Security Analysis of Key Fob Installation at ECE & CS

Justin Fu, Steven Tse, Gavin Yip, and Christina Young, *Students, EECE412*

***Abstract*— The access control system used in the University of British Columbia (UBC) Electrical Engineering and Computer Engineering (EECE) department buildings has recently been upgraded to interface a key FOB and card reader to the user instead of a numeric key pad. The upgrade has also changed the backend structure to now use Access Control Panels and the Institute for Computing, Information and Cognitive Systems (ICICS) Access Control Management System (ACMS) database. User access to restricted areas of the buildings are now granted depending on the information that is passed between the key FOB, card reader, ACPs, and the ICICS ACMS. Although the exchange of data between a key FOB and a card reader is encrypted, the exchange between a card reader and ACP uses the Wiegand protocol to pass unencrypted information back and forth. This vulnerability could potentially be exploited by attackers. This report discusses the vulnerability in detail and recommends the use of a microcontroller, user programmable key, and FPGA as a feasible implementation to encrypt the plain text messages sent using the protocol.**

I. Introduction

The term “access control” refers to the practice of restricting the use of a resource. The purpose for access control is to permit access to valuable information to only those who are allowed to utilize them, and to prevent the disclosure of such resources to external, unauthorized persons. In previous decades, people have tried different methods of implementing access control: Key-Locks, Guards, Identification badges, swipe cards, numeric keypads, RFID tags, voice recognition, fingerprint scanners, and even iris scanners.

These technologies are not perfect, as soon as they are widely deployed, users and attackers alike have found ways to suppress these access control systems and gain unauthorized access.

At the University of British Columbia, the administrative staff upgraded the access control system in the Macleod building (which houses the Electrical and Computer Engineering Department) and the surrounding buildings last year, and has increased the coverage under the access control system.

The legacy access control system in Macleod building relies on a numeric keypad interface, which a) cannot tell who has accessed the protected resource, b) can be easily affected by mechanical failure, and c) cannot prevent unauthorized users from acquiring the access code. The access code can be acquired from authorized users willfully sharing the access code or by reading over the shoulder of an authorized user, or by examining the wear on the buttons on the key pad. The keypad interface

The improved system uses RFID card readers and RFID key fobs to handle user authentication – which is supposedly more secure. Team 7 has investigated the system and has come up with several vulnerabilities inherent with current system, along with recommendations to mitigate (perhaps even eliminate) these vulnerabilities.

This report contains a technical overview of the RFID interface, a discussion on how the team has arrived at this focus, an overview of the entire access control system, a list of identified vulnerabilities, and a technical recommendation that the team proposes may augment the current level of security.

II. Approach to Analysis

A. Initial Strategy

When we first approached the project topic, we made the decision to limit our scope to only the MacLeod building’s security system. Specifically, we planned to analyze the ICICS Access Control Management System (ACMS). Our analysis would have focused on methods to gain unauthorized access to restricted zones and on seeking out vulnerabilities which may allow a disruption of the ACMS in the building.

Our strategy was to begin by looking closely at the exchange of encrypted data that is passed between an installed card reader and a key fob. We hoped that the results of the investigation would lead us to clues as to how an attacker might attempt to spoof the system or create a Denial of Service (DOS) attack. Our definition of attackers covered those on campus who possess a key fob or have access to one, and those who do not.

B. Results of Initial Strategy

We approached our initial strategy by first noting that the ICICS ACMS was implemented using the iCLASS R40 card reader manufactured by HID Corporation, one of the major companies in the access control industry. A quick check on the HID Corporation website confirmed our speculation that the exchange of messages between a card reader and the key fob is indeed encrypted. All RF data transmission is encrypted using a secure algorithm to reduce the risk of compromised data or duplicated cards[1].

Our second step was to find a way to analyze the encrypted messages exchanged between a card reader and a key fob. Our preliminary research led us to discover a tool named RFDUMP created by German security consultant Lukas Grunwald[2]. The tool is known to exploit the data stored on passive RFID chips used today by sniffing messages passed through the air.

Ambitiously, we hoped to be able to use the RFDUMP tool to copy a message and replicate the process of a granted access. We had also discovered, by this point, that a card reader scans the ID on a key fob and sends the data to a back-end system in order to determine whether access should be granted.

C. Revised Strategy

It soon became apparent that we did not have the resources needed to replicate the process of a granted entry. Those resources included equipment used to measure an RF signal to a computer and a card writer to write over a new key fob.

We decided to shift our focus to a higher level view of the MacLeod building security and enlarge our scope to include the Kaiser building security as well. Our new strategy was to, instead, do a risk analysis of the assets in both buildings along with a threat model that would include Data Flow Diagrams (DFDs).

D. Findings for Revised Strategy

We tackled this new strategy first by doing an assessment of the MacLeod and Kaiser buildings for our risk analysis. We discovered that a key vulnerability of both buildings is the slow upgrade from the old security system to the new ICICS ACMS. For example, an interview with Professor Lemieux revealed that placeholder key locks were used on doors of his research lab instead of card readers. The request for a keypad installation to allow (graduate) student entry required a two month's wait and the occurrence of a theft before the lab's request was taken more seriously. At another point in time, the key pad lock mechanism broke down and the door to the lab was left permanently unlocked. This also took an unreasonable amount of time to have the key pad repaired.

The impact of the slow upgrade is not as serious in the MacLeod building, but is still prevalent. Two examples are off-hours entry to the building by punching this year's or last year's key code into the existing mounted keypad lock and the open access to all floors of the building by use of the elevator.

The next step of our assessment was to tally the estimated value of assets in both buildings in Canadian dollars. The total estimated value came to $4 - $5 million. This estimate includes the expected annual revenue generated by IP of a little more than $3.9 million[3].

About $450 thousand of the total estimate is attributed to undergraduate facilities and about $2 million of the total estimate is from assets in the MacLeod building, not including the research labs.

To tackle the learning curve of the threat modeling process, we used different strategies[4] in an attempt to make our analysis as effective as possible. The threat modeling included use cases describing the interaction between a user and the security system, a description of the system along with DFDs, and methods to identify risks and potential threats in the system.

Our unfamiliarity with the usage of threat models led us to modify our strategy once more. We, instead, decided to focus our attention back to only the ICICS ACMS, thereby narrowing our broadened scope. We returned to our initial goal of seeking out the vulnerabilities of the ICICS ACMS, but this time, decided not to approach the goal by analyzing the encrypted messages. Instead, after an interview with the ECE Network and Computing Facilities Manager, Luca Fillipozzi, we decided to approach our goal by looking into the back end of the ACMS. A short discussion with Professor Beznosov suggested that we should, instead, conclude our findings with a recommendation to address the vulnerabilities, as we are not yet knowledgeable enough to simply confirm the strength of the security system.

E. Findings for Final Strategy

From our interview with Luca Fillipozzi, we learned that the card readers in the Kaiser and MacLeod building are connected to Access Control Panels (ACP), which interact with the ICICS ACMS server to extract user permission information. The information returned from the ACP signals the mechanical lock on an Access Controlled Door (ACD).

We also learned that the communication link between the card reader and the ACP utilizes the Wiegand Protocol[5], also known as the Security Industry Association AC-01 1996.10 standard[6]. The Wiegand protocol is an unencrypted protocol that is shared by the card reader and access control panel manufacturers alike. The protocol has been around long enough to establish its place in the current industry.

F. Ongoing Feasibility Issues

With each step of our investigation into the ICICS ACMS, we encountered hurdles that led us to believe our strategies and approaches were often unfeasible. This is what brought us to revise our initial strategy. The following are the three key reasons behind our revisions.

1) Security Concerns

The UBC ECE IT staff was largely unable to disclose any details concerning the ICICS ACMS due to the sensitivity of the information. We were only able to learn that release of the system's finer details would pose a threat to the security system itself. Since the details were released strictly on a need-to-know basis, our group turned to the Internet as an alternate main source for information.

2) Security by Obscurity

Online resources about the key fob and card reader and technology behind the ACMS are very limited. One of the first sites we visited was the HID Corporation website to learn more about the products installed in the Kaiser and MacLeod buildings. However, we found that only a few specs of their products were somewhat useful: the ISO compliance, the transmitting frequency used, and the use of encryption. Our search for information about the use of the Wiegand protocol proved to be even more futile as searches on Google and databases accessible through the UBC Library, such as Compendex, INSPEC, and IEEE, provided much less information than expected. We concluded that security companies using the protocol worked on a “security by obscurity” basis and kept the information from being released into the public for proprietary reasons.

3) Testing Platform

Experimentation on the card readers and a key fob issued by the ECE IT department is a foolish idea. Our interview with the ECE Network and Computing Facilities Manager, Luca Fillipozzi, helped us realize that tampering with the card readers is unacceptable by undergraduate students like ourselves.

III. ICICS ACMS

A. High-level Description

The ICICS Access Control Management System (ACMS) is the new security system that is implemented in the Dempster Pavilion, ICICS building, Kaiser complex, and Macleod building. Our focus in this report is obviously on the latter two. The implementation of this system in these two buildings started in early 2005 and continuous effort is being made to update the older keypad locks which are still in use. There are five aspects of the ICICS ACMS:

1. Access Controlled Door
2. Zone
3. Role
4. User
5. Key Fob

An Access Controlled Door (ACD) is any door equipped with a card reader. The purpose of the ACD is to restrict access to a zone. Each ACD is assigned to one or more zones.

A zone refers to a specific area of the building that is accessible through one or more ACDs. Access through an ACD is dependent on the role that is issued to the user making the request. Each zone is assigned to one or more roles.

Roles are issued to users of the system. The issued role is what will grant a user access to a certain zone.

The body of users is largely made up of students, staff, and faculty. Other users include those needing access to certain zones or needing access to the building after hours.

A key fob is an RFID and smart card hybrid. ICICS ACMS uses the iCLASS key fob manufactured by HID Corporation[7].

B. Components

The ACMS system is comprised of 3 additional components. The key fobs, the card readers, and the access control panels (ACPs).

1) Key Fob

The key fob is a small passive RF transponder that holds the user’s credentials, which are used to authenticate the user within the system. Being a passive transponder, the fob does not have its own power supply and must rely on an external entity (the card reader) to provide power.

2) Card Reader

The card reader is a device located at each access point that powers and securely communicates with the key fob. The main purpose of the card reader is to extract the user’s credentials (a unique ID) from the fob and relay them to the Access Control Panel.

3) Access Control Panel (ACP)

The ACP is a device that governs multiple access points and is the ACMS component responsible for physically granting or denying access through a specific access point. The ACP permits access based upon two factors: a user’s Access Level and the state of the Timezone [8]:

- Access Level - an Access Level (equivalent to a role) is a grouping of authorized access points that is assigned to a user.
- Timezone - a dynamic group of access rights based upon the current day and time.

The AMCS populates each ACP with the relevant Access Level and Timezone authorization data for the access points governed by the ACP. The combination of Access Level and Timezone authorization data determines precisely where and when a user may be granted access.

4) Wiegand Protocol

Access control technology has been around for decades and today, there are an abundance of card reader and ACP manufacturers in the market. To communicate between card readers and ACPs from different manufacturers, the industry utilizes the Wiegand protocol. The Wiegand protocol comes in various formats, in some cases customized for a particular manufacturer; however, the standard is a 26-bit format[9].

When the card reader authenticates a key fob, the card reader will then send the Wiegand protocol message that identifies the particular user to the ACP. Each key fob is identified by one particular 26-bit Wiegand message. Thus, there can be a maximum of 256 facilities and 65,536 individual identifications. The format of the message is as follows:

Bits	**Description**
1	Even parity over bits 2-13
2-9	Facility code
10-25	Identification code
26	Odd parity over bits 14-25

Table 1 - Standard 26-bit Wiegand Format

The physical connection between the card reader and the ACP is handled by three wires. The wires are ground, data 1 and data 0. Data 1 represents the ‘1’ bit and data 0 represents the ‘0’ bit. When the system is idle, both the data 1 and data 0 lines are high. When a 26-bit message is sent, the data 1 and data 0 lines pulse 0’s in a sequential and non-overlapping order[10] to represent the message. When the ACP receives this message, they can determine whether the particular user has access and if the user does, the ACP will unlock the door.

C. Security Features

The following is a description of the various security features implemented by the key fob/card reader subsystem[11]:

- Mutual authentication.
- Encrypted data transmission.
- Cryptographic data storage.
- Read/Write protection.

1) *Mutual Authentication*

Mutual authentication ensures that both the key fob and the card reader are valid entities within the system. Successful mutual authentication must occur before the authentication and authorization process can continue.

2) *Encrypted Data Transmission*

Both the key fob and card reader contain industry standard cryptographic algorithms as well as random number generators, factoring a random number into the algorithm each time it is run. As a result, not only is the transmission encrypted, but also the transmission is different each time.

3) *Cryptographic Data Storage*

Each key fob allows for DES and Triple-DES encryption of its stored data.

4) *Read/Write Protection*

64-bit diversified authentication keys protect data stored on the key fobs.

D. *Use Case Scenario*

The following scenario describes the communication and data flow of the authentication and access authorization process. Please see the figure below for a visual representation of the system.

1. Prior to the process, the ICICS ACMS populates the ACP with Timezone and Access Level authorization data relevant to the access points governed by the ACP.
2. Through mutual authentication, the key fob and card reader both identify each other, respectively, as valid entities of the system.
3. Via encrypted radio frequency transmission, the key fob's identifying credential is communicated to the card reader.
4. Using the Wiegand protocol, the card reader relays the key fob's credential to the Access Control Panel.
5. Based upon the key fob's Access Level and current state of the Timezone, the ACP either permits or denies access.

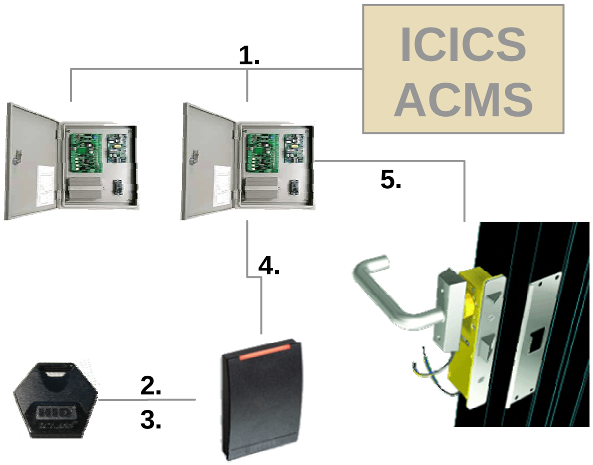

Figure 1 - System Overview

E. *Vulnerabilities*

Several vulnerabilities are identified during the group's analysis and will be presented below.

1) *Card Reader*

As mentioned above, the card reader system and the tags is an application of a RFID system. A passive RFID access control system consists of an access fob that has an antenna and an IC chip, as well as a card reader/writer that will emit and receive signals from the RFID tag[12]. In its normal mode of operation, the card reader (normally installed as a stationary fixture near access control doors (ACD) will emit an omni-directional signal to the RFID tags when one is in range. Since the system is contact-less, the RF signal transmit through the air and will be picked up by the RFID tags once the signal pass through the antenna on the passive tag. Described as a 'passive' tag, these RFID tags do not have a power source by itself; rather, these tags are powered by the weak electrical current generated by induction when the RF signal originated from the card reader pass through its coil antenna.

Powered by electro-magnetic effect generated by the pass through of RF signals, the IC (integrated circuit) on the RFID tag will compute an appropriate value and pass it back to the card reader to verify the tag's (and tag holder's) identity. Limited by the amount of energy that is used to drive the RFID key fobs, these returning RF signals are usually not as strong.

Vulnerability is found here as the returning signals from the RFID tags are easily overpowered, or interfered, by stronger signals in the same band frequency, if broadcasted within proximity. A malicious attacker could possibly emit a strong RF signal in the same band frequency that the RFID card reader / key fobs communicate (which the group is learned, at 13.56MHz[13]) and that would prohibit any key fobs from identifying themselves to gain access to protected resource.

2) *Access Control Panel*

Vulnerabilities can also be found when compatibility issues arise. The group has learned that the RFID access control security system was installed no more than one year ago and is one of the higher-end security systems offered by HID Corporation. This system also includes a tamper protection feature, which will notify the associated Access Control Panel if there is an attempt to tamper the card reader. However, the benefits realized by such a feature are limited by the ACP that this RFID card reader system is working with.

The Macleod building has been fitted with numeric keypads for building access for some time and the group has learned that these access control interfaces must be supported by decision making components of an access control system such as an ACP, access control panel. Because of the high replacement cost of ACPs, it is reasonable to assume that not all of the ACP controlling the security in Macleod, Kaiser, and any other Computer Science buildings are modern enough to support all the feature set supported by the RFID card reader system, although we are not able to verify this from the ECE IT staff.

Given that some of the ACP used in the Macleod/Kaiser ACMS may not support all the feature set of the RFID card reader system, that means the data from some of the advanced feature set, such as tamper-protection, on the individual card readers are ignored by the ACP it is connecting to.

This is a vulnerability in the system as it may fail to detect should a card reader, connected to a legacy ACP, be tampered. The group is unable to confirm this as the ECE IT staff is unable to supply us with information regarding to which ACP (manufacturer, model number) is currently in place right now in ACMS.

3) *Wiegand Protocol*

Further analysis in the access control industry revealed that most of the card readers and numeric keypads, which users will interface with, communicate with the back end Access control panels using the 'Wiegand protocol'. As pointed out by the Wiegand data format document[14], the Wiegand protocol is relatively simple and unencrypted.

No matter how advanced the access control interfaces are, the content gathered were transmitted to the ACP without encryption. The ACMS system is vulnerable to malicious users who have access to the physical wirings behind the access control interfaces. This malicious user could listen on what is being transmitted on the wire and perform replay attacks and cut and splice attacks.

IV. Analysis of Vulnerabilities

After determining the vulnerabilities of the system, two different approaches were used. For the DOS attack and ACP vulnerabilities, potential attacks or solutions to the problem were considered; however, they were not feasible due to the challenges we faced, such as the inability to determine the manufacturers of the ACPs due to security concerns of the ECE IT services as well as the technical challenges that would be involved in executing successful attacks. For the last vulnerability using the Wiegand protocol, a new custom add-on to the card reader and ACP is recommended to protect the communication between these two entities.

A. *DOS Vulnerability*

To launch a DOS attack on the card reader, it requires a signal that is stronger than the key fob's transmission and at the same frequency used by the key fob and the card reader, 13.56 MHz[15]. To execute this attack, one would need a powerful RF signal generator capable of emitting signals at the 13.56 MHz range. There are some low-cost RF signal generators available on the market[16]; however, the output power of these generators may not be powerful enough to affect the key fob and card reader communication channel. More powerful signal generators are quite expensive and the fact that we were not able to get permission to simulate an attack on the card readers limited the group to speculative analysis.

B. *ACP Compatibility Vulnerability*

It is difficult to launch an attack on this vulnerability without the knowledge of the manufacturer of the ACPs and we were not able to acquire permission to use any testbed to attempt to take advantage of this vulnerability. This is understandable due to the nature of the attack because if this is actually vulnerability in the ECE & CS security system, one can potentially combine this attack with the attack against the Wiegand protocol vulnerability to gain access to any access-control-protected entry points. A proposed solution presented in the next section for the Wiegand protocol vulnerability does attempt to deal with this vulnerability as well.

C. *Wiegand Protocol Vulnerability*

This last vulnerability is the most dangerous of them all. By simply sniffing the three-wire connection between the card reader and the ACP when access has been granted to the zone provides the attacker with the 26-bit Wiegand message that can be replayed to gain access to the system. To execute this attack, ideally the attacker would locate both the ACP and the connected card reader. The next step is to locate the three wires that connect the card reader to the ACP. Once the wires have been located, a simple data acquisition microcontroller can be used as a proxy between the two devices.

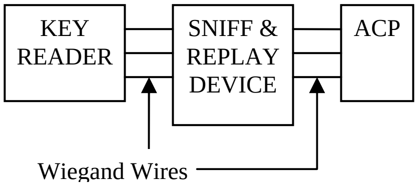

Figure 2 – Wiegand Protocol Vulnerability Attack

As shown in the figure above, the proxy device, labeled as "Sniff & Replay Device", can capture the Wiegand messages so they can be replayed in the future to gain access through the particular entry point.

V. Proposed Solution

A proposed solution to remedy the ACP and this vulnerability is to build an inexpensive add-on device that would connect to both ends of the card reader and the ACP. The device would have tamper sensors to halt communications if the system or the connected card reader is hampered with. The main feature of the device is being able to encrypt the stream of data sent between the access control panels and card readers.

To achieve this capability, the system would have two major hardware components with associated software components. The figure below displays the components: a microcontroller and an FPGA.

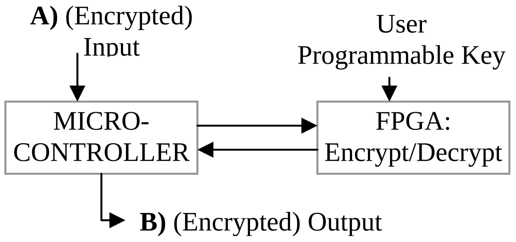

Figure 3 – Wiegand Protocol Vulnerability Proposed Solution

If the device is connected to the card reader, input A would be the unencrypted Wiegand message and the output B would the encrypted output, such as an encrypted stream of data sent via rs232 or serial. Otherwise, when the device is connected directly to the ACP, the input A would be the Encrypted data and the output B would be the original unencrypted Wiegand message.

The microcontroller's purpose would be to convert the communications between the Wiegand message (three wires) into the 26-bit standard format and the encrypted format which could simply be an encrypted stream of data that is sent using a serial connection. The FPGA, will be used to encrypt and decrypt streams of data. FPGAs are used because they are a low-cost and high-performance solution for encryption and decryption. There are several open-source crypto cores, or FPGA designs, available to implement several encryption schemes including AES/Rijndael[17] and Blowfish[18]. The device could potentially utilize the Cipher Feedback (CFB) or Output Feedback (OFB) encryption modes. Thus, there would always be a constant stream of encrypted data sent to and from the card reader and the ACP. Alternatively, if the Wiegand messages are encrypted one at a time, it might be necessary to utilize some asymmetric key exchange model. For the purposes of this report, it is assumed that this particular device will use the OFB or CFB mode of operation.

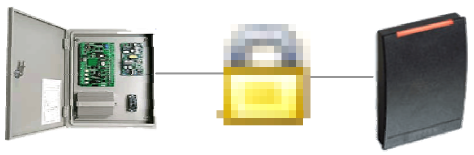

Figure 4 – Secure Wiegand

If this inexpensive device is implemented on the card reader and ACP systems, it would be difficult to sniff the communication between the card reader and the ACP, which would hamper the ability to use the replay attack on the system.

REFERENCES

[1] "ICLASS R40 Reader." 2 Dec. 2005 <http://www.hidcorp.com/pdfs/iclass/iCLASS_R40.pdf>.

[2] RFDump.org. Nov.-Dec. 2005 <http://www.rf-dump.org/>.

[3] Income generated by research ENG. Nov.-Dec. 2005 <http://www.apsc.ubc.ca/research/eng_income2004.html>.

[4] "Demystifying the threat modeling process." Security & Privacy Magazine, IEEE Sept.-Oct. 2005: 66-70.

[5] HID Products - R40 Reader. 2005. HID Corporation. 2 Oct. 2005 <http://www.hidcorp.com/prod_detail.php?prod_id=27>.

[6] Access Control - Weigand Card Reader Interface Standard. 2005. Security Industry Association. 30 Nov. 2005 <http://www.siaonline.org/response.asp?c=storeproduct_42&r=1280>.

[7] "ICLASS R40 Reader." 2 Dec. 2005 <http://www.hidcorp.com/pdfs/iclass/iCLASS_R40.pdf>.

[8] "Understanding Access Control." Nov.-Dec. 2005 <http://www.atiaccess.com/PDFCORPDOCS/Understanding%20Access%20Control.pdf>.

[9] "Wiegand Data Format." Farpointe Data. 29 Nov. 2005 <http://pyramidseries.com/tech-docs/Pyramid-Series-Wiegand-Format-Reference-Document.pdf>.

[10] "Wiegand Data Format." Farpointe Data. 29 Nov. 2005 <http://pyramidseries.com/tech-docs/Pyramid-Series-Wiegand-Format-Reference-Document.pdf>.

[11] "ICLASS Theory." RF IDeas. Nov.-Dec. 2005 <http://www.pcprox.com/Products/ProxCard_Theory/iCLASS Theory/iclasstheory.html>.

[12] "RFID." RFID - Wikipedia, the free encyclopedia. 2 Dec. 2005. 2 Dec. 2005 <http://en.wikipedia.org/wiki/Rfid>.

[13] HID Products - R40 Reader. 2005. HID Corporation. 2 Oct. 2005 <http://www.hidcorp.com/prod_detail.php?prod_id=27>.

[14] Wiegand Data Format. Farpointe Data, Inc. 30 Nov. 2005 <http://www.pyramidseries.com/tech-docs/Pyramid-Series-Wiegand-Format-Reference-Document.pdf>.

[15] "iCLASS Reference Guide." HID. 27 Nov. 2005 <http://www.hidcorp.com/pdfs/products/irg_us.pdf>.

[16] RF Signal Generator SK-303. Transtronics. 1 Dec. 2005 <http://xtronics.com/kits/SK-303.htm>.

[17] Weaver, Nicholas. A High Performance, Compact Rijndael (AES) core for the Virtex Family FPGA. 28 Nov. 2005 <http://www.cs.berkeley.edu/~nweaver/rijndael/>.

[18] Free Blowfish VHDL Core. 28 Nov. 2005 <http://sourceforge.net/projects/blowfishvhdl/>.