructing or updating a legitimate keystroke template, the mean, and standard deviation are maintained for each of these three features. This will allows us to calculate both the expected value for any of these characteristics as well as a measure of variability demonstrated by a particular user in the past. Furthermore, in order to be able to update these numbers a vector consisting of the most recent one hundred valid measurements for

---

[5] The words "keystroke signature" and "keystroke template" are used interchangeable throughout this paper

[6] Note that in this algorithm flight time was arbitrarily selected as the time preceding the first instance of measured pressure.

each characteristic is maintained. When constructing a claimant signature there are no mean values or standard deviations because the sample size is 1. Consequently, we only need to record the actual observed flight time, down time, pressure, and pressure curve for each letter typed.

Storing the pressure curve entry in each letter signature is slightly different than the method presented above for the obvious reason that curves must be modeled as lines while the other measurements can be represented as simple points. The curves must be constructed from the information as it is received by the keyboard which in its initial form is a vector of pressures. The particular keyboard used in our research pulses the operating system at a frequency of approximately 100 Hz. Thus the pressure measurements we received from the keyboard were spaced out evenly by about ten milliseconds. Using this information we can fit a curve to the resulting plot of the data in the *xy* plane. We attempted to model all pressure curves as third degree polynomials to better represent scenarios where the either the depression or the release of the key came very quickly while the opposite action came more gradually, such as that seen in the "**a**" and "**o**" characters in Figure 3.7[7]. By using this method we were able to store the relevant information about the shape of these curves by maintaining only the mean and standard deviation for *a, b, c*, and *d* of the equation:

$$ax^3 + bx^2 + cx + d$$

[7] For a moderate number of curves this degree of accuracy was not needed and the coefficient corresponding to the x^3 term was effectively ignored.

In order to update the standard deviation we also maintained a vector of these coefficients in the twenty five most recently observed pressures curve as well.

4.3 Entry Scoring

Entry scoring is the next crucial aspect of a keystroke dynamic algorithm. The goal of our scoring algorithm is to calculate a difference measurement between the features of a claimant template and a legitimate user template that varies directly with claimant distance from the mean but indirectly with the standard deviation. In this manner the difference measurement will increase as the distance from the mean grows but not penalize user's who have a high degree of variability associated with a given feature. Much like the methods we used to create the keystroke signatures, this difference measurement must be calculated differently for the point like characteristics of flight time, down time, and maximum pressure and the line like characteristics of the pressure curve measurement. Originally, our research efforts attempted to calculate the difference measurement for the point-like characteristics (Δp_i) as a function of the legitimate template mean (μ_i) and standard deviation (σ_i) and the claimant sample (z) using the formula:

$$\Delta p_i = \frac{|\mu_i - z|}{\sigma_i}$$

The individual difference measurements for flight time, down time, and maximum pressure ($i = 0$, 1, and 2, respectively) are then added together and combined with the difference measure of the pressure curve, which is discussed momentarily. However, this approach neglects to place an upper bound on the affect that any one particular point-like

feature can have on the overall penalty applied to a letter signature. Furthermore, we want the difference measurement to reach this bounded maximum only when the observed sample z reaches some number of standard deviations away from the legitimate template mean μ_i. Through our research we found this optimal number of standard deviations to be three, changing the formula for the difference measurement of point-like characteristics to:

$$\Delta p_i = \min\left\{\frac{1}{3}\cdot\frac{|\mu_i - z|}{\sigma_i}, 1.0\right\}$$

The next step in the entry scoring process was to establish a method for calculating a difference score between the claimant and legitimate users pressure curve characteristics. As we stated, the process for evaluating the similarity of these measurements is different because they are modeled as a line while the other three keystroke characteristics can be represented as points. The most obvious approach is to simply calculate area between the legitimate template pressure curve ($l(t)$) where the domain is given by $D(l(t)) = n$ and the claimant template pressure curve ($z(t)$) where the domain is given by $D(z(t)) = m$ normalized by some factor (η) which is given by the equation:

$$\Delta c = \frac{1}{\eta}\left|\int_0^n l(t)dt - \int_0^m z(t)dt\right|$$

This approach yields interesting questions related to the calculation of a difference measurement on line-like objects. Firstly, we must address the situation where the domain of the two curves is not equivalent ($n \neq m$). Visually we can think of this as a scenario in which one pressure curve has more points than the other and thus is longer in

the *t* dimension. The interesting and at first counter-intuitive point here is that even though this situation obviously increases the amount of difference between two curves, we do not want to increase the pressure curve difference measurement. At this point in the algorithm's development we have not attempted to apply any weight to dictate which features contribute most significantly to the final claimant difference measurement. While these weights will eventually become an important aspect in optimizing the entry scoring process, we want to maintain the ability to easily and transparently modify the weights to fit the particular circumstances of the algorithm's operation. By penalizing the curve for being of differential length in the *t* dimension we are implicitly adding additional weight to the down time measurement, which is the characteristic specifically designed to estimate dissimilarity in the domain of each letter signature's depression time. Consequently, when faced with two curves of differing domains, we must horizontally stretch the curve associated with the smaller domain without penalty. We know that the pressure felt on any key must be 0 and both time $t=0$ and the final observed time $t=t_n$. Mathematically this means that any pressure curve is "anchored" at the points (0, 0) and (t_n, 0). Knowing this fact allows us to apply a simple geometric stretch to either the function $l(t)$ or $z(t)$ depending on which has the smaller domain. Mathematically, we can express this as:

$$l'(t) = \begin{cases} l(t), D(l(t)) \geq D(z(t)) \\ l(\frac{D(l(t))}{D(z(t))} \cdot t), D(l(t)) < D(z(t)) \end{cases}$$

$$z'(t) = \begin{cases} z(\frac{D(z(t))}{D(l(t))} \cdot t), D(z(t)) < D(l(t)) \\ z(t), D(z(t)) \geq D(l(t)) \end{cases}$$

The result of this function can be seen in Figures 4.2 and 4.3 on two pressures curves obtained during testing and modeled in graphical software. Figure 4.2 shows a legitimate user's pressure curve ($l(t)$) for some letter in red and a claimant pressure curve ($z(t)$) for the same letter in green. We can visually inspect the domains and determine that $D(l(t)) \approx 55$ and $D(z(t)) \approx 30$. Therefore according to the above equation $l'(t) = l(t)$, meaning the legitimate user pressure curve has the greater domain larger and therefore stays the same. The claimant pressure curve however needs to be stretched horizontally, given mathematically by $z'(t) = z(\frac{30}{55}t) \approx z(.54t)$. The result of this stretch can be seen in Figure 4.3.

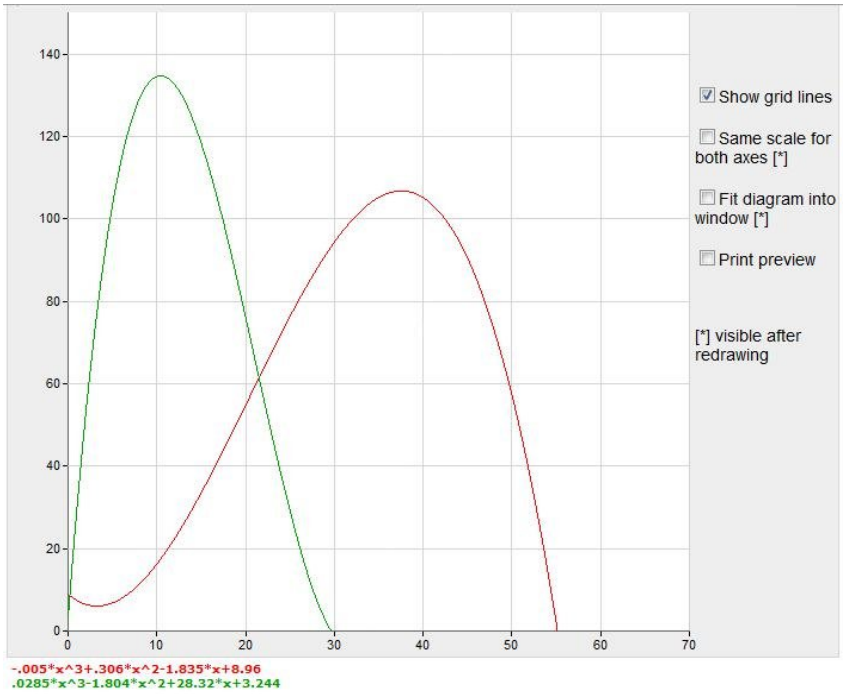

Figure 4.2 - Non Equalized Claimant and Legitimate User Pressure Curves

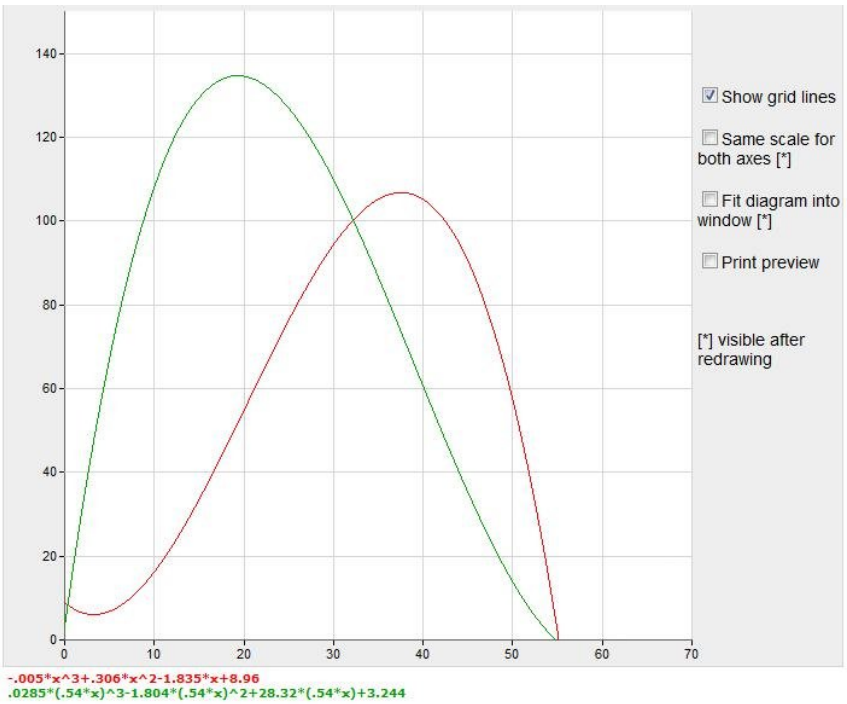

Figure 4.3 - Equalized Claimant and Legitimate User Pressure Curves

The next interesting problem brought up by the application of the difference measure to line-like objects is the question of what to normalize the difference by. Originally, our approach was to normalize the area difference by the total area under the legitimate user curve. However, we found that using this method made it easier for a user to get good pressure curve difference scores against legitimate users who had letter signatures with high maximum pressures. This interdependence between maximum pressure and pressure curve score again violates the idea that at this point in the algorithm all features are weighed as autonomous and equal. Instead we concluded that the difference measurements for two curve-like models should be proportional to those model's R^2 values, which mathematically can be related to a measure of unexplained variance between the two datasets. Again, we also want to limit the total negative affect that this

particular characteristic's difference measurement can have on the entire letter signature difference score. This resulted in the difference equation for pressure curves being established as:

$$\Delta c = \min\left\{\frac{\left|\int_0^n l'(t)dt - \int_0^n z'(t)dt\right|}{R^2(l'(t), z'(t))}, 1.0\right\}$$

Resulting in the total difference measurement for a given letter signature Δd_k where each w_i is the eight applied to i^{th} characteristic being:

$$\Delta d_k = \sum_{i=0}^{3} w_i \min\left\{\frac{1}{3}\cdot\frac{|\mu_i - z|}{\sigma_i}, 1.0\right\} + w_4 \min\left\{\frac{\left|\int_0^n l'(t)dt - \int_0^n z'(t)dt\right|}{R^2(l'(t), z'(t))}, 1.0\right\}$$

And the net difference measurement for an entire keystroke signature Δf with j letter signatures:

$$\Delta f = \frac{\sum_{k=0}^{j} \Delta d_k}{j}$$

Chapter 5

RESULTS

This section discusses the results obtained by this research. First, the switching reduction observed when employing the electromagnetic register design is discussed. Secondly, the accuracies associated with a brief human trial of the modified keystroke dynamic algorithm are presented.

5.1 Results for Electromagnetically Neutral Register

Table 4.1 outlines the results obtained when the Corrected Hamming distances are calculated for the electromagnetically neutral register as described in Section 3.3. As we can see all but four input transitions cause the number of nets switching from 0 to 1 to be exactly equal to the number of nets switching from 1 to 0. Furthermore, these anomalies were the transitions predicted by the matrix represented by Table 3.4. Consequently this design as a whole draws a nearly constant amount of current regardless of the operation of the register. Because there are no sudden spikes in current flow, significantly less electromagnetic interference is produced by the device.

Table 5.0.1 - Switching Results from Electromagnetically Neutral Register

Input	Output	Corrected HD	Input	Output	Corrected HD
001	001011101	NA	111	111101010	0
000	000011101	0	001	001011101	0
000	000011101	0	111	111101010	0
001	001011101	0	010	010010101	0
001	001011101	0	011	011010101	0
010	010010101	0	010	010010101	0
010	010010101	0	100	100011101	1
000	000011101	0	010	010010101	-1
010	010010101	0	101	101111001	0
001	001011101	0	010	010010101	0
011	011010101	0	110	110010101	0
011	011010101	0	010	010010101	0
000	000011101	0	111	111010101	0
011	011010101	0	011	011010101	0
001	001011101	0	100	100011101	0
100	100011101	0	011	011010101	0
100	100011101	0	101	101111001	0
000	000011101	0	011	011101110	1
100	100011101	0	110	110010101	-1
001	001011101	0	011	011010101	0
101	101111001	0	111	111010101	0
101	101111001	0	100	100011101	0
000	000011101	0	101	101111001	0
101	101111001	0	100	100011101	0
001	001011101	0	110	110010101	0
110	110010101	0	100	100011101	0
110	110010101	0	111	111101010	0
000	000011101	0	101	101111010	0
110	110010101	0	110	110010101	0
001	001011101	0	101	101111001	0
111	111101010	0	111	111101010	0
111	111101010	0	110	110010101	0
000	000011101	0	111	111010101	0

5.2 Results for Augmented Keystroke Dynamic Algorithm

In order the gauge the results of our approach to keystroke dynamics we need to evaluate how often a User A is prevented from logging into their account on the first attempt and how often User B, who happens to know User A's password, is able successfully imitate User A's typing habits and gain access to his/her account. The former case is an example of Type II or false negative error and the later is an example of a Type I or false positive error. Obviously, errors of the second type are much less severe because they only constitute the simple inconvenience of forcing the user to type their password again, while Type I Errors correspond to a much more serious unauthorized account access.

Our experiment involved asking 35 computer science students to attempt to gain access to a theoretical bank account. Two passwords were generated by the research team, one having complicated letter signatures and the other having a relatively simple pattern. Each student was then told the password for the complex system and given five chances to attempt to enter the system. This was then repeated on the system protected by the simple password. Following this test we allowed each student to see the visual password signature (much like the one in Figure 3.7) and explained how the keystroke dynamic algorithm worked and why it was preventing them from successfully accessing the account. Furthermore, the researcher who generated the password successfully logged into the system three times while the test subject watched, allowing them to visually measure how typing habits were translated into the signatures they were observing. Each student was then given five more attempts on both the complex and

simple system where after each try they could see an overlaid model of their most recent typing signature and the legitimate user signature for the account password.

This test allowed us to obtain false acceptance information for two sets of types of individuals; a naïve participant and a well informed user, as well as false rejection information for participating researchers. Furthermore, we were able to observe how the algorithm performed on both a simple and complex keystroke signature. Finally, by recording and applying this data to the entry scoring algorithm using a variety of different weights for the various characteristics we were able to determine the optimal amount of influence each measurement had on the overall keystroke template difference score. These weights are outlined in Table 4.2.

Table 5.0.2 - Optimal Weighting for Entry Scoring Function

Characteristic	**Optimal Weighing**
Down Time	.3
Flight Time	.25
Maximum Pressure	.25
Pressure Curve	.2

The first result we obtained was that there was no noticeable difference between the naïve and well informed participant entry scores. However, this was largely a psychological experiment and not directly related to the accuracy of the routine. We did observe a significant statistical difference in the performance of the keystroke dynamic routine when it operated on complex and simple passwords. Figure 5.1 demonstrates this

point by showing the receiver operating characteristic (ROC) curve for the two types of passwords using optimal weighing characteristics. The area under the curve for the complex password was .997 for the complex password while the area under the curve for the simple password was only .952.

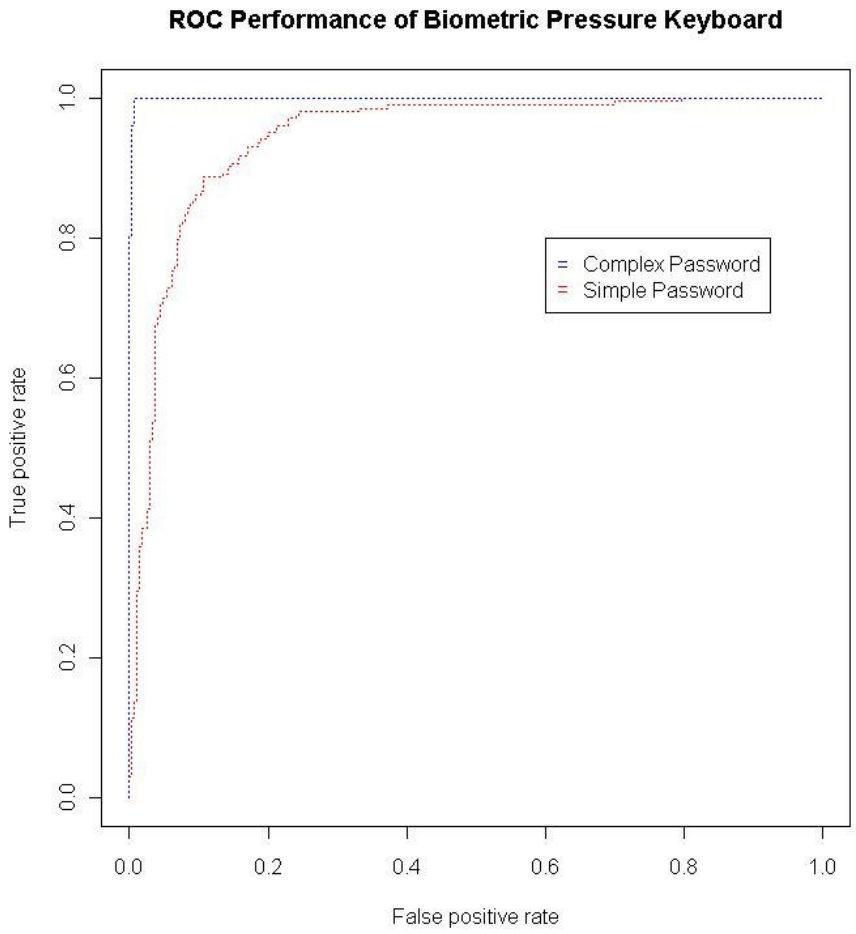

Figure 5.1 - Receiver Operating Characteristic Curve for Simple and Complex Password

Determining an exact False Rejection and False Acceptance rate is an arbitrary matter because it depends on our selection of a threshold. In physiological biometrics the threshold is usually selected as the point where no False Acceptance errors occurred.

However, behavioral outliers are far more common than physiological ones and consequently this branch of biometrics usually allows for some percentage of False Acceptance error. For purely summarization purposes Table 4.1 shows the False Acceptance and False Rejection rates for thresholds similar to those used by [18].

Table 5.3 - Comparison of False Acceptance and Rejection Rates

	False Acceptance Rate	**False Rejection Rate**
Complex Password	0.6%	3.9%
Simple Password	2.6%	23.0%

Chapter 6

CONCLUSIONS AND FUTURE RESEARCH

6.1 Conclusions

While the possibility of retrieving sensitive information by analyzing the electromagnetic waves produced by a device has been known for decades, Vaugnoux and Pasini's recent study [21] place renewed emphasis on the development of methods to counter this security concern. We have quantitatively shown that the deployment of electromagnetically neutral registers greatly reduces the amount of circuit switching and therefore produced electromagnetic interference generated by the standard keyboard design, making it significantly harder for an attacker to isolate these signals. Furthermore, we have discussed how the real world deployment of keystroke dynamic algorithms can offer security against this type of attack and outlined a novel augmentation to these types of algorithms that increases their accuracy. We believe the deployment of these two countermeasures significantly reduces the likelihood of password sniffing via an electromagnetic side channel attack. Additionally, these techniques can easily be incorporated into future systems for a minimal cost yet offer a relatively substantial degree of protection.

6.2 Future Research in the Field of Electromagnetic Neutrality

While the design implemented by this research appreciably reduces the amount of electromagnetic interference produced by a keyboard, additional research into signal balancing could further these results. The keyboard controller is one element of a

standard keyboard's design we did not examine. This is largely due to the fact that electromagnetic properties are dictated by a component's gate level model, which for the keyboard controller would vary depending on manufacturer, synthesis techniques, and the type of system interface a particular keyboard is using. Also, additional research is required address security concerns associated with wireless keyboards. This research focused on limited the amount of electromagnetic interference that was inadvertently generated as a result of differential current flow within a device. However, the signals produced by wireless keyboard are another example of electromagnetic waves (although purposely generated in this case) and therefore could contain sensitive information.

6.3 Future Research in Keystroke Dynamics

The most pressing need for the keystroke dynamics field at this point is a standard database of keystroke information that could be used to compare various algorithms. Presently, each individual researcher who has developed some algorithm has done their own independent subject tests in an attempt to determine how their accuracy compares to other published findings. However, unless other known algorithms are run on the same set of data these accuracy comparisons will never truly measure what methods and augmentations produce the best results. Furthermore, having a standard database of keystroke dynamics routines relieves the research team of any burden associated with IRBs or other human subject testing issues. In terms of algorithmic development, additional work could be done to increase the frequency with which the keyboard communicated to the operating system, thus increasing the amount of pressure information we have to model the pressure curves on. This would likely led to increased

accuracy in the pressure curve difference measurement and possibly allow the curves to be modeled as higher degree polynomials. Furthermore, the idea of pressure curves could be expanded in a trigraph type fashion much like measurements of down time were in the late 1980s. This would facilitate research into notions that pressure curves vary depending on the preceding and following keys pressed in a sequence, which could increase the accuracy of keystroke dynamic algorithms.

REFERENCES

[1] J. R. Young, and R.W. Hammon, Method and Apparatus for Verifying an Individual's Identity. U.S. Patent 4,805.222, filed December 25th, 1985, and issued February 14th, 1989.

[2] R. Joyce and G. Gupta, Identity Based Authentication Based on Keystroke Latencies, *Communications of the ACM*, Volume 33 Number 2, February 1990, pp. 33- 42.

[3] F. Bergadano, D. Gunetti, and C. Picardi, User Authentication through Keystroke Dynamics, *ACM Transactions on Information and Security Systems*, Volume 5, Number 4, November 2002, pp. 367-397.

[4] J. Garcia, Personal Identification Apparatus, U.S. Patent 4,621,334, filed August 26th 1983, and issued November 4th 1986.

[5] M. Brown and S Rogers, Method and Apparatus for Verification of a Computer User's Identification Based on Keystroke Characteristics, U.S. Patent 5,557,686, filed January 13th 1993, and issued September 17th, 1996.

[6] D. Agrawal, B. Archambeault, J. Rao and P. Rohatgi, The EM Side Channels, Cryptographic Hardware and Embedded Systems 2002, pp. 29 – 45.

[7] S. Chari, C. Jutla, J. Rao, P. Rohatgi, Toward Sound Approaches to Counteract Power-Analysis Attacks, Proceedings on Advances in Cryptology 1999, pp. 398 – 412.

[8] P. Kocher, J. Jaffe and B. Jun. Differential Power Analysis: Leaking Secrets, *Proceedings of CYPTO 99*, pp.388-397.

[9] M. Orceyre and R. Courtney Jr., Considerations in the Selection of Security Measures for Automatic Data Processing Systems, *NBS Special Publication*, June 1978, pp. 500-533.

[10] A. Jain, L. Hong and S. Pankanti, Biometric Identification, *Communications of the ACM*, Volume 43, Issue 2, February 2000, pp. 90-98.

[11] F. Monrose and A. Rubin, Keystroke Dynamics as a Biometric for Authentication, *Future Generation Computer Systems 16*, 2000, pp. 351-359

[12] R. Gaines, W. Lisowski, S. Press and N. Shapiro. The keystroke Level Model for User Performance Time with Interactive Systems. *Communications of the ACM*, Volume 23, Issue 7, 1980, pp. 396 – 409

[13] J. Leggett and G Williams, Verifying Identity via Keyboard Characteristics, *The International Journal of Man-Machine Studies,* Volume 23, Issue 1, January 1988, pp. 67-76.

[14] J. Leggett, G Williams and D. Umphress, Verification of User Identity via Keyboard Characteristics, *Human Factors in Management Information Systems*, Ablex Publishing, Norwood, NJ.

[15] D. Umphress and G. Williams, Identity Verification through Keyboard Characteristics, *International Journal of Man-Machine Studies*, Volume 23, Issue 3, September 1985, pp. 263-273.

[16] M. Brown and S. Rogers, User Identification via Keystroke Characteristics of Typed Names using Neural Networks, *International Journal of Man-Machine Studies,* Volume 39, Issue 6, 1993, pp. 999-1014.

[17] D. Mahar, R. Napier, M. Wagner, W. Laverty, R. Henderson and M. Hiron, Optimizing Digraph Latency Based Biometric Typist Verification Systems: Inter and Intra Typist Differences in Digraph Latency Distributions, *International Journal of Human-Computer Studies* Volume 43, Issue 4, 1995, pp. 579 – 592

[18] H.R. Lv and W.Y. Wang, Biological Verification Based on Pressure Sensor Keyboards and Classifer Fusion Techniques, *IEEE Transactions on Consumer Electronics*¸ Volume 53, Issue 3, pp. 1057 – 1063.

[19] W. Peter, SpyCatcher – The Candid Autobiography of a Senior Intelligence Officer. William Heinemann Publishing, Australia, 1987.

[20] Electromagnetic Pulse (EMP) and Tempest Protection for Facilities, Engineering Pamphlet EP 1110-3-2, U.S. Army Corp of Engineers Publications Depot, Hyattsville, December 1990

[21] M. Vuagnoux and S. Pasini, Compromising Emanations of Wired and Wireless Keyboards, *18th USENIX Security Symposium*, August 2009.

[22] M. Kuhn, Compromising emanations: Eavesdropping Risks of Computer Displays, University of Cambridge Computer Laboratory, Cambridge, December 2003.

[23] V. Nalwa, Method for Detecting Forgery in a Traced Signature by Measuring an Amount of Jitter, U.S. Patient 5745592, filed July 27 1995 and issued April 28 1998.

[24] W. Hamming, Error Detection and Error Correcting Codes, *Bell Systems Technical Journal*, Volume 26, Issue 2, 1950, pp. 147 – 160.

[25] J Allen and J Howard, Design and Implementation of Novel Concepts in Behavioral Biometric Identification, Society for Design and Process Science 2010 Symposium.

[26] U.S. Department of Justice, Federal Bureau of Investigates, Process of Handwriting Comparison, *FBI Law Enforcement Bulletin*, Volume 48, Issue 10, October 1979.

[27] The Ganssle Group, A Guide to Debouncing, accessed March 2010, written June 2008, http://www.ganssle.com/debouncing.pdf.