[Pla-ce-bo : *Something of no intrinsic remedial value that is used to appease or reassure another*.]

Introduction

I am truly amazed sometimes at how the security industry operates with regards to access control. I am referring not only to the numerous vendors that manufacture security related products but also to the security departments within major corporations whose main function is to protect the physical and intellectual property assets of the company to which they are employed. Simply put, it is a joke!!

As someone who has worked for a major defense contractor for over thirty years I have been able to experience firsthand how many government institutions, defense contractors, and numerous Fortune 500 companies operate with regards to physical access control. Government organizations in general have made many improvements in security since the attack on the New York World Trade Center in 2001 but the commercial industry sector has been much slower to react.

It is the opinion of this author that the lack of effective security in these facilities can be attributed to three main factors:

1. Under-funded Security budgets.
2. A marketplace saturated with "Less-than-adequate" security products
3. Security managers lack of knowledge regarding the vulnerabilities inherent within the products they use.

The exponential growth of the Internet over the last ten years has resulted in a plethora of information being made available about almost any subject of interest. Easy access to detailed technical information has spawned a huge number of hackers who find it a challenge to investigate, discover, and share vulnerabilities that exist with many of the new products and technologies that we interact with on a daily basis. The RFID based products used in access control and security related products in general are a primary target for many of these hackers. To my knowledge there are only a few access control products/technologies on the market today that have not been hacked or compromised to some extent. As a result, virtually all commercial and government facilities which rely on these systems to protect their perimeter security are vulnerable in one way or another. As an example, the iClass contactless smart card technology (manufactured by http://hidcorp.com) has been extensively hacked over the last couple of years yet it continues to maintain a solid presence among end users of access control systems due to the lack of better, more secure solutions.

The Problem

The problem with most access control products today is that they are still being designed to only address the most basic threats. That is, the typical street criminal who might be looking for a simple method to gain access in order to commit a crime. Access control vendors appear to focus their attention on features that are primarily intended to protect against misuse related to lost or stolen cards. There are however bigger and more sophisticated threats to security today and they are very real. Corporate and foreign espionage is more prevalent today than ever before. In addition, the threat of a

insider attack warrants even more concern due to the potentially severe financial implications. The access control products available today due very little to stop a technologically savvy thief from gaining entry to any facility that he (or she) chooses.

In the last couple of decades the access control industry has slowly migrated from using mechanical locks to magstripe technology, to proximity cards, and more recently to smart cards in an attempt to improve physical security. In an effort to add an additional layer of security the use of multi-factor authentication has also recently become standard practice within many organizations. Security vendors today are recommending that access control users should employ a minimum of two of the following authentication mechanisms in order to be secure:

1. Something you have (e.g. Proximity card or smart card)
2. Something you know (e.g. PIN)
3. Something you are (e.g. Fingerprint)

The question that begs asking of course is: "Does implementing multi-factor authentication actually improve security?" The short answer is "Not always".

HID bioCLASS Technology

The HID bioCLASS family of products is an example of one of a more recent technology which supports multi-factor authentication including contactless smart card, fingerprint, and PIN options. The bioCLASS RKLB57 and RWKLB575 are two of the readers within the iClass family that incorporate biometric and PIN capability. A stock photo of the RKLB57 bioCLASS reader is shown below.

Figure 1. RKLB57 bioCLASS reader

According to HID sales brochures: *"HID's bioCLASS readers offer the highest level of security"*

If you were to buy into all of the marketing hype surrounding HID's bioCLASS products you would tend to believe that an access control device that employs smart card technology along with fingerprint

verification and PIN capability must be extremely secure. As a result, how could any criminal (or hacker) ever hope to circumvent all of those high security features?

Based on my testing, it is not all that hard!

The bioCLASS readers are capable of supporting three different modes of authentication including:

- Card Only
- Card + PIN
- Card + Fingerprint
- Card + Fingerprint + PIN

The factory default mode is Card + Fingerprint. The use of any other mode requires that a configuration card be used to put the reader in the new mode.

PIN Security

There have been numerous articles written over the years that address the ineffectiveness of PINs and the numerous ways they can be defeated. There are also quite a few hacker websites that discuss some of the many ways to obtain user PINs. This information is usually targeted towards ATM PIN hacking but the techniques described are equally applicable to access control systems. These techniques include but are not limited to the following:

- Selecting PIN code based on statistical probability of use.
- Covert observation techniques (e.g. hidden Cam).
- Using ultraviolet fingerprint powder to identify pressed keys.
- Thermal imaging to capture residual heat on pressed keys (see Figure 2).
- Monitor keypad communication interface to capture PIN data being sent to backend controller.
- Calculating PIN using reverse engineered PIN generation algorithm.

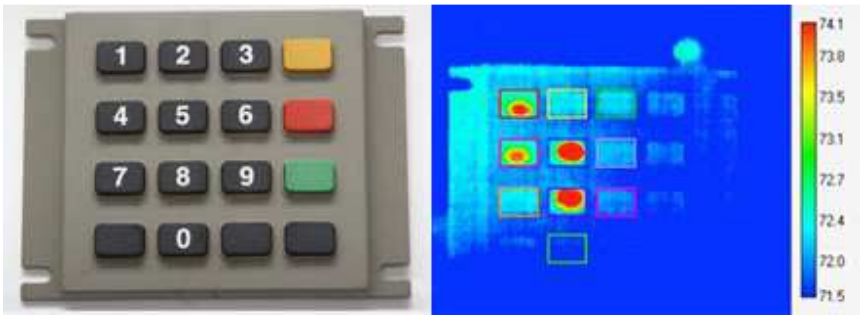

Figure 2. Example showing thermal image of keypad following PIN entry.

In access control systems, the use of PINs have historically been seen as a simple way to prevent unauthorized users from entering a facility in the event that they have somehow obtained a lost or stolen card. Since they do not know the correct PIN, simply having the physical card will not allow them access.

In iClass systems, if the use of a PIN is desired the system administrator has the option of either having the reader itself verify the PIN based on information stored on the card, or he has the option to have the PIN transmitted to the backend controller where it will be verified. Storing the PIN on the smartcard itself is promoted as being a "more secure" solution. I might normally agree with this statement except for one small fact. **"The iClass authentication and encryption keys have previously been hacked!!!"**

If a potential perpetrator has already extracted the iclass keys from an iClass reader (using one of several methods published in various papers) then obtaining the PIN is as simple as reading and decrypting a few data blocks within the iclass card. A dump of the first sixteen data blocks of a typical iClass card is shown below.

```
Blk   Stored Value    Decrypted Value
00  2D801B00F9FF12E0  ----------------
01  12FFFFFF99FFF3C   ----------------
02  D4FEFFFFFFFFFFF   ----------------
03  FFFFFFFFFFFFFFF   ----------------
04  FFFFFFFFFFFFFFF   ----------------
05  FFFFFFFFFFFFFFF   ----------------
06  0000000000100C517 ----------------
07  5E3DDD017D3AE003  0000000005980796
08  2AD4C8211F996871  0000000000000000
09  8E9D32BB53F4564D  1234500000000000
0A  FFFFFFFFFFFFFFF   ----------------
0B  FFFFFFFFFFFFFFF   ----------------
0C  FFFFFFFFFFFFFFF   ----------------
0D  FFFFFFFFFFFFFFF   ----------------
0E  FFFFFFFFFFFFFFF   ----------------
0F  FFFFFFFFFFFFFFF   ----------------

Legend:
PIN Code Length = 5
Wiegand Code =0x5980796 (FC=204, Card No.=00971)
PIN Code = 12345
```

The iclass design supports user defined PIN code lengths of up to ten digits. Five bytes of memory within Block 9 have been reserved to store the normally encrypted PIN code. Information that defines whether a PIN has been stored onto the card along with the length of the stored PIN is stored in a separate byte within Block 6.

In applications that use an iClass card that has a locally stored PIN, the recovery of the PIN may not even be necessary in order to gain access. The reason for this will become evident in the next section where fingerprint hacking techniques are discussed.

bioCLASS Overview

HID bioCLASS readers support the ability to utilize fingerprints as part of the mutual authentication/user verification process. User fingerprints are stored locally on the card instead of sending the fingerprint template to the backend controller and having it perform the verification. According to HID marketing brochures:

"Storing the fingerprint template only on the iCLASS smart card, users benefit from the increased security, faster throughput, easier system management, lower costs for the biometric reader and reduced concerns over individual privacy."

Fingerprint templates initially get stored within the cards EEPROM memory using a process referred to by HID as "User Enrollment". User fingerprint information is enrolled onto a 16K or 32K iClass card by a system administrator who has been granted special card write privileges. System administrator rights are assigned to one or more cardholders during initial startup and configuration of the RKLB57 or RWKLB575 bioClass reader/enroller. A special "Reset" configuration card can also be used to reset the reader back to the factory default state to support the assignment of a different system administrator if necessary. Each user typically enrolls two different fingerprints onto an iClass card. This process allows a second finger to be used during the authentication process in the event that the primary finger cannot be used. A standard 16K iClass card is capable of storing up to two fingerprint templates. The fingerprint templates are stored on a iClass 16K card according to the memory map shown below.

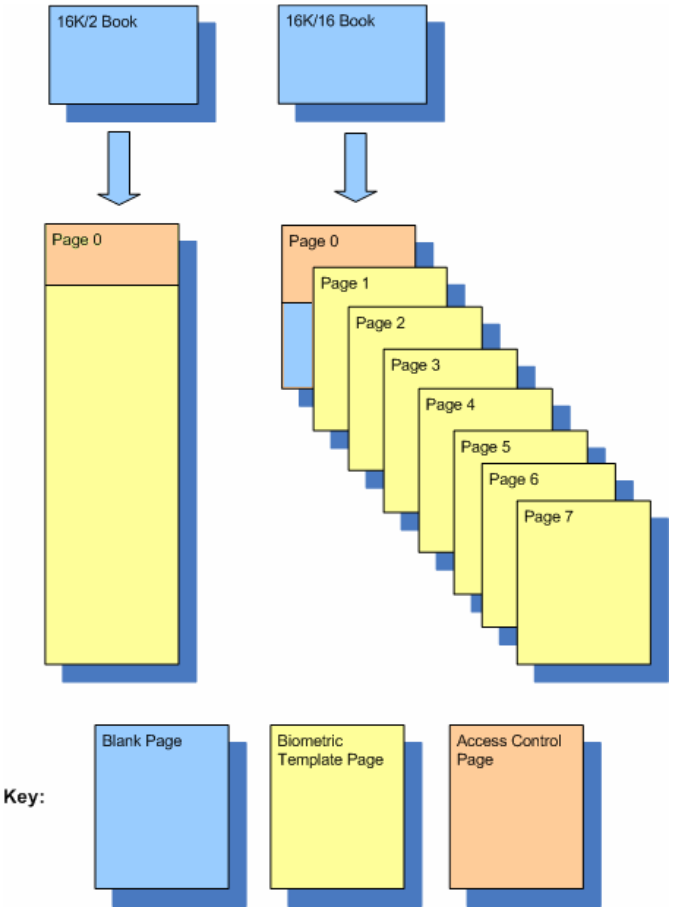

Figure 3. bioCLASS biometric template storage areas.

The process for reading a card and performing user authentication is as follows:

1. The user presents his/her card to the reader. The card is checked to verify that a fingerprint has been enrolled on the card. The bioCLASS reader will not respond to iCLASS cards that do not have a bio template enrolled on to them.
2. If a valid template is stored on the card the reader will read the fingerprint information and card number from the card and place the information into local reader SRAM memory.
3. The user places his/her finger on the reader which then tries to match the fingerprint being presented to the cards fingerprint template recently stored in reader SRAM.
4. If the data from the card matches the data being read from the sensor then the card data (facility code and card number) is transmitted to the backend controller via the wiegand interface. If the card number is accepted by the backend controller the door opens.

The bioCLASS Flaw

Consider the following scenario …..

Bill Smith works for company ABC who's security department has mandated the use of HID bioCLASS readers to secure the doors to several top secret laboratories within their facility. In order for Bill to gain access to the lab two things have to happen. The reader has to perform a fingerprint verification and the backend controller has to perform a verification of the card number. If both are successful, the door opens and Bill is allowed to enter. *Can anyone see the problem here??*

The problem is that the reader is NOT verifying that the fingerprint presented is Bill's. It is simply verifying that the fingerprint presented to the reader is the same as the one stored on the card. If another card holder (e.g. John Doe) were to present a card that had his own fingerprint template enrolled, then the card information read from his card would also be sent to the backend controller. However, since John's card number is probably not in the controllers authorized user database, the door would not open. In this scenario the "High Security" bioCLASS technology is no more secure than any standard proximity card using only single factor card number verification.

Now, what if John Doe somehow learned Bill Smith's card information, maybe in part by reading the card number printed on his card. John could possibly use that information to simply order a pre-programmed card (using Bill's number) from any of the many iclass card sellers found on the web. He would then use his own bioCLASS enroller to put his own fingerprint template on the card. Now when John presents this card to the reader installed on Bill's "High Security" lab door, the fingerprint will validate , the card information will be sent via the wiegand interface, and the backend controller will open the door since it sees Bill's authorized card number.

However, since John is a hacker by trade, he already has the ability to modify HID iClass cards. He simply enrolls his own fingerprint on a new card and then modifies the content of Block 7 to hold whatever wiegand code he needs in order to emulate the appropriate card format, facility code and card number. The same concept could also be applied if Bill's high security lab required the use of a PIN in addition to the fingerprint. The reader DOES NOT verify that the PIN entered is Bill's, it simply verifies that the PIN keyed in by the user is the same PIN that is stored on the card!! So much for multi-factor authentication. In this case it is nothing more than a security placebo.

The example card dump shown below depicts how the reader determines whether a fingerprint template has been enrolled on the card and what privileges have been assigned to the cardholder.

```
Blk   Stored Value    Decrypted Value
00  2D801B00F9FF12E0  ----------------
01  12FFFFFF99FFF3C   ----------------
02  D4FEFFFFFFFFFFF   ----------------
03  FFFFFFFFFFFFFFF   ----------------
04  FFFFFFFFFFFFFFF   ----------------
05  FFFFFFFFFFFFFFF   ----------------
06  0000000001 00C517 ----------------
07  5E3DDD017D3AE003  0000000005980796
08  2AD4C8211F996871  0000000000000000
09  8E9D32BB53F4564D  1234500000000000
0A  FFFFFFFFFFFFFFF   ----------------
0B  FFFFFFFFFFFFFFF   ----------------
0C  FFFFFFFFFFFFFFF   ----------------
0D  FFFFFFFFFFFFFFF   ----------------
0E  FFFFFFFFFFFFFFF   ----------------
0F  FFFFFFFFFFFFFFF   ----------------

Legend:
0x1 Denotes Fingerprint template loaded
Wiegand Code = 0x5980796 (26-bit FC=204, Card No.=00971)
User Rights:0xC Denotes Administrator Privileges
```

Regardless of HID's claims, storing biometric templates and/or PIN information local to a card "DOES NOT" improve security. The fact is, it actually compromises security! The only way to ensure that the PIN and biometric information belongs to the intended user is to store the users information in a secure database that a hacker cannot access. This could either be in a secure reader or on a secure remote server. The card itself cannot be considered a secure database so long as anyone can buy a reader on the open market that allows them to enroll templates and PINs.

Figure 3 below shows two hypothetical iClass access cards from two different companies. The cards belong to two different people with two different fingerprints. Each card has a unique PIN. The two cards do however share the same card number information. When used with a HID bioCLASS reader the two cards are considered to be identical. It is the opinion of this author that this is a fatal design flaw in the bioCLASS architecture. This security loophole is obviously not fully understood by the numerous users who purchased bioCLASS products expecting to strengthen their security through the use of multi-factor authentication.

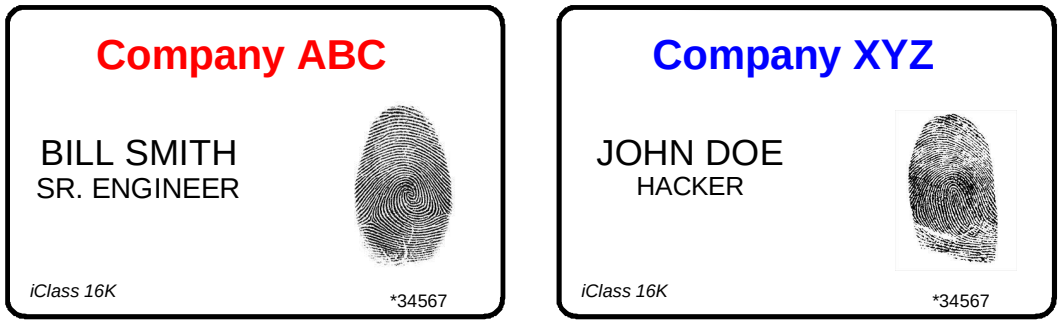

Figure 4. Different cards, yet they are considered identical from the bioCLASS reader and backend controller perspective.

Conclusion

I have attempted to show that the HID bioCLASS technology using two and three factor authentication actually provides very little (if any) extra security over single factor authentication systems . Storing PIN and biometric data local to the card does absolutely nothing to assure that the person requesting access is an authorized user.

To support my claims, I have purchased two different bioCLASS readers on eBay for less than $200. I have demonstrated that I can assign myself administrator privileges and successfully enroll PINs and biometric templates. I did not have to understand the details or complexities of how biometric templates are created or how they are stored. I simply used HID's own tools to circumvent their self-proclaimed "High Security" multi-factor authentication system.

The photo below shows the RKLB57 bioCLASS Reader/Enroller connected to a custom wiegand decoder and display circuit. This setup allowed me to see the information that is normally being sent to the backend controller. I was able to use this setup to confirm that the bioCLASS reader and backend controller could easily be fooled into thinking that two totally different users with two different cards were actually identical. The decision to grant access (or not) is made by the backend controller based solely on the information it receives from the reader. If the reader has been fooled, then the backend controller is basically granting access on the card number alone. This results in a single factor authentication approach that operates no different than the older proximity systems that bioCLASS was originally designed to replace.

Figure 5. HID RKLB57 bioCLASS Reader/Enroller connected to a custom wiegand decoder and display circuit.

Based on this author's own tests, it has been found that circumventing two and three factor authentication is fairly simple and straightforward. The level of difficulty does increase if the system uses a more restricted card format (e.g. Corporate 1000). The level of difficulty increases even more if the system employs the use of high security (HID-Elite) authentication keys. That being said, a persistent hacker might be slowed down but not stopped. I myself have previously demonstrated the ability to penetrate even the most secure iClass systems. I have now added bioCLASS to my list of vulnerable access control products.