Radio Frequency Identification Access Control Security

William Beard
University of Hawaii West Oahu

Abstract

With security becoming an ever-growing concern for modern organizations there has been a boom in companies installing access control systems designed to provide access to authorized individuals while maintaining a reasonable amount of security. Unfortunately, not all access control systems are created equal, and some companies are installing subpar systems. In some instances, these access control systems are easier to bypass then your standard deadbolt. One of these such access control systems is that of the Radio Frequency Identification or RFID. RFID access control systems can be bought for about $80 - $400 online and come in many different shapes and sizes. This brings to mind the question if an RFID access control system can be bought so cheap than how secure is it?

Introduction & Research Question

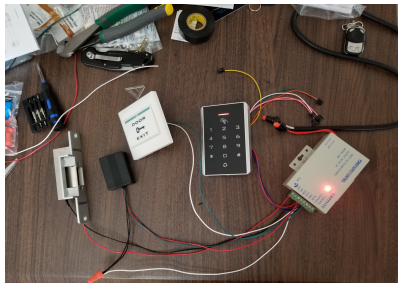
Introduction
In this research I tested a cheaper access control system by trying to clone, spoof, and simulate the access cards or tags used when authenticating access. To do this I used the Proxmark3, a pen-testing tool designed to access these cards and systems.

Research Question
The main question of this research was, how easy would it be to bypass the normal security of a lower cost access control system?

Hypothesis
Under the right circumstances I believe it would be relatively easy to bypass the security of the lower cost RFID access control systems.

Research Design & Data Collection

The research design for this project involved the setup of an access control system. The second step was to setup and configure the Proxmark3 which is pictured below with the access control system. Once configured three tests were conducted which included a spoof test, clone test, and a sim test. Each card and tag were evaluated five times for each test. All data from the tests was collected and analyzed using Microsoft Excel.



Access Control System
And
Proxmark3

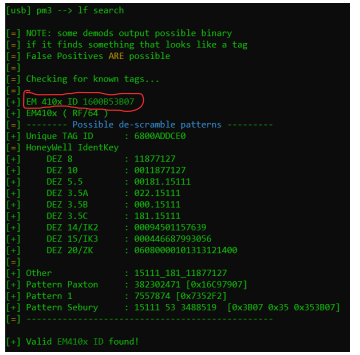


Figure 4. Low Frequency Search

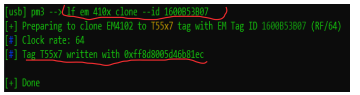


Figure 5. Cloning a Card ID

Results

As illustrated in Figures 1, 2, and 3 all three tests were successful on each card and tag except card #3 which was determined to be inoperative. The green blocks represent successes and the red blocks the failures which resulted in a 90% success rate for all three tests.

Discussion

All three tests are similar but with minor differences. The spoof test copies a card or tag to the Proxmark3 and requires an authenticated RFID card or tag. The clone test also requires an authenticated card for tag but instead copies it to a blank card or tag. The simulation test only requires an authenticated card or tag ID which can then be programmed into the Proxmark3. Figures 4 and 5 demonstrate the process required to scan an authenticated card and copy the information to a blank card.

Conclusions

The results of this research showed that the Proxmark3 can be used to spoof, clone and simulate authenticated cards or tags to bypass the security of RFID based access control systems. The cost of the access control systems was approximately $100 and the Proxmark3 approximately $320 for a total cost of $420. The security provided by this cost of this access control system was consistent with the hypothesis. The higher priced access control systems offer better security with encryption and network connectivity which allows improved authentication.

Spoof Test Results						
	Test 1	Test 2	Test 3	Test 4	Test 5	Total
Card 1						5/5
Card 2						5/5
Card 3						0/5
Card 4						5/5
Card 5						5/5
Tag 1						5/5
Tag 2						5/5
Tag 3						5/5
Tag 4						5/5
Tag 5						5/5

Figure 1. Spoof Results.

Clone Test Results						
	Test 1	Test 2	Test 3	Test 4	Test 5	Total
Card 1						5/5
Card 2						5/5
Card 3						0/5
Card 4						5/5
Card 5						5/5
Tag 1						5/5
Tag 2						5/5
Tag 3						5/5
Tag 4						5/5
Tag 5						5/5

Figure 2. Clone Results

Sim Test Results						
ID #	Test 1	Test 2	Test 3	Test 4	Test 5	Total
1600687666						5/5
16006867b3						5/5
Card 3 DOA						0/5
16006867c9						5/5
1600b53b07						5/5
13007c13ac						5/5
13007c4985						5/5
13008d55e2						5/5
13007c438d						5/5
13008c6018						5/5

Figure 3. Simulate Results

Contact

William Beard
UHWO

References

1. Munoz-Ausecha, C., Ruiz-Rosero, J., & Ramirez-Gonzalez, G. (2021). RFID Applications and Security Review. *Computation*, *9*(6), 69.
2. Kumar, A., Jain, A. K., & Dua, M. (2021). A comprehensive taxonomy of security and privacy issues in RFID. Complex & Intelligent Systems, 7(3), 1327-1347.
3. Gabsi, S., Beroulle, V., Kieffer, Y., Dao, H. M., Kortli, Y., & Hamdi, B. (2021). Survey: Vulnerability Analysis of Low-Cost ECC-Based RFID Protocols against Wireless and Side-Channel Attacks. *Sensors*, *21*(17), 5824.
4. Wang, R., Gong, Q., Zhen, K., Hou, X. Z., He, M., & Wang, L. Y. (2021). Research on RFID Security Evaluation Method in smart meter. In *IOP Conference Series: Earth and Environmental Science* (Vol. 645, No. 1, p. 012081). IOP Publishing.
5. Lenko, F. (2021). Specifics of RFID based access control systems used in logistics centers. *Transportation Research Procedia*, *55*, 1613-1619.
6. Shariq, M., Singh, K., Bajuri, M. Y., Pantelous, A., Ahmadian, A., & Salimi, M. (2021). A Secure and Reliable RFID Authentication Protocol using Schnorr Digital Cryptosystem for IoT-enabled Healthcare in COVID-19 Scenario. *Sustainable Cities and Society*, 103354.
7. Sujatmoko, B. A., & Sujarwo, A. (2020, April). Dual Security System for Room Access Control Using RFID at Islamic University of Indonesia (UII). In IOP Conference Series: Materials Science and Engineering (Vol. 803, No. 1, p. 012029). IOP Publishing.
8. Anaza, S. O., Jiya, J. D., Haruna, Y. S., Equipment, P., Balewa, E. A. T., & Balewa, A. T. RISK ASSESSMENT OF A RFID-GSM BASED LOCK SYSTEM USING FMECA.
9. Emakpor, S., & Esekhaigbe, E. (2020). Development of an RFID-based security door system. *Journal of Electrical, Control and Technological Research*, *1*, 9-16.
10. Verma, G. K., & Tripathi, P. (2010). A digital security system with door lock system using RFID technology. *International Journal of Computer Applications*, *5*(11), 6-8.