Fall Prediction using Anomaly Detection

By Peter Malinovsky, ECE '20

Abstract

Over 60 million Americans, about 18% of the population, use a wearable device on a regular basis to track their fitness (Statista, 2020). Their buying decisions are influenced by features available, cost, and several other factors. Unfortunately, the security of the device is typically not considered when making this decision. To save costs, manufactures reuse old designs, leading to inefficiencies and a less secure product. Many people do not understand the risk they put themselves at when using a mobile medical device because they don't know how security works.

Introduction

The market of mobile medical devices covers a wide range of devices containing smart watches, fitness trackers, smart shoes, smart insulin pumps and more. Although all these devices transmit different data and perform different operations, they need to have similar considerations made when designing them. The core functionality they share is the transmission of sensitive data. Data is often sent from a mobile medical device to a cell phone and is extremely personal health information. Security needs to be at the forefront of design and is often implemented without understanding how it impacts the whole system.

The most common way to add security to a communication protocol is to add a "layer" that encrypts the message. When you send a letter, there is a protocol to follow: first you write the letter, next you put it in an envelope, write the address on it, put a stamp on it, and place it in a mailbox. Transmitting information over the internet requires similar steps, and without security, both snail mail and internet messages can allow a third party with the message to read the contents. A very simple example of security, or encryption, invented almost 2000 years ago is the Caesar Cipher. The Caesar Cipher shifts the letters in the original message by a certain number of characters. A shift of 1 would shift A to B, B to C so on wrapping Z around to A.

```
Original: Hello World
Cipher: Ifmmp Xpsme
```

To a human this looks like a scrambled mess, but to a computer, all it takes is 26 shift attempts to break the cipher. For the era, this cipher accomplished its goal, but for computer-based communication, much greater security is needed. In order to create a more robust encryption scheme, computationally challenging math is used.

In a very oversimplified model, the more time and effort put into encrypting information, the more time and effort it would take for someone to break the encryption. This leads to a very key point: encryption is not secure or insecure, it's a scale of security. When designing devices for medical applications, consumers want them to be small, fast, cheap, and have long lasting batteries. To save cost, manufactures reuse previous designs and modify security methods on existing platforms to suit their needs. Part of this modification can entail reducing the computational complexity to save power, which reduces the security of the device.

Materials and Methods

In order to understand the implications of some of these decisions, let us consider the difference in power usage between two different chip architectures. To compare the power difference in the devices, we will compare the devices using the encryption algorithm AES-256 because it is the most common encryption method according to Lee, Mal, and Nah, and the encryption algorithm ChaCha (20) because it has been developed as an alternative to AES-256 and offers similar features for the express use on ARM devices (Lee, 2007).

The two different chip architectures that will be considered are ARM and AVR. ARM is often used in mobile phones and AVR is used in smaller, lower powered devices such as mobile medical devices, and has many of the same algorithms implemented for it. Unfortunately, these algorithms are not optimized for the AVR platform and are extremely inefficient.

	ARM	AVR
AES 256	9.30 us	46.61 us
ChaCha (20)	.87 us	14.87 us

Table 1 – Architecture vs Algorithm Encryption Time per Byte (doxygen, 2018)

Table 1 shows the difference in time for each algorithm, but these are not comparable sets. The ARM measurements were taken on a chip running at 84 MHz, compared to the AVR chip which was running at 16MHz (doxygen, 2018). This means the ARM chip is running 5.25 times faster than the AVR chip. To compare these sets, we need to look at the number of clock cycles per algorithm.

	ARM	AVR
AES 256	781 cycles	745 cycles
ChaCha (20)	73 cycles	237 cycles

Table 2 – Architecture vs Algorithm Encryption Cycles per Byte

Table 2 shows the algorithms normalized to the clock cycle. We can see the efficiency of the ChaCha protocol on the ARM platform as it only uses 73 cycles, less than 10% of the cycles of AES. To understand how much power each algorithm uses, the power per clock cycle is needed. From the datasheets of the two devices, we can see that the ARM chip requires .81 mW of power per MHz (Atmel, 2015).

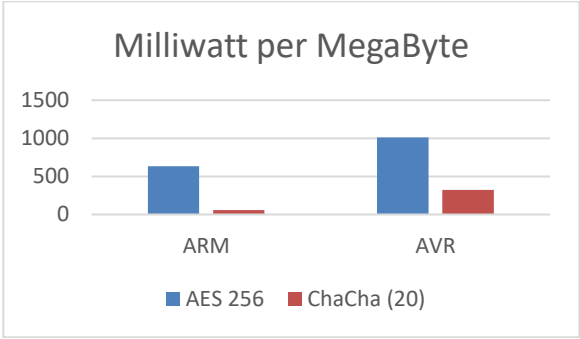

Figure 1 - Architecture vs Algorithm Encryption Power Usage per Megabyte

The AVR chip requires 1.36 mW per MHz (Atmel, 2009). In Figure 1 we can see the power usage difference between the two algorithms and architectures. Just from visual inspection the AVR chip uses more power in both cases and when the full system is considered, the AVR uses a much larger percent of its battery on encryption. The largest point that can be noted is that the most efficient algorithm across the two architectures is ChaCha running on the ARM architecture. ChaCha on ARM uses 18% of the power when compared to ChaCha on AVR, 9% of the power when compared to AES on ARM, and 6% of the power when compared to AES on AVR.

Given the previous data, we have one final aspect of the system to consider for the encryption scheme, the battery. The size of the battery will determine the level of encryption that can be carried out. For the ARM architecture, an average smartphone will have a capacity around 2500 mAh, whereas a high end mobile medical device will have a battery capacity of around 200 mAh. This means that if a mobile phone uses 5% of its battery for AES encryption, a mobile medical device would have to use 100 % of its battery to perform the same operation. For a phone using 5% battery on ChaCha encryption, a mobile medical device would have to use 341% of its battery.

Results

Comparing the ARM and AVR architecture gives us insight to the performance, but the value that it gives is the insight to the design behind the products. If manufactures were to implement a full AES 256 encryption suite, that would be the most secure route. Looking at the data present, it is unrealistic to expect them to spend 20 times as much power on encryption as compared to a mobile phone

platform. To circumvent this, more efficient algorithms such as ChaCha (20) have been designed for the ARM architecture, but not the AVR architecture. On the ARM platform a ChaCha encryption requires 9.3% of the power of an AES encryption and offers a similar level of security, whereas on the AVR platform ChaCha requires 31.8% of the power of AES. To bring down the power usage, manufactures may use less secure protocols such as AES 192, AES 128, or other lower power algorithms. Until a new algorithm is optimized for lower power platforms, security measures will remain inefficient and insecure.

Encryption can also be improved on low power platforms by including hardware for the express purpose of encryption. Doing this raises the cost of design and requires manufactures to go back to the drawing board. This cost is often passed on to consumers which creates an unfortunate situation. These products have the power to save people's lives, but if they are priced too high then only a select portion of the population will have access to them. If cheap and insecure products are released, customers will be placing their medical information at risk.

Unfortunately, there is no easy solution to this problem. Educating consumers on how security works is a step in the right direction. This can be followed by manufacture transparency regarding how their products are designed, but there is no permanent solution to this problem. To maximize profits companies will continue to design products that just meet expectations. Without in-depth analysis of how every product works it is impossible to determine the level of security present, leaving users potentially vulnerable.

Mobile medical devices will continue to increase in popularity as their utility increases and cost decreases, and the only way to for consumers to protect themselves from an increased security risk is through education. Unfortunately, this is a very complex topic and even individuals who design these products have little understanding of the implication of their design. A system of standards from a centralized source such as the government or a professional society such as IEEE could aid in this process but mandating that every mobile medical device undergo this process could have negative consequences such as raising development cost.

Consumers must do significant research before deciding to use a mobile medical device. By approaching the situation weary of security, consumers should be able to weigh the pros and cons for themselves. If the worst-case scenario is always kept in mind, then realistic purchasing decisions can be made.

Glossary

us – Microseconds, one millionth of a second
MHz – Megahertz, million cycles per second
mW – Milliwatt, on thousandth of a watt
Watt – Standard unit of power
mAh – Milliamp hour, unit of charge
Milliamp – One thousandth of an amp
Amp – Standard unit of electrical current

References

Atmel. (2009). *ATMega328 Datasheet*. https://www.sparkfun.com/datasheets/Components/SMD/ATMega328.pdf

Atmel. (2015). *SAM3X / SAM3A Series Datasheet*. https://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-11057-32-bit-Cortex-M3-Microcontroller-SAM3X-SAM3A_Datasheet.pdf

doxygen. (2018, April 27). *Arduino Cryptography Library*. https://rweather.github.io/arduinolibs/crypto.html

Lee, H. K. (2007). *Cryptographic Strength of SSL/TLS Servers: Current and Recent Practices*. http://www.cs.columbia.edu/~homin/papers/psst/LeeMalNah-2007.pdf

Statista. (2020). *Number of Wearable Device Users in the US 2014-2022*.