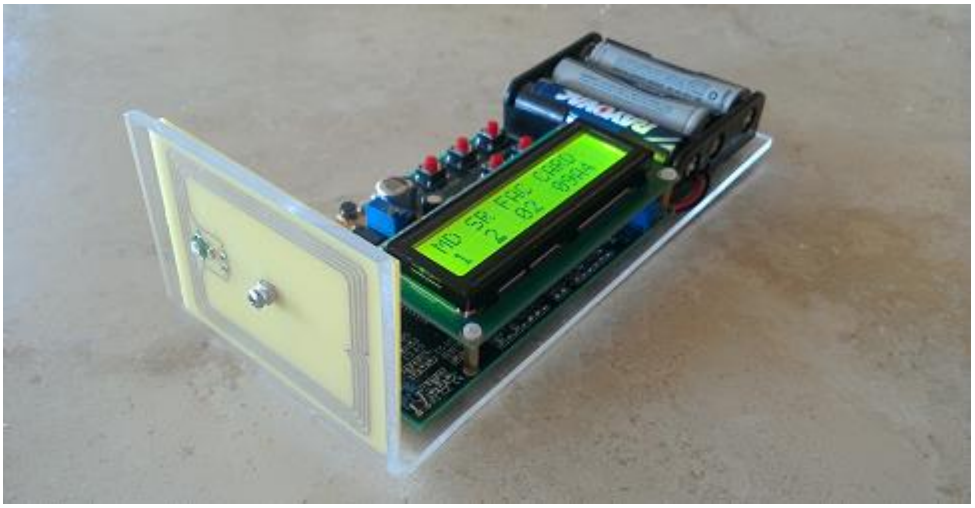
Spoofing iClass and iClass SE



Introduction

The concept of emulating (spoofing) security access cards has become more and more difficult with the introduction of smart card technology. The older proximity based RFID access cards were much easier to spoof since they were only required to transmit a single unique identifier code whenever they entered the electromagnetic field of the reader. Smart cards however contain sufficient processing resources to allow them to interact with a reader using significantly more sophisticated communication protocols, thereby increasing the overall security of the system where they are being used. These communication protocols typically involve the use of complex proprietary algorithms that are not readily available in the public domain. In order to replicate the operation of a specific smart card these algorithms must first be obtained through other means such as reverse engineering.

There are quite a few smart card technologies being used throughout the world today that are targeted to security access control applications. This paper focusses exclusively on the iClass smart card technology which is manufactured by HID Global Corporation. The iClass brand of access control products currently holds the largest U.S. market share of all the smart card based access control systems that are in use today. As a result of its popularity, extensive analysis of iclass has been done over the last few years by various security researchers around the world. This research has resulted in multiple technical papers being published. These papers have provided significant insight into the overall operation of iclass and the various secure algorithms that it employs.

This author has attempted to leverage the extensive suite of iClass information published to date in an attempt to determine whether a simple iclass spoofer circuit could be built. To be considered successful, this circuit would be required to emulate virtually any legacy iClass credential that is in use today, regardless of the format being used and whether it was being used in a standard security system or a high security system. The result of my testing indicated that not only was it possible, but that the spoofer could also be made to operate with the newer " iClass SE" family of readers that was recently introduced by HID as a replacement for the previously hacked legacy iClass devices.

iClass versus iClass SE

The original iClass technology, herein after referred to as "legacy" iClass, has been around since approximately 2002. The legacy iclass technology was successfully hacked in 2010 which exposed the iclass reader firmware, Master authentication key and Master encryption keys. By leveraging this information, the hacker community now possessed the ability to read and write data stored on any standard security iclass credential. Since the stored data was not bound to any particular cards serial number, it was demonstrated that a clone card could be made simply by copying the content of one card over to a second card.

In an attempt to address some of the security vulnerabilities in the legacy iclass design, HID released an updated version of the iclass technology (termed iclass SE) in the 2011 timeframe. The “SE” term referred to HIDs new Secure Identity Object (SIO) or “SIO Enabled (SE)” technology. The access control payload (wiegand code, PIN, password, etc.) was now being placed in a secure data wrapper that also included the cards serial number information, effectively binding the information stored on a card to that specific card. The ability to copy the information from one card over to another card was no longer possible. In addition to incorporating the new SIO technology, new Master Authentication and encryption keys were also assigned.

However, since a huge user base already existed for the legacy iclass, a need was recognized to also provide backwards compatibility with those existing products. This forced HID to offer SE card and reader variants that were able to support both the legacy and SIO credential formats.

[It should be noted that this decision to provide support for legacy products introduces a significant security vulnerability that can be exploited to support iClass SE credential spoofing. Details of this vulnerability are discussed in a later section of this paper.]

The three types of iClass credential types currently be offered can be summarized as follows:

- Legacy iClass: This credential supports the original access control payload and utilizes a key that was diversified from the legacy master authentication key. (See table below)
- iClass SE: This credential contains a single SIO access control payload and utilizes a key that is diversified from the new SE master authentication key. (See table below)
- iClass SR: This credential contains two access control payloads (legacy and SIO). The SR credentials utilize a key that is diversified from the legacy master authentication key.

iClass Credential Types					
Legacy iClass		**iClass SE**		**iClass SR (SIO Ready)**	
Blk		Blk		Blk	
0	Serial Number	0	Serial Number	0	Serial Number
1	Configuration Block	1	Configuration Block	1	Configuration Block
2	e-purse	2	e-purse	2	e-purse
3	Debit Key	3	Debit Key	3	Debit Key
4	Credit Key	4	Credit Key	4	Credit Key
5	Application Issuer Area	5	Application Issuer Area	5	Application Issuer Area
6-9	Application 1 Access Control Payload	6-12	Application 1 Secure Identity Object	6-9	Application 1 Access Control Payload
10-18	Unused – Application 1	13-18	Unused – Application 1	10-16	Application 1 Secure Identity Object
19-31	Application 2	19-31	Application 2	17-18	Unused - Application 1
				19-31	Application 2

All of the above card types are based on the same PicoPass smart card with the only difference being what is actually programmed into the various data blocks of the card.

The iclass reader is able to identify the type of card that it is interacting with by first reading the Application Issuer Data value stored in Block5. The information contained in this data block indicates whether the reader should interpret the data payload as legacy or SIO. It also tells the reader whether authentication should be performed using the legacy Master Authentication key or the newer SE authentication key.

Access Control Payload Examples

The following table includes data dumps from three actual iClass SR cards that have contiguous card numbers. The access control information stored on each card is replicated within the legacy payload data blocks (6-9) and the SIO data blocks (10-16).

iClass SR Credentials – Sample Data Dumps

Dual Payload [Legacy iClass = Red; iClass SE (SIO) = Blue]

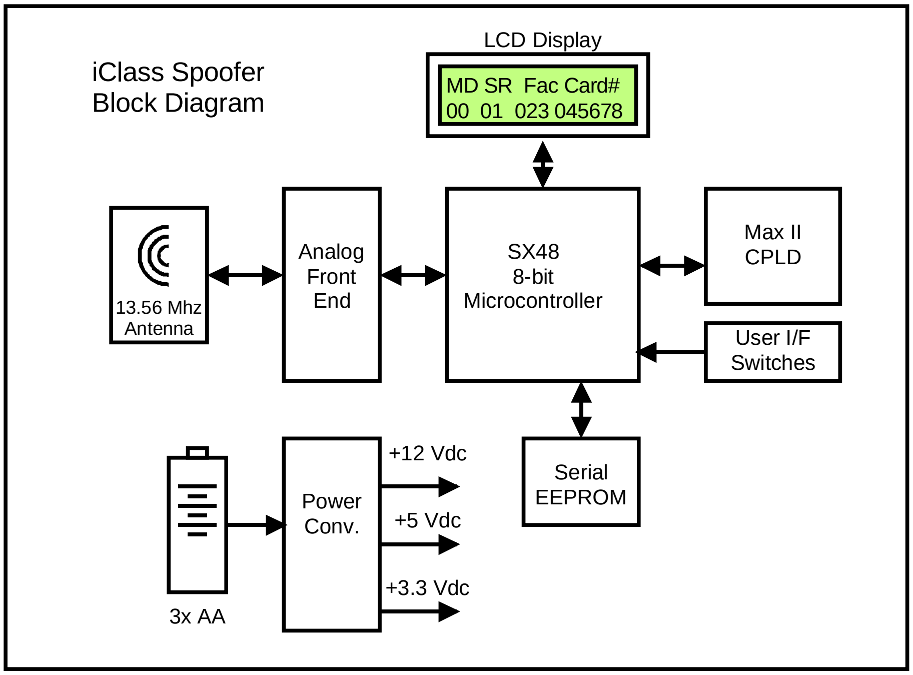
Blk	Sample Card #1 Fac=177 Card=32768
0	87CDCA01F9FF12E0
1	12FFFFFF7F1FFF3C
2	FEFFFFFFFFFFFFFF
3	FFFFFFFFFFFFFFFF
4	FFFFFFFFFFFFFFFF
5	FFFFFFFFFFFFFFFF
6	A30303030003E017
7	0342D14788F4C479
8	2AD4C8211F996871
9	2AD4C8211F996871
10	3031810401A47101
11	A5020500A6088101
12	010403030009A717
13	8515E8B969E62C75
14	8EA0D90ACF4F00F0
15	A89B91721DFF64A9
16	0205000500000000
17	FFFFFFFFFFFFFFFF
18	FFFFFFFFFFFFFFFF
19	FFFFFFFFFFFFFFFF
20	FFFFFFFFFFFFFFFF
21	FFFFFFFFFFFFFFFF
22	FFFFFFFFFFFFFFFF
23	FFFFFFFFFFFFFFFF
24	FFFFFFFFFFFFFFFF
25	FFFFFFFFFFFFFFFF
26	FFFFFFFFFFFFFFFF
27	FFFFFFFFFFFFFFFF
28	FFFFFFFFFFFFFFFF
29	FFFFFFFFFFFFFFFF
30	FFFFFFFFFFFFFFFF
31	FFFFFFFFFFFFFFFF

Blk	Sample Card #2 Fac=177 Card=32769
0	86CDCA01F9FF12E0
1	12FFFFFF7F1FFF3C
2	FEFFFFFFFFFFFFFF
3	FFFFFFFFFFFFFFFF
4	FFFFFFFFFFFFFFFF
5	FFFFFFFFFFFFFFFF
6	A30303030003E017
7	505292356040E44B
8	2AD4C8211F996871
9	2AD4C8211F996871
10	3031810401A47102
11	A5020500A6088101
12	010403030009A717
13	8515BE2F6863ADAD
14	AC1CA881FA69B46F
15	445204261BF024A9
16	0205000500000000
17	FFFFFFFFFFFFFFFF
18	FFFFFFFFFFFFFFFF
19	FFFFFFFFFFFFFFFF
20	FFFFFFFFFFFFFFFF
21	FFFFFFFFFFFFFFFF
22	FFFFFFFFFFFFFFFF
23	FFFFFFFFFFFFFFFF
24	FFFFFFFFFFFFFFFF
25	FFFFFFFFFFFFFFFF
26	FFFFFFFFFFFFFFFF
27	FFFFFFFFFFFFFFFF
28	FFFFFFFFFFFFFFFF
29	FFFFFFFFFFFFFFFF
30	FFFFFFFFFFFFFFFF
31	FFFFFFFFFFFFFFFF

Blk	Sample Card #3 Fac=177 Card=32770
0	94CCCA01F9FF12E0
1	12FFFFFF7F1FFF3C
2	FEFFFFFFFFFFFFFF
3	FFFFFFFFFFFFFFFF
4	FFFFFFFFFFFFFFFF
5	FFFFFFFFFFFFFFFF
6	A30303030003E017
7	5F00C2A64207805D
8	2AD4C8211F996871
9	2AD4C8211F996871
10	3031810401A47103
11	A5020500A6088101
12	010403030009A717
13	8515BDEB67A8AA4F
14	A7C6E56D84073D88
15	C1D8BD2860C23CA9
16	0205000500000000
17	FFFFFFFFFFFFFFFF
18	FFFFFFFFFFFFFFFF
19	FFFFFFFFFFFFFFFF
20	FFFFFFFFFFFFFFFF
21	FFFFFFFFFFFFFFFF
22	FFFFFFFFFFFFFFFF
23	FFFFFFFFFFFFFFFF
24	FFFFFFFFFFFFFFFF
25	FFFFFFFFFFFFFFFF
26	FFFFFFFFFFFFFFFF
27	FFFFFFFFFFFFFFFF
28	FFFFFFFFFFFFFFFF
29	FFFFFFFFFFFFFFFF
30	FFFFFFFFFFFFFFFF
31	FFFFFFFFFFFFFFFF

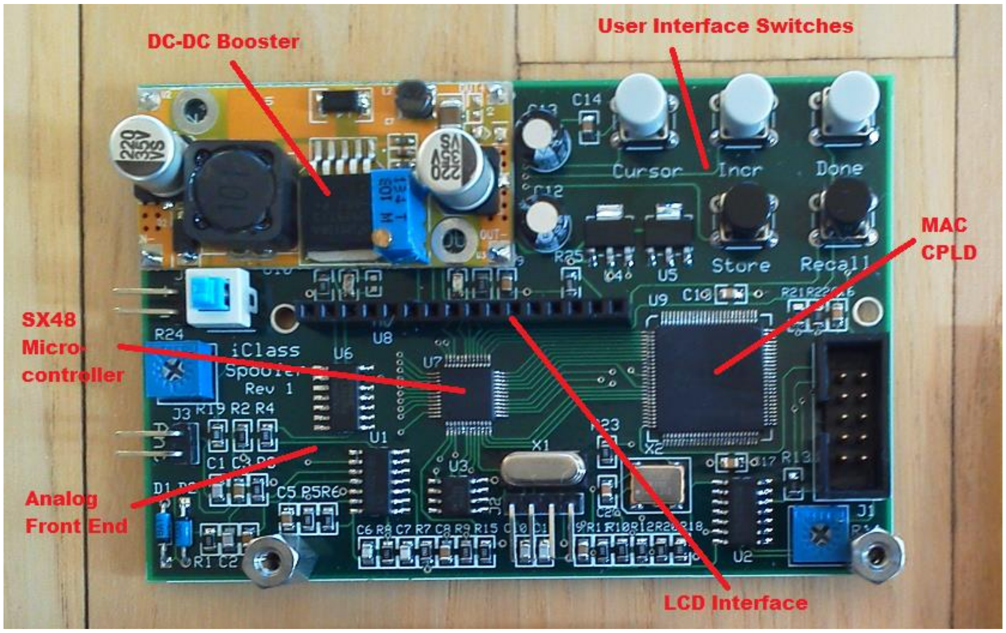
Spoofer Design Implementation

In order to emulate (spoof) an iclass smart card, a customized circuit had to be developed that would perform the functions normally handled by the Inside Secure PicoPass chip that is embedded inside every iclass credential. A high level block diagram of the spoofer design is shown in the figure below.



iClass Spoofer Block Diagram

The Parallax SX48 microcontroller is the heart of the spoofer circuit. It performs multiple roles including handling all ISO 15693 communication with the reader, CRC calculations, maintaining and updating all credential payload information, driving the LCD display and managing all user inputs. The MAXII CPLD is responsible for generating all message authentication codes (MACs) that are used during the mutual authentication between the iclass reader and the emulated credential. A small serial EEPROM memory device is used to store a collection of user defined card identities (e.g. wiegand codes).
A photo of the spoofers printed circuit board is shown below.



Spoofer Operation

The spoofer circuit was designed to be capable of emulating any iclass credential. However, to simplify the development of the initial prototype unit , the firmware currently only supports the HID H10302 26-bit card formats. The emulation of other card formats (e.g. 35-bit Corporate 1000) would require a firmware update but no changes to the underlying hardware.

During communication with an iclass reader, the spoofer circuit utilizes a fixed CSN value and diversified key that allows it to authenticate with any standard security reader. In order to function within a high security / Elite system the diversified key (stored in firmware) must be modified to a value based on the particular high security key being used.

The design supports four different modes of operation as follows:

1. Setup Mode – This mode allows a user to define the card parameters (e..g. Facility Code & Card Number) that are to be used when interacting with a reader. The card parameters can also be stored or recalled to/from memory to simplify user operation.
2. Fixed Credential Mode – This mode is selected when a fixed set of card parameters is to be used during interaction with the reader. When operating in this mode the same facility code and card number will be sent to the reader during every Block 7/8/9 read request.
3. Incrementing Facility Code – When operating in this mode the facility code of the credential being emulated will be incremented after each Block 7/8/9 read . This mode can be used to try a set of sequential facility codes when the user does not have knowledge of the facility code being used in a particular system.
4. Incrementing Card Number – When operating in this mode the card number of the credential being emulated is incremented after each Block 7/8/9 read request. This mode can be used to emulate a series of credentials with card numbers that are within a particular range.

Spoofer / Reader Communication

To emulate an iclass credential the operator simply powers on the spoofer unit, enters the desired card parameters, presses the “Done Setup /Run” button and then places the spoofer unit near the reader. The spoofer will initiate communication with the reader just like a legitimate iclass credential .

The tables shown below depict the communication sequence that occurs between the reader and spoofer when interacting with both a legacy iclass reader and a newer iClass SE reader that supports both SIO and legacy interpreters.
It should be noted that the spoofer circuit does not currently support operation with iClass SE readers that contain only the SIO interpreter and use the optional “Standard Security 2” keyset.
However, iClass SE credentials that have a single SIO payload can still be spoofed by fooling the reader into thinking it is talking to an SR card. The SIO payload (copied from the SE credential) is placed in Blocks 10-16 of an emulated (virtual) SR card where its data payload will now be read by the reader using the old legacy “Standard Security 1” keyset.

[Note: To simplify the spoofer design, encrypted communication between the reader and spoofer has been disabled via Blk 6. This is an iclass option that is neither documented nor acknowledged by HID.]

iClass Spoofer Communication Sequence (Legacy iCLASS Reader 6100CKNN0000)

Instruction	iClass Reader / Spoofer	Comment
ACTALL	0A	Rdr asks all cards present to respond
	SOF	Resp indicates that the spoofer is present
IDENTIFY	0C	Rdr asks for anti-collision serial no.
	20 40 60 20 FF 5F 02 1C F2 01	Spoofer responds with ACSN + CRC
SELECT	81 20 40 60 20 FF 5F 02 1C	Rdr asks for CSN
	00 01 02 03 F9 FF 12 E0 54 F1	Spoofer responds with CSN + CRC
SELECT	81 00 01 02 03 F9 FF 12 E0	Rdr asks for CSN
	00 01 02 03 F9 FF 12 E0 54 F1	Spoofer responds with CSN + CRC
PAGE SELECT	84 00 73 33	Reader specifies Page 0
	No Response	Chips with single page do not answer
READCHECK	88 02	Rdr asks for Blk2 data
	FE FF FF FF FF FF FF FF 55 74	Spoofer responds with e-Purse + CRC
CHECK	05 N0 N1 N2 N3 M0 M1 M2 M3	Rdr initiates Auth with Nonce + 1st half of MAC
	M4 M5 M6 M7	Spoofer responds with 2nd half of MAC
UPDATE	87 02 FD FF FF FF FF FF FF FF C9 C9 FE 16	Rdr initiates e-purse update with crypto signature
	FD FF FF FF FF FF FF FF 85 FE	Spoofer responds with new e-purse value + CRC
READ	0C 01 FA 22	Rdr asks for Blk1 data (Configuration Block)
	12 FF FF FF 7F 1F FF 3C 8C 87	Spoofer responds with Blk1 data + CRC
READ	0C 06 45 56	Rdr asks for Blk6 data
	03 03 03 03 00 03 E0 14 D8 11	Spoofer responds with Blk6 data + CRC
READ	0C 07 CC 47	Rdr asks for Blk7 data
	00 00 00 0C 64 61 52 9B 3B 7B	Spoofer responds with Blk7 data + CRC
READ	0C 08 3B BF	Rdr asks for Blk8 data
	00 00 00 00 00 00 00 00 8F 72	Spoofer responds with Blk8 data + CRC
READ	0C 09 B2 AE	Rdr asks for Blk9 data
	00 00 00 00 00 00 00 00 8F 72	Spoofer responds with Blk9 data + CRC
ACTALL	0A	Above Seq repeats while card present

iClass Spoofer Communication Sequence (iCLASS SE Reader P/N 920NTNNEK00000)

Instruction	iClass Reader / Spoofer	Comment
ACTALL	0A	Rdr asks all cards present to respond
	SOF	Resp indicates that the spoofer is present
IDENTIFY	0C	Rdr asks for anti-collision serial no.
	20 40 60 20 FF 5F 02 1C F2 01	Spoofer responds with ACSN + CRC
SELECT	81 20 40 60 20 FF 5F 02 1C	Rdr asks for CSN
	00 01 02 03 F9 FF 12 E0 54 F1	Spoofer responds with CSN + CRC
READ	0C 05 DE 64	Rdr asks for Blk5 data (to determine if SE card)
	FF FF FF FF FF FF FF FF EA F5	Spoofer responds with Blk5 data + CRC
READCHECK	88 02	Rdr asks for Blk2 data
	FE FF FF FF FF FF FF FF 55 74	Spoofer responds with e-Purse + CRC
CHECK	05 N0 N1 N2 N3 M0 M1 M2 M3	Rdr initiates Auth with Nonce + 1st half of MAC
	M4 M5 M6 M7	Spoofer responds with 2nd half of MAC
UPDATE	87 02 FD FF FF FF FF FF FF FF C9 C9 FE 16	Rdr initiates e-purse update with crypto signature
	FD FF FF FF FF FF FF FF 85 FE	Spoofer responds with new e-purse value + CRC
READ	0C 06 45 56	Rdr asks for Blk6 data
	03 03 03 03 00 03 E0 14 D8 11	Spoofer responds with Blk6 data + CRC
READ4	06 06 45 56	Rdr asks for Blk 6/7/8/9 data
	No Response	Spoofer ignores request (Read4 not supported)
READ	0C 06 45 56	Rdr asks for Blk6 data
	03 03 03 03 00 03 E0 14 D8 11	Spoofer responds with Blk6 data + CRC
READ	0C 07 CC 47	Rdr asks for Blk7 data
	00 00 00 0C 64 61 52 9B 3B 7B	Spoofer responds with Blk7 data + CRC
READ	0C 08 3B BF	Rdr asks for Blk8 data
	00 00 00 00 00 00 00 00 8F 72	Spoofer responds with Blk8 data + CRC
READ	0C 09 B2 AE	Rdr asks for Blk9 data
	00 00 00 00 00 00 00 00 8F 72	Spoofer responds with Blk9 data + CRC
ACTALL	0A	Above Seq repeats while card present

Summary

I have attempted to provide a high level overview of a functional iclass spoofer device. This device has been tested on multiple iClass and iClass SE readers to verify its capability to emulate all types of iclass credentials. The prototype circuit however does not yet work with iClass SE readers that utilize the HID "Standard Keyset 2" option since that authentication key is not yet known within the hacker community.

The basic concept of spoofing allows a hacker the ability to possess a virtual set of keys that are capable of circumventing any system that employs this smart card technology in its access control system. Since the iclass authentication and crypto algorithms were compromised several years ago, the migration to using a Secure Identity Object (SIO) in the newer iClass SE family has successfully eliminated the ability to clone data from one card to another but it has done very little to prevent the type of card spoofing attack that has been addressed herein.