I, Cat

TUESDAY, SEPTEMBER 23, 2008

Laundry Part 3

Let's recall from last time: we're studying an Atmel AT88SC0404C ("CryptoMemory") in smart card form factor. We can communicate with it via a serial bus compatible with a regular PC serial port. We identified it using the Answer-to-Reset string, which ISO 7816 specifies all such cards must send when brought out of reset. Now we want to poke around the card a bit, hopefully doing something like reading the card's balance.

From this point on, the AT88SC0404C datasheet is an essential part of our work. At the very least, it's important to quickly scan it to get an idea of how the device works. There's a couple of tables you'll find yourself referring to fairly often:

- Figure 4-10 (AT88SC0104C, 0204C, 0404C Configuration Memory) on page 14;
- Table 8-2 (CryptoMemory Asynchronous Command Set) on page 41;
- Table 8-3. Asychronous Mode Return Status Definitions.

The chip has some fuses that provide chip-level protection. Let's try to read the fuse status byte:

```
ATR 3b b2 11 00 10 80 00 04
--> 00 b6 01 00 01
<-- (b6) 20 [90 00]
```

That `(b6)` is the INS byte (command) sent back to us, the `20` is the fuse byte, and the trailing `[90 00]` is the status code. According to the datasheet (page 24), this means that all fuses have been blown.

The AT88SC0404C has a great deal of configuration memory (256 B); let's try to dump it using the "Read Config Zone" command. Keep in mind that bytes that we don't have rights to read will appear as 20 (the fuse byte):

```
ATR 3b b2 11 00 10 80 00 04
--> 00 b6 00 00 f0
<-- (b6) 3b b2 ... 20 20 [69 00]
```

Here's the data, formatted for comparing with the configuration zone map on page 14 (and with potentially identifying data removed):

```
000000 3b b2 11 00 10 80 00 04
000008 40 40 ff ff ff ff ff ff
000010 69 x2 08 x2 28 x0 40 x0
000018 bf 00 00 00 x0 x5 xd xb
000020 df 08 df 08 df 58 df 58
```

About Me

Catalin Patulea
Ottawa, Canada
My Home Page

More...

Blog Archive

- ► 2010 (1)
- ► 2009 (6)
- ▼ 2008 (9)
  - ► November (3)
  - ► October (1)
  - ▼ September (1)
    - Laundry Part 3
  - ► July (1)
  - ► January (3)
- ► 2004 (12)

```
000028 ff ff ff ff ff ff ff ff
000030 ff ff ff ff ff ff ff ff
000038 ff ff ff ff ff ff ff ff
000040 ff ff ff ff ff ff ff ff
000048 ff ff ff ff ff ff ff ff
000050 ff 5d ae 47 5a 06 51 db
000058 20 20 20 20 20 20 20 20
000060 ff ff ff ff ff ff ff ff
000068 20 20 20 20 20 20 20 20
000070 ff ff ff ff ff ff ff ff
000078 20 20 20 20 20 20 20 20
000080 ff ff ff ff ff ff ff ff
000088 20 20 20 20 20 20 20 20
000090 20 20 20 20 20 20 20 20
000098 20 20 20 20 20 20 20 20
0000a0 20 20 20 20 20 20 20 20
0000a8 20 20 20 20 20 20 20 20
0000b0 ff 20 20 20 ff 20 20 20
0000b8 ff 20 20 20 ff 20 20 20
0000c0 ff 20 20 20 ff 20 20 20
0000c8 ff 20 20 20 ff 20 20 20
0000d0 ff 20 20 20 ff 20 20 20
0000d8 ff 20 20 20 ff 20 20 20
0000e0 ff 20 20 20 ff 20 20 20
0000e8 88 20 20 20 ff 20 20 20
0000f0 end
```

Let's take a look at some of the interesting fields and their values:

- Offset 18h - DCR = BFh
- Offset 19h - Identification Number Nc = "00 00 00 x0 x5 xd xb"
- Offset 20h - AR0 = DFh
- Offset 21h - PR0 = 08h
- Offset 22h - AR1 = DFh
- Offset 23h - PR2 = 08h
- Offset 24h - AR2 = DFh
- Offset 25h - PR2 = 58h
- Offset 26h - AR3 = DFh
- Offset 27h - PR3 = 58h
- Offset 50h - Reserved for Authentication and Encryption = "ff 5d ae 47 5a 06 51 db"
- Offset E8h - PAC = 88h

The DCR value is the Device Configuration Register and the meaning of its bits are explained in detail in section 5.3.8. The conclusion is that the Write 7 password (master password) has been disabled, "Unlimited Checksum Reads" is asserted, "Unlimited Authentication Trials" are not allowed and we are only allowed 4 incorrect password attempts before the device locks itself out in hardware, permanently. (Be careful not to "brick" your card!)

Next, we have an Identification Number that varies according to the number on the back of the card. It's not quite the same number, but the value of Nc does increase by 1 per every increment of the number of the back (i.e., it's just an offset).

The Access Registers are a bit more interesting. The AR values have PM(1:0)="11", meaning "no password", but since AM(1:0)="01", this means the cryptographic authentication protocol is in effect. "Encryption Required" is set to 1, which appears to mean deasserted. The rest of the bits aren't too interesting.

The Password Registers tell us that the device's user memory is split into two areas, accessed by different passwords/keys. The first half uses AK(1:0)="00" and POK(1:0)="00" and the second half uses AK(1:0)="01" and POK(1:0)="01".

The next part appears to be "Cryptograms" (section 5.3.12). This is most likely part of the cryptographic authentication protocol. The first page of the datasheet states that the chips use a "64-bit Mutual Authentication Protocol" under license from ELVA. If you look them up, they appear to be a French company that has filed patents on the topic to the US Patent Office: Method of enabling a server to authorize access to a service from portable... The patent makes reference to various cryptograms that get shuffled around to validate the identity of the device and/or host. Of course, the patent omits the details truly valuable to an implementation or for cryptoanalysis. (Okay, fine, I didn't read it all. If anyone finds and juicy details, please post!)

The very last field we can look at is the Password Attempts Counter for the Write 7 password. Because I attempted to validate the Write 7 password a couple times, this counter has decreased to 88h. This means I only have one attempt before the card locks itself out completely. Ouch! Don't do this at home!

Well, that's about it for now. I ordered a kit from Atmel that includes all the libraries, in binary format, needed to use the cryptographic authentication protocol. When I have something new to report, rest assured you'll be the first to know. Until then, 73.

-Cat

Posted by Catalin Patulea at 11:04 pm

12 comments:

Anonymous said...

Aha! I had all but given up on the continuation of the laundry saga.. Well done :)

24 September 2008 at 23:18

Anonymous said...

You should take a look at this thread:
http://www.hackerthreads.org/phpbb/viewtopic.php?f=17&t=4785

There seems to have been some decent work done, but it was apparently abandoned. Looking forward to seeing how your work pans out.

1 October 2008 at 23:11

Chris **said...**

This is great, I am using the exact same smart card and also wish to crack it. Keep up the great work :)

24 October 2008 at 00:57

Chris **said...**

I'll pay you $50 to $100 if you find a way to get this going so I can make backup copies of my laundry card :P. I am using the exact same one you had a picture of in a previous post. Please please get this going, the laundry people here have raised the prices twice over the past month.

Please contact me - chris at ilikeforums.com

24 October 2008 at 21:12

Anonymous said...

One suggestion to you, I've seen people make devices that appear as a smart card reader, they stick the device into the laundry machine or whatever, then they copy the command issued to their computer since the card really isn't a card, just a chip with wires connecting back to the computer. The computer records the commands so you can then use those commands to issue to the card through your card reader. Then the card responds etc, then finally you get to the point where it's unlocked... idk if this can really be done, just an idea.

24 October 2008 at 21:33

Chris **said...**

Any news on part 4?

13 November 2008 at 21:49

Anonymous said...

Still no part 4 :-(

25 May 2010 at 22:55

svg1234 **said...**

"The AT88SC0404C has a great deal of configuration memory (256 KB);"

256 *BYTES* - not kilobytes.

5 July 2011 at 03:50

Catalin Patulea said...

You're absolutely right svg1234 - fixed.

5 July 2011 at 13:34

Anonymous said...

Did it work ??? Any updates ..

28 April 2012 at 13:31

Catalin Patulea said...

Sorry Anonymous - nothing new to report. How about you? Anyone else have information about this card?

29 April 2012 at 17:15

Anonymous said...

I know this is an old thread and you've likely all but moved on but I figured I'd comment to see what I could find. Any progress?

12 June 2014 at 21:15

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)