Wiegand Protocol Access: A Decade of Decryption

Brandon Chung

13 December 2017

Abstract

Wiegand based access systems are by far the most ubiquitous card access technology employed in modern establishments. Its overwhelming universality is in part due to its relatively simple installation as well as its incredibly vast selection of manufacturer support. Unfortunately, Wiegand interfaces are notoriously insecure and are among some of the most easy-to-hack card reader systems currently on the market. Although these vulnerabilities are not new by any means whatsoever, countless organizations continue to utilize Wiegand products to this day. This article will attempt to explain the history of the Wiegand technology and why in particular these exploits are possible; more importantly however, this article will explore how these decade-long vulnerabilities have not been properly addressed, what potential dangers exist with Wiegand products, as well as provide meaningful forms of defense against similar exploits.

1. Introduction

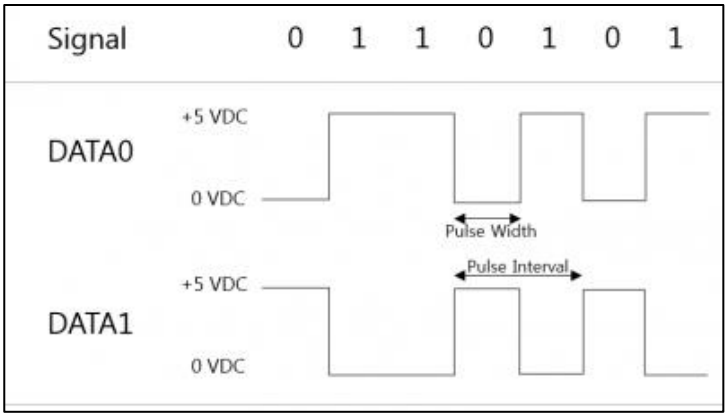
In regards to card reading technology, The Wiegand interface has been the most commonly used wiring standard since the late 1970s. Originally based on John R. Wiegand groundbreaking discovery, these products have and continue to be the most popular access interfaces for schools, corporations, and even government establishments. Although there have been a number of logistical updates in the past 40 some years, the general physical hardware and its complimentary software have been nearly identical since its inception.

On one hand, this is incredibly convenient for companies looking to purchase tried and true access control systems. Not only are they streamlined in design, but Wiegand interfaces are relatively cheap and supported by virtually all manufacturers. In fact, Wiegand access systems have become so pervasive that they are often considered the de facto gold standard.

That being said however, Wiegand's ubiquity also poses a number of unfortunate consequences. For instance, hacking the access system in itself is ridiculously easy; any person willing to read a brief tutorial online is capable breaking this technology. What's even more disconcerting, however, is that none of these hacks are new. There actually exist online forums dedicated to breaking Wiegand interfaces from as early as 2007. Even more unsettling is that these same apparent deficiencies that worked in 2007 can be more or less applied in 2017. Before diving into exactly what enables these exploits, it's important to first understand the inner-workings of the Wiegand interface itself.

1.1 Wiegand for dummies

After German scientist John R. Wiegand discovered specially aligned wires could produce magnetic fields, hardware engineers immediately began finding uses for this scientific phenomenon. What they found was that they could actually build this same wiring configuration into a plastic card through binary encodings. From here, the cards could be passed through a magnetic reader which would access the card's data through two aptly titled wires DATA 0 and DATA 1. Upon accessing this data stream, these cards could instantaneously identify credentials.



Traditional Wiegand cards generally possessed 26 bits of data. These bits consisted of two error checking bits, 8 facility bits, and 16 ID bits. The facility bits would be used to specify which sub location at an establishment was being accessed (e.g. storage room vs. classroom). The ID bits would contain the actual combination of bits that would provide access into the desired location.

The design of both the hardware and software components was exceptionally straightforward and made repairs very manageable. Additionally, this state-of-the-art technology allowed people to carry around lightweight keycards opposed to other more unwieldy forms of access. As a result, the Wiegand interface was a favorite among manufacturers and users alike.

1.2 What's nice

Nearly every access control manufacturer in the world has a Wiegand compatible interface. Keri, Systems, for example, allows customers to customize and tailor their security solutions to their individual needs. This way, customers can fully personalize their access systems whether it be for a pedestrian turnstiles or even more advanced selections such as proximity readers. Each of these products offers customers the ability to choose their own credential type. Customers either select a type from a preexisting library or create their own unique data format. Regardless of their decision, a large majority of the data formats have output types that are compatible with Wiegand interfaces.

1.3 What's not nice

Partially as a consequence of its streamlined design, the Wiegand interface is unidirectional; i.e., there only exists a conduit of communication from the reader to the controller and not vice versa.

Because of this, the devices cannot collectively be updated; instead, these readers must be patched manually. Meaning, if a firmware update is available, the customer must physically approach each reader device and install the firmware locally. This lack of bi-directionality offers a host of new potential security issues. For example, it's very possible that a particular organization employs large number of these Wiegand devices. If that's the case, it is also possible that the customer may forget to properly update all the readers. This in turn generates security vulnerability as not all the readers may be up-to-date. Consequently, hackers could take advantage of these readers by manipulating security flaws that weren't successfully patched.

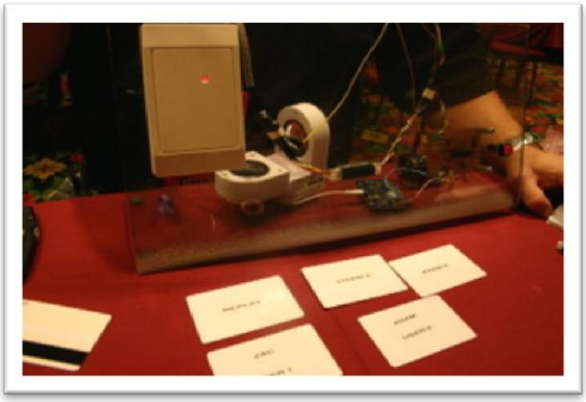
Furthermore, the lack of remote installation may unfortunately mean that many establishments that do employ Wiegand readers may be unknowingly using insecure firmwares. In fact, people have developed methods of breaking into these un-updated readers in the past.

Outside of the firmware issue however, one of the larger dilemmas with the Wiegand interface is actually customer misuse. Despite explicit recommendation, many customers do not possess a catalogued library of authorized card sequences. Meaning, if a card is lost and a duplicate is made, there now exist two valid cards that are unaccounted for: the duplicate and the lost card. Duplicating cards like this without proper archiving could result in cards being available to unauthorized personnel. Immediately, this poses a security threat as there no longer exists a record of valid keycards.

In addition, customers by and large purchase the 26-bit variation of the Wiegand products. The issue here is that the 26-bit format is meant to be installed only in the absolute least important security applications. Wiegand actively suggests that more secure formats such as the 32 or 37-bit variations be employed for more significant security solutions. Unfortunately, the majority of Wiegand products that are out in the world today are of the highly insecure 26-bit format. The widespread nature of these less secure options is one of the reasons why so many Wiegand systems today are still insecure and susceptible to attack.

2. What has been the issue (2007)

Up until now, this article only explored the issues that already exist within the Wiegand product itself. As noted above, it's clear that these devices are non-optimal forms of access control as they inherently possess a number of deeply-rooted operational deficiencies. Still, the greatest issue of them all is how easy it is to manipulate these products.



In 2007, Kim Zetter published a story on Zac Franken's DefCon presentation. Here, Franken presented a conference where he developed a method of exploiting a major vulnerability in Wiegand interfaces. In short, the hack enabled Franken to trick the card reading device into granting authorization without proper identification. Interestingly, Franken was able to further exploit this hack beyond mere unauthorized access. For example, Franken was able to both lock out other authorized users as well as harvest data regarding all personnel who accessed the entrance.

According to Franken, the hack involved physically inserting a PIC microcontroller into the rear of the card reading device. This entire ordeal can be completed in under five minutes if performed correctly. Franken actually stated that some card readers do have more advanced

security features that warn the primary backend if a reader was being tampered with. He then followed up by saying this security function is entirely bypass-able if you connect the correct wires. Once connected, Franken merely had to wait for someone with an authorized card use the reader like normal. Once used, the PIC microcontroller essentially spoofed the valid user and was able to reproduce that sequence on command, thereby providing unauthorized access indefinitely.

Though this presentation was certainly an impressive display of skill and expertise, it would be foolish to think that such a simple hack could still be used a decade down the line. Surprisingly however, not only is similar exploit still available, it is both easier and more malicious.

2.1 What is the issue (2015)

In 2015, Bernhard Mehl posted a blogpost and supplementary video that demonstrated him duplicating keycards from a Wiegand device. In his post, he explained how this hack could be performed with a $10 microcontroller that he purchased online. Even more shocking is that he was able to perform this entire procedure in under 45 seconds.

His order of operations began with first attaching the microcontroller to the rear of the card reader, similar to Zac Franken's 2007 exploit. Afterwards, he would then use his mobile device to determine a valid sequence and imprint that digitally onto a blank card of his choosing. Once complete, the card was now permanently inscribed with valid credentials and could be used as an identical duplicate.

A near decade has passed since the original exploit was first made public, yet the same insecurities that plagued the previous iterations of Wiegand devices still persist to this day. What's worse is that these procedures have gotten even easier to both recreate and perform. Moreover, Mehl's video shows him employing this hack to perform even more nefarious activities. Remote access, for instance, was now available at the mere touch of a button. Meaning, Mehl didn't even require a physical duplicate of the card in order to be granted access; instead, he merely had to tap on his phone and his mobile device would send the proper credentials to the reader. Even previous exploits from Franken's original hack such as the data acquisition are still available and now presentable in a clear mobile UI.

2.2 Why is this significant

Though Mehl's further exploitation of Franken's discovery was certainly entertaining and a sheer spectacle to witness, these two hackers present a bigger crisis that is far greater than merely granting authorized access. This greater dilemma is of course the lack of communication in tech.

The fact that exploits like this can persist for nearly a decade is simply unacceptable. It aptly portrays the lack of proper communication between technological services and real world applications. As stated prior, none of these security invulnerabilities are new. These security risks have surfaced multiple times by more than these two individuals. HID—one of the principal companies responsible for distributing Wiegand keycards—even dedicates a part of their site to safeguarding against vulnerabilities in legacy systems. Despite all this however, an embarrassingly huge number of establishments are still susceptible to these same exploits and, most likely, will continue to be susceptible in the future.

The most important thing to take away is that there needs to exist a more widespread awareness of these security flaws. Shortcomings like these are not uncommon in technology and it is simply unethical to continue to deploy this type of technology without considering the many potential hazards it may entail.

3. How do we protect ourselves

There exists an abundance of ways in which both manufacturers and consumers can protect against similar security vulnerabilities.

According to Franken, manufacturers of access control systems should ensure that all readers require a cryptographic handshake between itself and any keycard. By doing so, card readers will reject cards that do not possess a specifically encoded encryption. It is important to add that these encryptions should only employ the most up-to-date encryption techniques to absolutely ensure maximum security.

In terms of the actual hardware, all the card readers should be equipped with a signaling device that immediately reports its status to a remote controller. These signals should be sent as soon as the device is being tampered with so that hackers cannot bypass this security failsafe. Interestingly, many traditional Wiegand devices are not equipped with any form of hardware protection; as a result, it is impossible to determine if a reader is defective until someone physically determines that the machine is out of order.

Software-wise, card readers should be able to remotely report their current firmware as well as receive firmware revision without direct installation. This way, there can be a form control and organization of all devices in a given establishment.

Consumers also possess an equal responsibility for understanding as well as defending against security vulnerabilities.

For one, always keep a library of valid cards and its correspondent users. Whenever a card is lost or duplicated, mark the change in the archive and remove privileges for the cards that are no longer in use.

Secondly, consider checking to see what product is currently being used in your establishment. Research whether that product is known to be vulnerability prone and if so, consider replacing the devices with more secure products. Suggestions include Keri’s NXT

Series Readers which, unlike traditional Wiegand products, offer bi-directional communication from reader to controller.

4. Conclusion

Approximately 80% of companies the currently employ a form of access control use either a Wiegand system or a Wiegand-based product. This is not to say that all of these products are defective, but it does give some insight as to how relevant this threat is.

Security vulnerabilities are by far some of the least understood and well remedied aspects of all computer science. Not only do these topics generally get neglected, but even when they are examined there tends to be a lack of proper communication between parties.

SQL injection and cross-site scripting, for example, have been known web-based invulnerabilities since the very beginning of the Internet. In spite of all this, these two security risks are still among some of the highest and most common across the entire web.

Why is it that such simple insecurities can still exist so prevalently today? Frankly, it's simply because people don't care. Many times technological issues are simply brushed under the rug; far too many people put way too much trust into their tech. Consequently, common issues begin to surmount and identical problems arise over and over. In order to see change, there needs to be a shift in the way people think about technology. Technological advancements should be scrutinized as vigorously as new medicine or bridge building. There needs to exist more security standards for newer products, but at the same time finding solutions for legacy systems.

Unfortunately there doesn't seem to be a simple answer, but the best that we can do is to spread awareness of problems that we can fix, such as Wiegand services, and problems that we hope to fix somewhere down the road.

5. References

Zetter, Kim. “Open Sesame: Access Control Hack Unlocks Doors.” Wired, 4 Aug. 2007, www.wired.com/2007/08/open-sesame-acc/.

Mehl, Bernard. “How HID Readers Are Hacked Using the Wiegand Protocol Vulnerability.” Kisi Blog: News, Events, Product Updates and More, Kisi Inc., 22 Apr. 2016, blog.getkisi.com/hid-keycard-readers-hacked-using-wiegand-protocol-vulnerability/.

Mehl, Bernhard. “Any HID Keycard Can Easily Be Hacked Using A $10 Device.” Kisi Blog: News, Events, Product Updates and More, Kisi Inc., 19 Aug. 2015, blog.getkisi.com/hack-hid-keycard/.

Fenske, John. “Best Practices for Safeguarding Against Vulnerabilities of Legacy Systems.”HID Global, HID, 14 Sept. 2015, www.hidglobal.com/blog/best-practices-safeguarding-against-vulnerabilities-legacy-systems.

Geiszler, Dennis. “What Is Wiegand? A Brief History.” Keri Systems, Keri Systems, 27 July 2017, www.kerisys.com/latest-news/what-is-wiegand/.

M, Robert. “Wiegand Vulnerability Archives.” AlphaGuardian, 7 Oct. 2015, www.alphaguardian.net/category/wiegand-vulnerability/.

6. Try it Yourself

Here is a demonstration of how to exploit a simple Wiegand device by employing an Arduino device. This demo was adapted from an existing Arduino project written by JP Liew.

I personally tried this on my own device after purchasing a throwaway Wiegand utility interface.

Connect your Arduino device to a Wiegand RFID Reader by connecting the DATA 0 to your second pin and the DATA 1 to your third pin (I used a HID reader for this part and it worked just as well).

Create a folder and Git clone the source code.

```
cd arduino/libraries
git clone https://github.com/monkeyboard/Wiegand-Protocol-Library-for-Arduino.git
Wiegand
```

Afterwards execute the Arduino IDE.

This particular code will execute and register the name and return the code of the Wiegand device. Although this will not grant you access to any unauthorized locations, this quick project gives insight into how easily accessible these Wiegand products truly are.

Try the example code below excerpted from JP Liew's original project.

```
#include <Wiegand.h>

WIEGAND wg;

void setup() {
        Serial.begin(9600);
        wg.begin();
}

void loop() {
        if(wg.available())
        {
                Serial.print("Wiegand HEX = ");
                Serial.print(wg.getCode(),HEX);
                Serial.print(", DECIMAL = ");
                Serial.print(wg.getCode());
                Serial.print(", Type W");
                Serial.println(wg.getWiegandType());
        }
}
```