USER SPECIFIC FIREARM LOCKING SYSTEM

Andrew Weller
Yong Seok Lee
Steven Bettenhausen

ECE 445, Senior Design -
University of Illinois at Urbana-Champaign
10 May 2012

1. Introduction:

The objective of this project is to increase firearm safety by creating a simple and portable system that allows only authorized personnel to operate a firearm. This system is not intended to stop the theft of firearms; rather, it helps prevent the accidental firing of the weapon. While locked, the firearm's trigger cannot be pulled and its magazine cannot be removed.

The system consists of two main components: the control unit, a user-interfacing subsystem separate from the firearm, and the firearm unit, a subsystem attached to the firearm that physically puts the weapon into the desired lock or unlock state. Persons attempting to operate the firearm must first scan their fingerprint on the control unit; a successful scan allows the user to unlock the firearm for a user-selected duration. The unlock signal is then transmitted wirelessly to the firearm unit which places the weapon into the proper state.

2. Features and General Design:

1. User specific unlock authorization
    - Fingerprint scanner to identify
    - Multiple fingerprint storage
2. Simple user interface
    - LCD display for status and messages
    - Keypad for user input
3. Low impact on gun use once unlocked
    - Separate components into firearm unit and control unit.
    - Wireless communication between units
4. Automated Locking and Unlocking
    - Motor control of mechanical locks
    - State signal control
5. Pressure and timed unlock options
    - Pressure sensor for in use lock override
    - Timer for user defined unlock duration
6. Portability
    - Battery powered
    - Voltage regulation circuitry

3. Design:

3.1 Fingerprint Scanner

The fingerprint scanner's complex function, to scan and store fingerprint data, led to the decision to purchase a premade component. An optical scanner was chosen because they are easier to use and have fewer problems than slide scanners. The selected scanner, NITGEN FIM5360, comes with its own microcontroller which allows the comparing of fingerprint data to be done on the scanner unit. Another feature of this scanner is the internal memory and the ability to output a unique identification number serially for each fingerprint [1].

The serial communication for the fingerprint scanner was not as straight forward as one would first think. Because the PIC only had one set of serial UART ports, both the fingerprint scanner and the transmitter needed to be on the same port. The designed answer to this problem was to use two OR gates to effectively choose which peripheral, the fingerprint scanner or the transmitter, was communicating with the microcontroller. This method of serial communication followed the IEEE Standard488.1-1987, which explained the importance of the three fundamental elements of an effective communication link, "1) A device acting as a listener, 2) A device acting as a talker, 3) A device acting as a controller" [2]. In the planned design, the listener would be the fingerprint scanner and the transmitter both, and the OR gates in conjunction with signals from the microprocessormake up the controller device that controls which device the signals are routed to. Finally, the talker device would be the microcontroller. Although this was the initial design, it was found that using GPIO communication with the fingerprint scanner was better suited for this specific application. Serial communication was still used for the transmitter with the described design in place. This serial communication with the transmitter followed the IEEE standard and was successful as seen in the section explaining the transmitter.

Even though serial communication was not used, the network still contains the three fundamental elements of an effective communication link. The first three GPIO ports, Identify, Register, and Delete, are input to the scanner with the microcontroller acting as the talker and the scanner being the listener. The last two ports, Pass and Fail, are output to the microcontroller with the microcontroller acting as the listener and the scanner being the talker. Finally, the microcontroller was used as a controller by developing and integrating code into the user menu that brings the three input I/O lines from high to low to activate the various commands.

The Identify function compares the user's fingerprint to the database of fingerprints already in the system and drives the Pass output low if the fingerprint is in the system or it drives the Fail output low if the fingerprint is not in the system. The Register function compares the user's fingerprint to the database of fingerprints already in the system and drives the Pass output low if the fingerprint is not in the system or it drives the Fail output low if the fingerprint is already in the system. Fingerprints that are not already stored in memory are added to the memory. The Delete function compares the user's fingerprint to the database of fingerprints already in the system and drives the Pass output low if the fingerprint is in the system or it drives the Fail output low if the fingerprint is not in the system. Fingerprints stored in the system's memory are removed.

3.2 User Interface

The user interface was designed to create a way for the firearm's operator to easily manage user fingerprints and unlock and lock the firearm. The interfacing is done via a LCD display that prompts the user and a keypad that allows the user to respond to these prompts.

The chosen LCD display is a 16 character by 2 line display with a HD44780 Hitachi controller [3]. Utilizing the capability to display 32 characters at a time allows the created prompts to be detailed. The character data for these prompts is sent on data lines, 4 bits at a time, from the control unit's microcontroller. A prewritten code [4], [5] is used to display the proper characters on the LCD display. For proper communication with the microcontroller, the register select (RS), read/write enable (E), and read/write select (R/W) pins are connected to the microcontroller's I/O ports.

The keypad chosen is a 16 key conductive rubber keypad [6]. This particular keypad was selected because its keys consist of the numbers 0-9, the letters A-D, the '#' key, and the '*' key. Having many keys allows each one to have its own specific function in the menus. Communicating the user inputs to the microcontroller is done by connecting the keypad's outputs to eight I/O pins on the microcontroller. Since the keypad behaves as a switch matrix, its pins had to be probed systematically to determine which key was being pressed. An algorithm was created and called by the read_keypad() function which returns a number between 0 and 16.

As with the fingerprint scanner, IEEE standard 488.1 was applied. This process is done through the "talking" and "listening" of the microcontroller and keypad. The microcontroller begins this process by sending high voltages to the first four keypad pins and reading the value of the other four pins. When the microcontroller reads a high voltage on one of these pins, a key is pressed and the algorithm controlled by the microcontroller switches off power to the first four pins one by one until the input to the keypad is no longer high. At this point, the key that was pressed is identified and its value is returned to the main function.

The user menu is designed using a case statement so that the navigation within the program is simple and efficient. The acceptable keys are listed at each prompt along with the corresponding result of each key press. Only acceptable key presses allow the user to navigate through the menus, all other key presses are ignored. To make traversing the menu easier on the user, only two main tracks were created. In the fingerprint management track, the user is able to add or delete acceptable user fingerprints while the locking and unlocking track allows the user to input the duration of the unlocked state or override the unlock state to lock the firearm. While moving through the user menu, appropriate messages such as "scan successful" or "unlocking for 100 seconds", are displayed on the LCD display for two seconds to give the user status updates. While these messages are displayed, no user inputs are accepted.

3.3 Power Supplies

The various components in the control and firearm unit all required +5V dc or +3.3V dc power to run. The power supplies needed a way to regulate the voltage sent to these components. This was done via a voltage regulator with a +5V output. Supplied by the 9-volt battery, the regulator lowers to voltage to +5V which is sent to the microcontroller and other components, except the fingerprint scanner, ensuring they always have the correct voltage to operate. For proper operation of the voltage regulator component, capacitors and resistors are attached to its input and output. The values of these components were selected because they were used in a similar voltage regulator circuit [9].

Also for the control unit, a second voltage regulation circuit was required to pull the voltage down to +3.3V for the fingerprint scanner.

3.4 Wireless Communication

The communication between the control unit and firearm unit was chosen to be done wirelessly. This would allow the firearm to be separate from the control unit, making the firearm unit small and unobtrusive while still allowing for the interactive user interface and fingerprint scanner to be used. The wireless communication was done using Linx HP3 series receivers and transmitters because they are easily configured to communicate with the PIC microcontroller [7], [10]. Another benefit of these components is the 902 MHz to 927 MHz RF frequency range over which they can communicate [11]. To transmit the signals 916 MHz Linx antennas were chosen. For proper communication with the antennas, the transmitter and receiver were set to an operating frequency of 916 MHz, the closest channel that is able to be set with parallel ports to the antennas' center frequency. This was done by configuring the I/O ports CS0, CS1, and CS2 on the transmitter and receiver to the operating frequency.

The next step was to set up the RS-232 serial communication between the transmitter and receiver via the putc function in a prewritten piece of code [4], [5]. The wireless communication set-up follows the IEEE Standard Serial Interface for Programmable Instrumentation, Section 4.6 Signaling [12]. This section describes how serial interface signaling is handled. Transferring data "On circuits TXD and RXD" was done by connecting the TX UART port on the control unit microcontroller to the input data pin of the transmitter and then connecting the output data pin of the receiver to the RX UART port on the firearm unit microcontroller. The standard also states that "Data shall consist of characters sent using a start/stop data transmission system. Each character shall contain exactly 8 bits preceded by a start bit, space (0), and followed by a stop bit, mark (1), to create a frame", which can be seen in Figure 2. The baud rate of 9600 that was used was acceptable since "… the transmit and receive bit rates [are] the same".When testing this communication, there were initial troubles until it was realized that the clocking was different in the two microcontrollers controlling the transmitter and the receiver. Since the clocking rate directly affected the baud rate, the serial communication was being attempted with different baud rates. This was in direct opposition to the IEEE Standard and failed. When the problem was discovered and the clocks and baud rates were synched, the communication and the device ran as smoothly as designed. In this example the device ran properly when the IEEE Standard was followed and failed when it was not followed.

In the code, the receiver is always on and waiting for the transmitted byte to be sent. The default signal is high, and the data is sent by first sending a low start bit, then sending the 8 data bits from the least significant bit to the most significant bit. The transmitted data, the lock and unlock signals, are 8 bits and 32 bits respectively. The extra three bytes in the unlock signal are due to the three extra characters for the unlock time duration.

3.5 Locking Mechanisms

Initially, the locking mechanism circuitry was designed to consist of both analog and digital components. The thought was that the digital components would receive inputs from the firearm's microcontroller to behave as switches to control the voltage across the motors. In this design, the analog components, polarity reversing circuitry and comparators, would be used to ensure that the motors spun properly in response to different inputs from the firearm's microcontroller. Once it was determined that the motors used in the mechanical system would require up to 100 mA of current to operate, it became apparent that this design would not work since the logic circuitry would be unable to output the necessary current for the motors. To ensure that the motors would be supplied enough current to operate, the circuitry had to be designed using only analog components. Creating the proper functionality with switches while passing through enough power to operate the motors meant that high voltage and current MOSFETs were to be used.

Once it was determined that MOSFETs would be used, the next step was determining the type and quantity. Since both terminals on the motors need to be connected to +5V or ground, an H-bridge design was selected. This design necessitates the use of a pull-up and a pull-down network consisting of two PMOS and two NMOS transistors respectively. The pull-up network ties the motors to the output of the voltage regulator, while the pull-down network connects the motors to ground. Between the output of the voltage regulator and the pull-up network is a single PMOS transistor that controls the voltage input to the pull-up network. The gate of this transistor receives a signal from the firearm's microcontroller that controls when the motors were able to spin. The output is sent to the sources of the pull-up network's transistors. These transistors have two different gate inputs, one relaying the lock/unlock state and the other relaying the inverted lock/unlock state. This design ensures that one PMOS is conducting at all times, necessitating the use of the PMOS between the voltage regulator and the pull-up network. Each PMOS transistor output is tied to one of the motor terminals as well as the output of one NMOS transistor from the pull-down network.

The pull-down network consists of NMOS transistors whose sources are tied to ground. The gates of these transistors are fed with the same signal as the gate of the PMOS transistor that their output tied to. This configuration ensures that one terminal is connected to ground at all times and the other is connected to either +5V or ground, allowing the motors to spin clockwise or counterclockwise, depending on the firearm's desired state.

Another function the locking mechanism circuitry performs is sending signals to the microcontroller that relay when the locking mechanisms are in the locked or unlocked state. Using conducting plates placed in the locked and unlocked positions, signals are passed to the firearm's microcontroller which uses them to control the ENABLE input, thus controlling the movement of the motors. When the motors spin to the desired state, a connection is made that passes a high signal to the microcontroller. The microcontroller reads this signal and sets the ENABLE signal high to disable the motors. Every time the microcontroller receives a new state signal from the wireless receiver, it uses these signals as a check to see if the mechanisms are in the desired state. If the corresponding state signal is high, the ENABLE signal remains high keeping the motors from spinning; otherwise, ENABLE is set low until the mechanisms move to the new position.

3.6 Pressure Sensor

The pressure sensor's simple function, to detect when a user is holding the firearm, led to the decision to purchase a premade component. The sensor's basic function, acting as a switch, led to the realization that a simple switch would work perfectly. The pushbutton switch was selected since it would act as a closed switch only when pressed. The pushbutton is located on the firearm so that when a user held the firearm, the pushbutton would be depressed. The output of the pushbutton is fed to the microcontroller with a high signal indicating the firearm is being held and a low signal indicating the firearm is not being held. When pressed, the pushbutton passes through the voltage at its input directly to the microcontroller. This limited the pushbutton's input voltage to the maximum input that the microcontroller's input pins could handle, +5V.This is done by connecting the pushbutton's input to the output of the voltage regulator in the firearm's power supply. To keep the output signal to the microcontroller low when the button was not pressed, a pull-down resistor is placed at the output. This 33 kilo-ohm resistor ties the output to ground until the sensor is pressed and when that occurs, the large resistance maintains the+5V at the output.

4. Testing and Verification:

4.1 Fingerprint Scanner

The first step in verifying the functionality of the fingerprint scanner was confirming that the outputs ports of the scanner were properly connected. Since the port pins were very small and its connector was not a standard size, the connections were made by soldering wires directly to the back of the fingerprint scanner's board.

After these connections were made, the GPIO pins could be tested. A piece of code was written that would change the I/O line to the identify pin from high to low every time the number "1" was pressed on the keypad. Pressing "2" and "3" would change the I/O lines from high to low on the register and delete pins respectively. The Fail and Success pin outputs were fed to the control unit's microcontroller and two LEDs. The LEDs were used to show whether the fingerprint scan was successful or not while the microcontroller read the outputs to determine if the user was authorized to operate the firearm.

Next, the fingerprint scanning options were tested. The commands to identify a fingerprint, remove a fingerprint, and register a fingerprint were sent to the fingerprint scanner. These commands initiated a fingerprint scan approximately 95% of the time. The identify function and remove function were completed with a 90% success rate, but the register function worked only 50% of the time. This statistic, however, was dependent on the fingerprint being registered. Some users attempted to register their fingerprint several times before it was successful, while other users needed just one scan to register their print. This discrepancy is believed to be due to the different fingerprint characteristics of each person, making some easier to distinguish than others. Another possible explanation is that the registration function required clearer scans in order to properly save the fingerprint's characteristics to memory, whereas the identification and deletion functions likely required only a few such characteristics to match, thus increasing the success rate of these functions.

4.2 User Interface

Verifying that the user interface was 100% reliable was done by testing its components separately then connecting them together and retesting the entire system. The first component tested was the LCD display. Since the LCD constantly outputs new data, the easiest way to test it was by programming the microcontroller and checking that the LCD output the correct characters. Displaying alphabet and numeric characters on the top and bottom lines of the display was the first test. Apiece of code was written to program the microcontroller to output the signals corresponding to each number, letter, and symbol on the keypad and the LCD was checked to verify that the proper character was displayed.

The first step in verifying the keypad's reliability was to map each button press to the keypad's output pins to ensure proper connections were made. To test the keypad algorithm, the algorithm was programmed onto the microcontroller and code was added to display the key pressed onto the LCD screen. The program called for the read_keypad() statement every second, but this did not work initially because the voltages from the keypad pins that the microcontroller was reading were found to be floating. Once pull-down resistors were placed at these pins, the LCD displayed the characters corresponding to the key that was pressed, verifying that the algorithm performed properly. The final step in the keypad's verification was checking that each keypress was only registered once, no matter how long the key was held. This was tested by writing a piece of code that created a variable which incremented every time the signals for a new keypress were returned to the microcontroller. The counter's value was displayed by the LCD to verify that it would increment only once for each keypress, regardless of its length.

Verification of the user menu was done by stepping through the menu using the keypad and the LCD display. After this functionality was verified, unacceptable keys were pressed to check that the user menu did not respond to them. As expected, the user menu was traversed only when acceptable keys were pressed.

4.3 Power Supplies

To verify the batteries' lifetimes, voltage measurements were taken at different points in time and then the data was extrapolated. Using the Agilent 54642A oscilloscope, we measured the voltage being output from the batteries. One of the oscilloscope's probes was placed at the positive terminal of the battery, while the other was placed on the circuit board's ground plane. Initially, the voltage supplied by the battery was measured every 10 to 20 minutes until 120 minutes had passed. During this time, the lock and unlock signals were sent to the firearm unit multiple times to have the mechanisms move to simulate normal usage. After the 120 minutes were completed, a plot of voltage vs. time was made and the data points were fitted with a linear line. From this line, the lifetime of the battery could be estimated. Since the system will operate until the battery voltage is under 5V, a best-fit line was used to calculate the time when the voltage reached 5V. When comparing the measured battery life to the constant current plot [13], we noticed that the measured lifetime was significantly shorter than the expected value. Although some of the error comes from the 1 MOhm input resistance of the oscilloscope, it could not explain the large discrepancy. While reviewing IEEE Standard 120, we found that ground loops were the likely cause of the difference in the lifetimes "Ground loops […] can cause erroneous measurement results"[14]. Looking at our set-up, we determined that our ground loop could be removed by probing both terminals of the batteries because probing the ground plain on the circuit board formed the ground loop by connecting "Two points in a measuring system […] to the ground"[14]. Once this change was made, the measurements were repeated and Figure 1 was created using the collected data. Using equations 1.1-1.4, the actual lifetime of the batteries was extrapolated from the data.

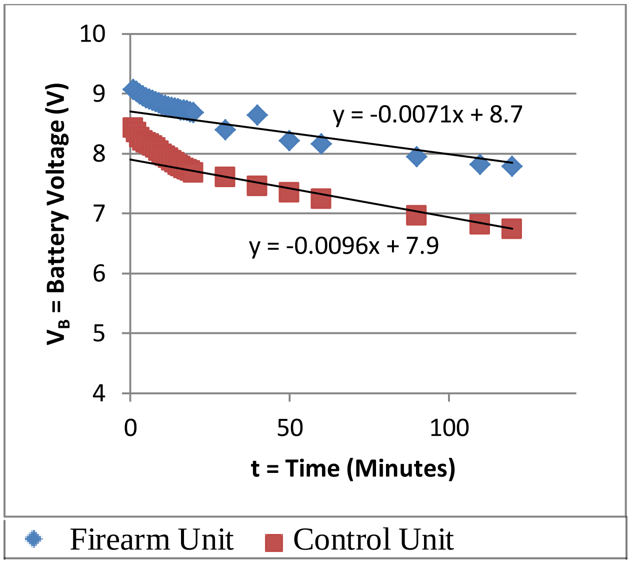

Figure 1. Voltage vs. Time for batteries

$$V_{Bfirearm} = -0.0071t + 8.7 \qquad (1.1)$$

$$V_{Bcontrol} = -0.0096t + 7.9 \qquad (1.2)$$

$$t\ V_{Bfirearm} = 5 \ = \frac{V_{Bfirearm} - 8.7}{-0.0071} = 521.1\ minutes = 8.69\ Hours \qquad (1.3)$$

$$t\ V_{Bcontrol} = 5 \ = \frac{V_{Bcontrol} - 7.9}{-0.0096} = 302.1\ minutes = 5.04\ Hours \qquad (1.4)$$

As can be seen from the above calculation, the battery for the firearm unit would last approximately 521 minutes or 8.7 hours. The battery for the control unit would last about 302 minutes or 5 hours.

The lifetime of the firearm's power supply was lower than we had initially hoped. From initial current drain measurements, we speculated that the firearm unit would use approximately 30 mA of current when the motors were still and approximately 70 mA when the motors spun. Using the constant current characteristics plot [13] from the battery's data sheet the battery life would be approximately 9.5 hours, see equations 2.1 and 2.2.

$$t = 17\,hrs * \frac{5V}{9V} \qquad (2.1)$$

$$t = 9.44\,hrs \qquad (2.2)$$

The small discrepancy between the theoretical and actual lifetime of the battery is due to the estimations made in both cases. For the theoretical value, the lifetime of the battery had to be estimated by reading the constant current performance plot while the actual lifetime was calculated by using a best-fit line from several measured data points. The only definitive way to determine the battery's lifetime would be to run the system until the battery can no longer power it.

4.4 Wireless Communication

The first step in verifying the wireless components was to test the microcontroller output to the transmitter to ensure that the correct data was being sent to the transmitter. The transmitter and receiver were then connected to their respective microcontrollers and antennas and once they were set to the same frequency, a piece of code was written that would have the control unit microcontroller send a data bit to the transmitter. To verify that the signal sent from the microcontroller was being sent to the firearm unit properly, voltage measurements were taken at the data ports of the transmitter and receiver, see Figure 2. The matching signals show that the wireless system transmission worked properly.

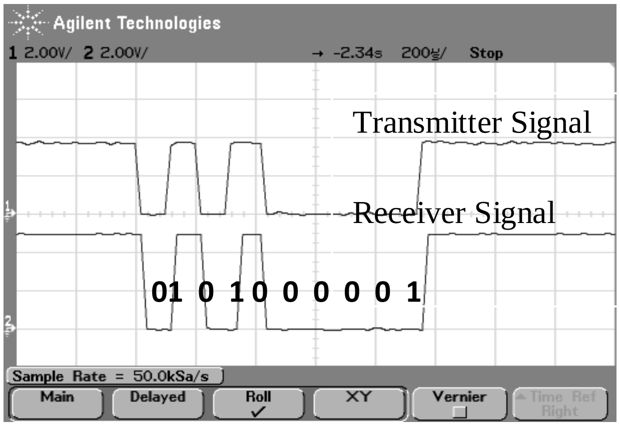

Figure 2. Wireless Signal: 00000101 (5)

After the functionality of the wireless system was verified, its range was checked. Placing the two units next to each other and sending several signals to the firearm revealed that even at such a small distance, the transmission success rate was only 90%. Testing the maximum range of the wireless system was carried out by sending lock and unlock signals from the control unit to the firearm unit while gradually increasing the distance between the two units. This procedure was repeated until the firearm no longer responded to the control unit's signals. It was found that the wireless system operated with a reliability of 80% at five feet, 50% at 10 feet, and 20% at 20 feet. While the wireless range did not reach the desired 30 feet, this issue could be resolved by using better components. Fortunately, the functionality of the project was largely unaffected by the lack of wireless range. The small wireless range would only affect performance when sending signals the firearm. With the timer for the unlock state being located in the firearm's microcontroller, the firearm could be moved out of the wireless range while unlocked and still relock once the unlock time runs out. The firearm could then be moved back within the wireless range to have new signals sent to it.

4.5 Locking Mechanisms

To verify the functionality of the locking mechanisms, the inputs to the MOSFETs' gates were hardwired to simulate the signals that would be received from the microcontroller. While these signals were varied between +5V and 0V to simulate the lock and unlock signals, voltages were measured at several points in the circuit to verify that the motor terminals would receive different voltages when the signals changed. The motors were then connected to the circuitry to confirm that the MOSFETs were able to pass through enough power to operate the motors. Next, the microcontroller was connected to the mechanisms' circuitry to test upper-level functionality. Signals were sent from the microcontroller to place the locking mechanisms into the lock or unlock state; once the motors moved to the proper position the signal was repeated. When the signal was sent for the second time, the locking mechanisms did not try to move into the position they were already in. As expected, the repeated signal did not cause the locking mechanisms to move. To verify that the mechanisms responded to locking and unlocking signals in less than five seconds, the mechanisms were placed into the lock/unlock state and then the unlock/lock signal was sent. When the second signal was sent, the locking mechanisms were observed to begin to move without a noticeable delay.

The locking mechanisms functioned as anticipated. They responded to the locking and unlocking in under the required five seconds and they did not try to move into the position they were currently in. The response time was not expected to be an issue since the datasheets for the MOSFETs [15], [16] indicated that the maximum delay of their configuration would be approximately 170 ns, see equation 4.

$$t_{+\,terminal} = t_{-\,terminal} = \max(2 * t_{PMOS}, t_{NMOS}) \qquad (4)$$

$$\begin{aligned} t_{+\,terminal} = t_{-\,terminal} &= \max\ 2 * 85\,ns, 90\,ns \\ &= \max\ 170\,ns, 90\,ns \\ &= 170\,ns \end{aligned}$$

When this was tested, the delay between a new input and the motors spinning was not noticeable which was expected since humans cannot perceive a delay on the order of nanoseconds.

4.6 Pressure Sensor

Verification of the pressure sensor's functionality was done by taking measurements at its output. The sensor's input was connected to a bench top power supply set to +5V to mimic the voltage that the sensor receives from the output of the power supply's voltage regulator. Using an oscilloscope, the voltage at the pushbutton's output was measured at +4.951V with respect to ground, when pressed and less than 100 mV when the button was not pressed.

These results were expected because the pressure sensor is designed to act as a switch, not dissipating any energy when closed and not allowing any power through when open. Although the pushbutton is not an ideal component, it is designed to minimize losses and behave as an ideal component. Therefore the measured voltage values were expected to be very close to 5V, when pressed, and 0V, when not pressed. The outputted voltage is non-zero due to leakage in the pushbutton, but it is less than 2% of the inputted +4.948V. The outputted +4.951V is within the desired 5% of the inputted +4.965V.

5. Conclusion:

5.1 Accomplishments

When demonstrated, this project successfully performed the desired function, increasing firearm safety. The final design has the potential to be used as a prototype for a consumer product. The user interface, which provides the user with the option to lock or unlock the weapon and allows the user to input new authorized users or remove old ones, creates a simple way for even the least experienced users to maximize the system's functionality. Using a fingerprint recognition system to authorize users makes the firearm secure and difficult to tamper with. Finally, the firearm unit is small enough that it does not interfere with the positioning of the user's hand while still performing the desired function. This was accomplished by placing the larger components on a unit separate from the firearm.

5.2 Uncertainties

Although our design functioned successfully, a few parts in the system could be changed to increase performance. The range of the wireless transmission was not as far as we would have liked. Initially, we hoped to have a range of 30 feet, but the components we used only gave us a reliable transmission range of 10 feet. Another issue that arose was the fingerprint scanner's serial interface. The initial design called for the scanner to interface with the control unit's microcontroller via serial communication, but the outputs never correctly functioned so the GPIO interface was used instead. The serial interface would have been convenient to fine tune the fingerprint scanner options and to store the fingerprints in our own system, but the GPIO interface the system could still perform the essential functions: identifying, adding, and removing fingerprints.

5.3 Future Work

To enhance the marketability of this project, some minor adjustments would need to be made. Smaller and more powerful antennas would be used to greatly increase the wireless capabilities up from the current 20 foot range. The components on the firearm unit would be replaced with smaller and more efficient ones to reduce the size of the unit and to increase the battery life. The size of the control unit could also be decreased by purchasing a LCD display without buttons attached to it. Along with the above changes, a sturdier housing must be added for this project to move from a simple prototype to an actual, consumer ready design.

6. References:

[1] *NITGEN FIM5360: Stand-Alone Fingerprint Identification Device with Built-in CPU,* datasheet, NITGEN Co., 2011. Available at: http://dlnmh9ip6v2uc.cloudfront.net/datasheets/Sensors/Biometric/FIM5360_DataSheet_v1.04.pdf.

[2] *IEEE Standard Digital Interface for Programmable Instrumentation,* IEEE Standard 488.1, 1987.

[3] LCD Front Panel Set, web page. Available at: http://www.piclist.com/techref/io/LCD/panel1.html.

[4] Custom Computer Services, Inc., *CCS C Compiler Package*, 2007.

[5] C Compiler Reference Manual, Custom Computer Services, Inc., 2011. Available at: http://www.ccsinfo.com/downloads/ccs_c_manual.pdf.

[6] *Series 96 Standard Keypads*, datasheet, Grayhill Inc., 2008. Available at: http://www.grayhill.com/catalog/keypads_96.pdf.

[7] *HP3 Series Receiver Module Data Guide,* datasheet, Linx Technologies, 2008. Available at: http://www.linxtechnologies.com/resources/data-guides/rxm-900-hp3-xxx.pdf.

[8] *PIC16F882/883/884/886/887*, datasheet, Microchip Technology Inc., 2009. Available at: http://ww1.microchip.com/downloads/en/DeviceDoc/41291F.pdf.

[9] D. Block, "GE423 Mechatronic Homework Assignment #3," class notes for GE 423, Department of General Engineering, University of Illinois at Urbana-Champaign, Feb. 22, 2012.

[10] *HP3 Series Transmitter Module Data Guide,* datasheet, Linx Technologies, 2011. Available at: http://www.linxtechnologies.com/resources/data-guides/txm-900-hp3-xxx.pdf.

[11] *ANT-916-PW-LP,* datasheet, Antenna Factor, 2008. Available at: http://www.linxtechnologies.com/resources/data-guides/ant-916-pw-lp.pdf

[12]IEEE Standard Serial Interface for Programmable Instrumentation, IEEE Standard 1174, 2000.

[13] 9V Battery (EN22), datasheet, Energizer. Available at: http://data.energizer.com/PDFs/EN22.pdf.

[14]*IEEE Master Test Guide for Electrical Measurements in Power Circuits,* IEEE Standard 120, 1989.

[15] *N-Channel MOSFET (MTP4N80E),* datasheet, On Semiconductor Corp., 1996. Available at: http://www.datasheetcatalog.org/datasheet/on_semiconductor/MTP4N80E-D.PDF.

[16] *P-Channel MOSFET (NTP2955),* datasheet, On Semiconductor Corp., 2006. Available at: http://www.onsemi.com/pub_link/Collateral/NTP2955-D.PDF.