RFID Security - Have you left your doors open?

BY SPENCER GILES, QSA, CTGA, GSNA, LPIC-1, CLA, LINUX+

If you have ever been to a downtown coffee shop on a Monday morning, I am sure you have noticed that seemingly everyone has a small, white plastic badge attached to them somewhere. These are RFID (radio frequency identification) badges and are widely deployed by organizations around the world to control physical access to buildings, data centers, and other sensitive areas. RFID is a rather simple technology that facilitates tracking, logging and identification via radio waves.

RFID badge systems allow organizations to reduce the cost of replacing lost keys, generate automated electronic access logs and restrict access based on variable factors such as the time or day of the week. It’s no wonder that the use of this technology has been adopted in almost every industry; it is a cost effective, modular and potentially powerful method of access control. However, are these systems giving organizations all over the world a false sense of security? How secure would you feel if I told you that with a wireless device the size of a deck of cards, it is possible to clone an RFID badge and gain access to a building secured with standard RFID technology within seconds?

TECHNOLOGY

Typically, there are three components within an enterprise RFID badge access system: the badges, the readers and the backend controller. When a badge is presented to a reader, the reader’s radio energy field energizes the RFID chip on the badge at which point the badge transmits its value to the reader. There are three frequencies that RFID typically operates at:

<table>
<thead>
<tr>
<th>Name</th>
<th>Frequency</th>
<th>Readable Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low Frequency (LF)</td>
<td>120 kHz – 140 kHz</td>
<td>&lt;3 ft. (usually ~1.5 ft.)</td>
</tr>
<tr>
<td>High Frequency (HF)</td>
<td>13.56 MHz</td>
<td>&lt;2.5 ft. (usually ~1.5 ft.)</td>
</tr>
<tr>
<td>Ultra-High Frequency (UHF)</td>
<td>860 MHz – 960 MHz</td>
<td>+/- 30 ft.</td>
</tr>
</tbody>
</table>

Once the badge has been read, the reader transmits the badge value to the backend controller to either approve or deny access. The reader does this by transmitting the badge value to the controller using the Wiegand protocol. The Wiegand protocol is a very simple (i.e., plain text, easily intercepted and replayed) technology that consists of two wires: DATA1 and DATA0. When the reader needs to send a “1” it lowers the voltage on the DATA1 wire and alternatively, when it needs to send a “0” it lowers the voltage on DATA0. The controller takes this information and decides whether or not the badge value has access to the specific door where it was read.
The most popular RFID badge system in use at enterprise facilities is the HID ProxCard. These low frequency (125 kHz) badges are known to be easily compromised, yet organizations are still deploying them to secure their sensitive locations around the world. These HID badges have a 44-bit value passively stored on the badge. This value is made up of several sets of numbers; the most important being the facility code and the actual unique badge number which together make up 26 bits. It is only these 26 bits that are used to identify the badge to the controller. Beyond this, there is no other form of authentication, encryption or hashing that takes place.

What this means is that 70% - 80% of organizations using RFID physical access control systems are relying upon an easily intercepted and replicated 26 bit value with no authentication or encryption which is then sent over two, easily tapped physical wires to secure their facility’s most sensitive areas. I am willing to bet that false sense of security is starting to fade away right about now.

**ATTACK VECTORS**

There are many different attacks that could be leveraged against RFID systems. I want to outline two easily executed attacks which can exploit RFID technology and can be launched using a simple device known as the Proxmark III.

The ProxMark III is the de facto device for attacking RFID-based physical access control systems. Originally created by Jonathan Westhues for his master’s thesis, both the software and the hardware has been continually developed by an active online community (www.proxmark.org). This very flexible and powerful device is the size of a deck of cards and is able to read, simulate and clone both high frequency and low frequency RFID devices. Anyone with $399 and a moderate amount of technical ability will have a viable platform to gain access to your facilities.
In order to better understand this device and to facilitate consulting with clients on these type of attacks, we got our hands on a ProxMark III. What we found was rather concerning. I was able to scan my company badge with the device, simulate it and use it to gain access to our building in about 15 seconds. The ability to hide a ProxMark in an innocuous location due to its small size, and its abilities to read badges from a distance and run off a battery, makes sniffing badges from a public location shockingly easy. Recorded badges can then be cloned to blank badges and used to gain access to secured locations all while being indistinguishable from the authentic badge in the electronic logs.

Another attack that can be carried out using the Proxmark III and some computer code is a brute force attack. Brad Antoniewicz at McAfee recently wrote a whitepaper exploring the viability of different brute force attack methods on the popular HID RFID systems. Because these systems only use the 26 bits that are made up by the static facility code and the unique badge number, the entire 44 bits on a valid badge do not have to be brute forced. The key space for the 26 bit value is $2^8$ (facility code) * $2^{18}$ (badge value), leaving us with 67,108,864 possible keys (3). According to Mr. Antoniewicz’s estimations, this would take around two years to brute force outright, which reduces the value of such an attack. However, there is another characteristic of HID badges that further reduces their effective security.

When HID badge cards are ordered, organizations must provide their facility code and an acceptable range for the new badge numbers. Because of this, badges are sequential and predictable which further reduces the key space to the attacker’s advantage. While this is clearly a viable external threat vector, the attack can also be leveraged internally by a disgruntled employee to cause significant harm which is digitally untraceable in the logs. Using a device like the ProxMark III, an employee could read their own badge and retrieve the facility code and their badge number. With the knowledge that other employees’ badges have the same facility code and that the badge values are numbered sequentially, the employee could easily brute force another employee’s badge and create a copy for themselves. Antoniewicz found that once a single valid badge number was known, he could solve for another valid card within five minutes (3).
SOLUTIONS

So, how should organizations be mitigating these significant risks to their environments? For one, the notion that having an RFID physical access control system guarantees that an organization is secure needs to be abolished. It is far too often forgotten that there are no “silver bullets” in security, and RFID security is a perfect example. Organizations need to stop relying solely on their RFID badge systems to provide security assurance for physical access control. Other mechanisms need to be implemented in conjunction with their RFID systems (i.e., defense in depth).

Probably the cheapest option involves educating your employees about RFID security. Organizations need to be instructing employees to not wear their badges in plain view while off company property (such as in the aforementioned coffee shop). Another inexpensive mitigating control could be the use of RFID blocking sleeves when the badges are not in use (although the practicality of ensuring all employees abide by this control is questionable at best). If you do decide to pursue the badge sleeve option, thoroughly test them with your organization’s badges. RFID operates at different frequencies and not all sleeves effectively block all frequencies.

A basic model which is often applied to IT security is time based security. Time based security is the idea that if you can decrease your detection and response times you will in turn reduce your exposure time if an attack is leveraged against your system. An example would be ensuring that video surveillance is located at every entrance and exit. While having video surveillance in and of itself will not prevent the attack, it may provide a means to quickly identify unauthorized individuals and to corroborate electronic logs generated by the badge system to an actual image of the event. The response to an attack would be much faster and more accurate if armed with the information provided by a video surveillance system.
One of the most common responses to RFID risks is the idea that if anyone gained access to a location they were not supposed to be in, they would be recognized by other personnel. However, if you were trying to gain access to a secured location, would you try doing it during business hours when the location is occupied? No, you would attempt access after-hours. If nobody needs to access secured areas after-hours, implementing a control that denies all access after a particular time mitigates risk related to attack timing. An organization could go beyond this for locations that are not frequently accessed by default disabling all access and implementing a process for requesting access and only granting it for a specific time period.

ALTERNATIVE TECHNOLOGIES

So while all of these controls would be a step in the right direction, none of them address the root cause of the risk, which is that HID and many other RFID technologies are fundamentally insecure. However, in recent years, several alternative systems have been marketed which utilize secured technologies. One possible option to consider is an active RFID system. These systems utilize “contactless smart cards” which incorporate encryption, mutual authentication and message replay protection, essentially mitigating most RFID attack vectors.

A quick note on biometric scanners. As a self-described “geek”, biometric scanners are on the top of my list for their cool factor. However, while these systems are not traditionally vulnerable to a remote “sniff” attack, or theft of credentials, many biometric systems still use the Wiegand protocol to communicate to the controller. As previously discussed, this is an insecure protocol which is (unfortunately) the standard form of communication in many physical access control systems. If the Wiegand protocol is used in any physical access control implementation, transmissions are plain text, easily intercepted (depending on physical implementation) and easily replayed, therefore reducing the potential security assurance gained from use of biometrics (2).

CONCLUSION

Physical access controls need to be thought of and managed just like any other form of security. Much like a reserve parachute, mitigating security controls need to be implemented alongside your primary method of security because sooner or later your main chute will fail. When it does, you do not want to leave your facility’s doors wide open.
REFERENCES:

(1) Fransis Brown, “Live Free or RFID Hard” Black Hat 2013 presentation
      or-RFID-Hard-Slides.pdf

(2) Zac Franken “Physical Access Control Systems” Black Hat 2008 presentation
   a. https://www.blackhat.com/presentations/bh-dc-08/Franken/Presentation/
      bh-dc-08-franken.pdf

(3) Brad Antoniewicz “ProxBrute: Taking ProxCard Cloning to the Next Level”
      proxbrute.pdf