Security Vulnerability Report

SE-2011-01 Issues #22-23

[cumulative report]

2011 Security Explorations. All Rights Reserved.

DISCLAIMER

INFORMATION PROVIDED IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW NEITHER SECURITY EXPLORATIONS, ITS LICENSORS OR AFFILIATES, NOR THE COPYRIGHT HOLDERS MAKE ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE INFORMATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS, OR OTHER RIGHTS. THERE IS NO WARRANTY BY SECURITY EXPLORATIONS OR BY ANY OTHER PARTY THAT THE INFORMATION CONTAINED IN THE THIS DOCUMENT WILL MEET YOUR REQUIREMENTS OR THAT IT WILL BE ERROR-FREE.

YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE SELECTION AND USE OF THE INFORMATION TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE INSTALLATION, USE, AND RESULTS OBTAINED FROM IT.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL SECURITY EXPLORATIONS, ITS EMPLOYEES OR LICENSORS OR AFFILIATES BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, DATA, OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY, INTERRUPTION OF BUSINESS, LOSS OF BUSINESS INFORMATION, OR FOR ANY SPECIAL, DIRECT, INDIRECT, INCIDENTAL, ECONOMIC, COVER, PUNITIVE, SPECIAL, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, TORT, NEGLIGENCE, OR OTHER THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE INFORMATION CONTAINED IN THIS DOCUMENT, EVEN IF SECURITY EXPLORATIONS OR ITS LICENSORS OR AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THIS PUBLICATION COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS.

2011 Security Explorations. All Rights Reserved.

This report presents information related to security vulnerabilities discovered by Security Explorations in Conax Conditional Access System (CAS). Below, we provide a brief summary of them as originally[1] reported to the vendor.

[Issue #22 – Conax entitlements' evaluation flaw]

There is a security vulnerability in the implementation of entitlements evaluation algorithm used by the Conax card. We found out that entitlements stored in a subscriber's card and corresponding to some past subscription period are also taken into account when it comes to processing of ECM messages (encrypted messages containing Control Words information) from the current period.

We successfully verified that Conax card used by the polish digital satellite TV platfom N successfully released Control Words for a Video on Demand movie, regardless of the fact that the entitlement period for the movie indicated past subscription period.

The description below is based upon the most recent test that was conducted on 21 Dec 2011 and that in particular illustrates the existence of reported Issue #22. This test makes use of commands executed in the environment of ITI5800SX set-top-box device (Platform 'N's DVR set-to-box device with HDD and Push VOD capability). The commands were executed in the environment of a shell that's been spawned on a target device. This shell is actually our Proof of Concept code as described on SE-2011-01 project webpages.

First, "sysinfo" command is issue in the environment of the PoC shell in order to verify the target set-top-box device to which other commands would be later issued.

```
box> sysinfo
[system info]
- boxtype                  ITI5800SX (nBox HDTV Recorder)
- serial #                 BZZBXXXXXXXXXXXXX
- hw version               178.179:69
- sw version               4.b5a 29
- sw dnld time             Thu Aug 18 22:41:32 CEST 2011
- MHP ver                  MHP 1.1.1 v4467_6 RELEASE
- mac addr                 00:03:91:c7:35:cc
```

Next, "subsinfo" command is issed in order to check current Conax entitlements of a set-to-box subscriber:

```
box> subsinfo
- "ITI Neovision  "
   01.12.2011 - 31.12.2011  0x01df643b
                          - Informacja i rozrywka
                          - Kultura, Nauka, Swiat
                          - Dzieci
                          - Style, Moda, Muzyka
                          - Hity filmowe
   01.11.2011 - 30.11.2011  0x01df643b
                          - Informacja i rozrywka
                          - Kultura, Nauka, Swiat
                          - Dzieci
                          - Style, Moda, Muzyka
```

[1] Description of Issue 22 was extended for the purpose of this report.

2011 Security Explorations. All Rights Reserved.

```
                          - Hity filmowe
- "ITI VOD 1       "
   01.12.2011 - 31.12.2011  0x01000001
   01.11.2011 - 30.11.2011  0x01000001
- "ITI VOD 2       "
   01.12.2011 - 31.12.2011  0x01000000
   01.11.2011 - 30.11.2011  0x01000382
- "ITI VOD 3       "
   01.10.2011 - 31.10.2011  0x01004000
   01.03.2010 - 31.03.2010  0x01002000
- "ITI 2 Neovision"
   01.12.2011 - 31.12.2011  0x01000061
   01.11.2011 - 30.11.2011  0x01000021
```

The entitlements for "ITI VOD 2 " provider name are of particular interest here. As ilustrated above, the entitlement for a time period of Dec 2011 points to the value of 0x01000000 (rather empty entitlement set). However, the entitlement set for a previous time period (Nov 2011) points to a non-empty value of 0x01000382.

Conax entitlements denote subscriber's access rights to a given programming. Provider name denotes the provider of a given content. 32-bit entitlement value represents the actual access rights to the content. Each bit value denotes whether a given programming package or VOD content can be accesses (1) or not (0).

Below, a command is issued in order to find out the meaning of the bits from the entitlement value of 0x01000382.

```
box> jdumpfs /oc/9
getting /oc/9/vod.xml                              (   166149) [###############]
getting /oc/9/config.xml                           (      421) [###############]
getting /oc/9/resource.xml                         (     7283) [###############]
getting /oc/9/schedule1.xml                        (    10758) [###############]
```

The command above, dumps files from the object carousel (as defined by MPEG DSMCC) mounted under directory /oc/9 in a target system and visible to the Java middleware only. These files are the configuration files for the VOD service available for the subscribers of a digital satellite TV platform 'N'.

Upon inspecting the value of vod.xml file, the following can be discovered:

```
    <file duration="6848"
          entitlement_bits="0x000002"
          entitlement_name="ITI VOD 2"
          expiration="2011-12-30 00:00:00"
          id="7437"
          key_id="226"
          name="P_LINCOLN_LAWYER_0511"
          priority="0"
          size="2290507776"
          version="0"/>

    <file duration="7662"
          entitlement_bits="0x000100"
          entitlement_name="ITI VOD 2"
          expiration="2012-01-30 00:00:00"
          id="7440"
```

2011 Security Explorations. All Rights Reserved.

```
        key_id="233"
        name="P_WAY_BACK_0511"
        priority="0"
        size="2559832064"
        version="0"/>

    <file duration="6060"
        entitlement_bits="0x000200"
        entitlement_name="ITI VOD 2"
        expiration="2012-01-30 00:00:00"
        id="7461"
        key_id="234"
        name="P_JESTEM_BOGIEM_0911"
        priority="0"
        size="2026477568"
        version="0"/>
```

These are XML descriptions of the VOD movies that correspond to some of the bits of the 0x01000382 entitlement value. The entry "entitlement_bits" provides the actual bit value for a given "entitlement_name" string.

From the above, one can also obtain id's of the recordings for the corresponding Push VOD files as well as their file names:

```
        id="7437"
        name="P_LINCOLN_LAWYER_0511"

        id="7440"
        name="P_WAY_BACK_0511"

        id="7461"
        name="P_JESTEM_BOGIEM_0911"
```

Next, "dvrinfo" command is issued with -p argument that obtains a list of Push VOD recordings available on the system:

```
box> dvrinfo -p
[PVOD info]
RECORDING 000
- id                    0x07567d19
- asset.id              7321
- asset.ver             0
- program               PVOD_0x00001c99_0
- time                  00h 00m 34s
- locator               dvr://123108633
- state                 COMPLETED_STATE
...
RECORDING 017
- id                    0xb981f3e2
- asset.id              7437
- asset.ver             0
- program               PVOD_0x00001d0d_0
- time                  01h 54m 08s
- locator               dvr://3112301538
- state                 COMPLETED_STATE
...
RECORDING 023
- id                    0xcf604f9c
```

2011 Security Explorations. All Rights Reserved.

```
- asset.id                  7440
- asset.ver                 0
- program                   PVOD_0x00001d10_0
- time                      02h 07m 42s
- locator                   dvr://3479195548
- state                     COMPLETED_STATE
...
RECORDING 027
- id                        0x7c682081
- asset.id                  7461
- asset.ver                 0
- program                   PVOD_0x00001d25_0
- time                      01h 41m 00s
- locator                   dvr://2087198849
- state                     COMPLETED_STATE
...
```

By matching the id's of a given recording with the "asset.id" value from the list above, one can discover the locator for given VOD movies. For example, file id 7437 has a locator of "dvr://3112301538".

Next, "play" command is issued with the use of discovered locator values:

```
box> play dvr://3479195548
```

As a result of the command above, the VOD movie starts playing (the movie can be watched as if it was sucessfully rented).

The JMF player is then instructed to stop playing the movie by issuing the following command:

```
box> play -s
```

We repeat the same steps with two other movie locators:

```
box> play dvr://2087198849
box> play -s
box> play dvr://3112301538
box> play -s
```

In each case, VOD movie starts playing without any problems. But, that's actually a problem as none of the movies should be available for playing on Dec 21 2011 as ilustrated by the entitlements for the current month (Dec 2011):

```
box> subsinfo
- "ITI Neovision  "
   01.12.2011 - 31.12.2011  0x01df643b
                          - Informacja i rozrywka
                          - Kultura, Nauka, Swiat
                          - Dzieci
                          - Style, Moda, Muzyka
                          - Hity filmowe
   01.11.2011 - 30.11.2011  0x01df643b
                          - Informacja i rozrywka
                          - Kultura, Nauka, Swiat
                          - Dzieci
                          - Style, Moda, Muzyka
```

2011 Security Explorations. All Rights Reserved.

```
                          - Hity filmowe
- "ITI VOD 1       "
   01.12.2011 - 31.12.2011  0x01000001
   01.11.2011 - 30.11.2011  0x01000001
- "ITI VOD 2       "
   01.12.2011 - 31.12.2011  0x01000000  <--- NO VOD MOVIES AVAILABLE
   01.11.2011 - 30.11.2011  0x01000382       FOR WATCHING IN DEC 2011
- "ITI VOD 3       "
   01.10.2011 - 31.10.2011  0x01004000
   01.03.2010 - 31.03.2010  0x01002000
- "ITI 2 Neovision"
   01.12.2011 - 31.12.2011  0x01000061
   01.11.2011 - 30.11.2011  0x01000021
```

The VOD movie "P_JESTEM_BOGIEM_0911" was rented on Nov 10 2011. This is illustrated by the log below showing the contents of the EMM message (and some debug info from our PoC) delivering the entitlement to the Conax card for this movie:

```
emmreq data:
Thu Nov 10 19:46:54 CET 2011
 size: 0000008c
       0000:  dd 84 00 00 87 12 85 82 70 82 00 00 00 00 33 48  ........p.....3H
       0010:  83 70 79 64 10 4a 40 3c e8 79 86 6e b9 3f 43 df  .pyd.J@<.y.n.?C.
       0020:  ae 09 de 53 a2 29 b9 ad f7 26 63 3b 83 16 cc 83  ...S.)...&c;....
       0030:  df b2 ce 24 aa 9a e9 c8 01 83 90 2f a7 3b c6 b9  ...$......./.;..
       0040:  b8 63 ba 40 6f 42 c9 79 59 be a4 a9 68 04 a1 96  .c.@oB.yY...h...
       0050:  be 99 f7 af 52 34 50 41 74 79 6b 77 47 96 40 22  ....R4PAtykwG.@"
       0060:  6c c1 e9 f4 e6 1c 6a 80 2b d3 b3 8e 3a f2 d7 0e  l.....j.+...:...
       0070:  08 e5 8d d2 d8 9c 82 f7 07 79 13 60 c1 a5 99 2f  .........y.....`/
       0080:  65 fb c6 6f be 62 24 76 3e d1 3c 47  e..o.b$v>.<G
Entitlement.diff
- cur emm:
- "ITI Neovision  "
   01.11.2011 - 30.11.2011  0x019e6433
                          - Informacja i rozrywka
                          - Kultura, Nauka, Swiat
                          - Style, Moda, Muzyka
                          - Hity filmowe
   01.10.2011 - 31.10.2011  0x019e6433
                          - Informacja i rozrywka
                          - Kultura, Nauka, Swiat
                          - Style, Moda, Muzyka
                          - Hity filmowe
- "ITI VOD 1       "
   01.11.2011 - 30.11.2011  0x01000001
   01.10.2011 - 31.10.2011  0x01000000
- "ITI VOD 2       "
   01.11.2011 - 30.11.2011  0x01000080
   01.01.2010 - 31.01.2010  0x01000000
- "ITI VOD 3       "
   01.10.2011 - 31.10.2011  0x01004000
   01.03.2010 - 31.03.2010  0x01002000
- "ITI 2 Neovision"
   01.11.2011 - 30.11.2011  0x01000021
   01.10.2011 - 31.10.2011  0x01000021
- new emm:
- "ITI Neovision  "
   01.11.2011 - 30.11.2011  0x019e6433
                          - Informacja i rozrywka
```

2011 Security Explorations. All Rights Reserved.

```
                          - Kultura, Nauka, Swiat
                          - Style, Moda, Muzyka
                          - Hity filmowe
   01.10.2011 - 31.10.2011  0x019e6433
                          - Informacja i rozrywka
                          - Kultura, Nauka, Swiat
                          - Style, Moda, Muzyka
                          - Hity filmowe
- "ITI VOD 1       "
   01.11.2011 - 30.11.2011  0x01000001
   01.10.2011 - 31.10.2011  0x01000000
- "ITI VOD 2       "
   01.11.2011 - 30.11.2011  0x01000280
   01.01.2010 - 31.01.2010  0x01000000
- "ITI VOD 3       "
   01.10.2011 - 31.10.2011  0x01004000
   01.03.2010 - 31.03.2010  0x01002000
- "ITI 2 Neovision"
   01.11.2011 - 30.11.2011  0x01000021
   01.10.2011 - 31.10.2011  0x01000021
- diff:
- "ITI VOD 2       "
   01.11.2011 - 30.11.2011  0x00000200  <--- ENTITLEMENT BIT SET BY SNIFFED EMM
                                             MESSAGE
store ITI_VOD_2_______07.47_10.11.2011_0x00000200_add.emm size 140
```

Similarily, the VOD movie "P_WAY_BACK_0511" was rented on Nov 11 2011. This is also illustrated by the log below showing the contents of the EMM message delivering the entitlement to the Conax card for this movie:

```
emmreq data:
Fri Nov 11 18:34:07 CET 2011
 size: 0000008c
       0000:  dd 84 00 00 87 12 85 82 70 82 00 00 00 00 33 48  ........p.....3H
       0010:  83 70 79 64 10 4a 40 3c e8 79 86 6e b9 3f 43 df  .pyd.J@<.y.n.?C.
       0020:  ae 09 de 53 a2 29 b9 ad f7 26 63 3b 2d 5b 8b 6b  ...S.)...&c;-[.k
       0030:  95 10 1a 26 39 98 e5 5d af 93 a2 30 42 05 02 88  ...&9..]...0B...
       0040:  02 6c c7 58 69 a0 ab 30 7a 58 63 2c ea ba 67 a1  .l.Xi..0zXc,..g.
       0050:  55 e2 c1 70 68 3e 8a 3f a2 1e e8 85 03 58 9f 8a  U..ph>.?.....X..
       0060:  f5 2d 76 b1 24 8d 90 26 31 c3 1d 33 6d a9 32 b5  .-v.$..&1..3m.2.
       0070:  ce 94 0c ae 84 4e 03 60 fb 3a ce d8 67 c9 99 9e  .....N...:..g...
       0080:  e2 3e fe a9 44 e4 0e 19 01 e1 ce 7e  .>..D.......
Entitlement.diff
- cur emm:
- "ITI Neovision  "
   01.11.2011 - 30.11.2011  0x019e6433
                          - Informacja i rozrywka
                          - Kultura, Nauka, Swiat
                          - Style, Moda, Muzyka
                          - Hity filmowe
   01.10.2011 - 31.10.2011  0x019e6433
                          - Informacja i rozrywka
                          - Kultura, Nauka, Swiat
                          - Style, Moda, Muzyka
                          - Hity filmowe
- "ITI VOD 1       "
   01.11.2011 - 30.11.2011  0x01000001
   01.10.2011 - 31.10.2011  0x01000000
- "ITI VOD 2       "
```

2011 Security Explorations. All Rights Reserved.

```
   01.11.2011 - 30.11.2011  0x01000200
   01.01.2010 - 31.01.2010  0x01000000
- "ITI VOD 3      "
   01.10.2011 - 31.10.2011  0x01004000
   01.03.2010 - 31.03.2010  0x01002000
- "ITI 2 Neovision"
   01.11.2011 - 30.11.2011  0x01000021
   01.10.2011 - 31.10.2011  0x01000021
- new emm:
- "ITI Neovision  "
   01.11.2011 - 30.11.2011  0x019e6433
                          - Informacja i rozrywka
                          - Kultura, Nauka, Swiat
                          - Style, Moda, Muzyka
                          - Hity filmowe
   01.10.2011 - 31.10.2011  0x019e6433
                          - Informacja i rozrywka
                          - Kultura, Nauka, Swiat
                          - Style, Moda, Muzyka
                          - Hity filmowe
- "ITI VOD 1      "
   01.11.2011 - 30.11.2011  0x01000001
   01.10.2011 - 31.10.2011  0x01000000
- "ITI VOD 2      "
   01.11.2011 - 30.11.2011  0x01000300
   01.01.2010 - 31.01.2010  0x01000000
- "ITI VOD 3      "
   01.10.2011 - 31.10.2011  0x01004000
   01.03.2010 - 31.03.2010  0x01002000
- "ITI 2 Neovision"
   01.11.2011 - 30.11.2011  0x01000021
   01.10.2011 - 31.10.2011  0x01000021
- diff:
- "ITI VOD 2      "
   01.11.2011 - 30.11.2011  0x00000100  <--- ENTITLEMENT BIT SET BY SNIFFED EMM
                                             MESSAGE
store ITI_VOD_2_______06.34_11.11.2011_0x00000100_add.emm size 140
```

Finally, we have a movie "P_LINCOLN_LAWYER_0511", which was rented on Nov 25 2011. Its EMM message along with a PoC debug log is given below:

```
emmreq data:
Fri Nov 25 18:07:41 CET 2011
 size: 0000008c
       0000:  dd 84 00 00 87 12 85 82 70 82 00 00 00 00 33 48  ........p.....3H
       0010:  83 70 79 64 10 4a 40 3c e8 79 86 6e b9 3f 43 df  .pyd.J@<.y.n.?C.
       0020:  ae 09 de 53 a2 29 b9 ad f7 26 63 3b 1c 9b d6 16  ...S.)...&c;....
       0030:  fb 68 f7 5c 63 e7 15 dd 63 05 7e 49 dc 8a 04 2e  .h..c...c..I....
       0040:  35 76 f5 ca 8e 5f 96 11 8d 06 fb 95 9f 85 94 92  5v..._..........
       0050:  45 c3 17 ce 3f 61 a0 ea 35 cc 50 fc 59 27 73 92  E...?a..5.P.Y's.
       0060:  72 47 16 f4 a4 80 8f fc c9 1b 56 09 5e 38 47 d6  rG........V.^8G.
       0070:  6a 29 f5 44 08 7b e6 56 cf 9d 7f 70 3b 2f 60 7e  j).D.{.V...p;/..
       0080:  aa 4a 97 c2 3e 52 4e 8d 41 88 f8 90  .J..>RN.A...
Entitlement.diff
- cur emm:
- "ITI Neovision  "
   01.11.2011 - 30.11.2011  0x01df643b
                          - Informacja i rozrywka
                          - Kultura, Nauka, Swiat
```

2011 Security Explorations. All Rights Reserved.

```
                          - Dzieci
                          - Style, Moda, Muzyka
                          - Hity filmowe
   01.10.2011 - 31.10.2011  0x019e6433
                          - Informacja i rozrywka
                          - Kultura, Nauka, Swiat
                          - Style, Moda, Muzyka
                          - Hity filmowe
- "ITI VOD 1       "
   01.11.2011 - 30.11.2011  0x01000001
   01.10.2011 - 31.10.2011  0x01000000
- "ITI VOD 2       "
   01.11.2011 - 30.11.2011  0x01000000
   01.01.2010 - 31.01.2010  0x01000000
- "ITI VOD 3       "
   01.10.2011 - 31.10.2011  0x01004000
   01.03.2010 - 31.03.2010  0x01002000
- "ITI 2 Neovision"
   01.11.2011 - 30.11.2011  0x01000021
   01.10.2011 - 31.10.2011  0x01000021
- new emm:
- "ITI Neovision  "
   01.11.2011 - 30.11.2011  0x01df643b
                          - Informacja i rozrywka
                          - Kultura, Nauka, Swiat
                          - Dzieci
                          - Style, Moda, Muzyka
                          - Hity filmowe
   01.10.2011 - 31.10.2011  0x019e6433
                          - Informacja i rozrywka
                          - Kultura, Nauka, Swiat
                          - Style, Moda, Muzyka
                          - Hity filmowe
- "ITI VOD 1       "
   01.11.2011 - 30.11.2011  0x01000001
   01.10.2011 - 31.10.2011  0x01000000
- "ITI VOD 2       "
   01.11.2011 - 30.11.2011  0x01000002
   01.01.2010 - 31.01.2010  0x01000000
- "ITI VOD 3       "
   01.10.2011 - 31.10.2011  0x01004000
   01.03.2010 - 31.03.2010  0x01002000
- "ITI 2 Neovision"
   01.11.2011 - 30.11.2011  0x01000021
   01.10.2011 - 31.10.2011  0x01000021
- diff:
- "ITI VOD 2       "
   01.11.2011 - 30.11.2011  0x80000002  <--- ENTITLEMENT BIT SET BY SNIFFED EMM
                                             MESSAGE
store ITI_VOD_2_______06.08_25.11.2011_0x00000002_add.emm size 140
```

To sum it up, all tests regarding the ability to play VOD movies were conducted on 21 Dec 2011. The VOD movies which were verified to be successfully played (and watched) were however rented on Nov 10 2011, Nov 11 2011 and Nov 25 2011.

The VOD service makes it possible to play a given movie for a limited amount of time (rental time). For Platform 'N's VOD service, this time is 48 hours (2 days). After that time, EMM

2011 Security Explorations. All Rights Reserved.

message is issued to the Conax card that disables the entitlement bit for a given movie, making it impossible to play it again.

One of the security abuses that can take place at this point is possible in the following way:

- The EMM indicating the end of VOD rental will not be delivered to the Conax card. This is a subject of Issue 23 reported to Conax AS under the name 'EMM blocking attack'. The original 'EMM blocking attack' reported to Conax AS did rely on a different scenario though. We informed Conax AS that attackers can block all EMM messages sent to the subscriber's card. As a result, no change to the subscriber's entitlements will be made. This is in particular important for EMM messages sent by the digital satellite TV operator that remove specific subscription bits from the subscriber's set of entitlements. This usually occurs at the beginning of a new subscription period (beginning of a new month).

The conducted test regarding Issue #22 verified the following:

- VOD movies could be played without any problems 39, 38 and 24 days after the end of the rental period. That's almost 6 weeks beyond the rental period in the longest case.
- VOD movies could be played even though Conax entitlements for the movies were from the past time period (Nov 2011) and current set of entitlements (Dec 2011) was clearly indicating no ability to play the movies (Dec 2011 set equal to 0x01000000).
- VOD movies could be played regardless of their status shown in the VOD menu (not rented in our case).

From our observations and conducted tests we concluded, that the effective entitlement bitmask was calculated with the use of the bitwise OR operation:

effective_entitlement_bitmask = (past_entitlement_bitmask | current_entitlement_bitmask)

[Issue #23 – blocking attack against Conax EMM data]

There is a security issue in a design of the Conax conditional access system. We found out that attackers can block all EMM messages sent to the subscriber's card. As a result, no change to the subscriber's entitlements will be made. This is in particular important for EMM messages sent by the digital satellite TV operator that remove specific subscription bits from the subscriber's set of entitlements. This usually occurs at the beginning of a new subscription period (beginning of a new month).

All Conax EMM messages (those affecting the status of subscriber's entitlements and keys) start with 0xdd 0x84 byte values. Sample message influencing one specific bit of a subscriber's set of entitlements is presented below:

```
0000:  dd 84 00 00 87 12 85 82 70 82 00 00 00 00 33 48  ........p.....3H
0010:  83 70 79 64 10 4a 40 3c e8 79 86 6e b9 3f 43 df  .pyd.J@<.y.n.?C.
0020:  ae 09 de 53 a2 29 b9 ad f7 26 63 3b 1c 9b d6 16  ...S.)...&c;....
0030:  fb 68 f7 5c 63 e7 15 dd 63 05 7e 49 dc 8a 04 2e  .h..c...c..I....
0040:  35 76 f5 ca 8e 5f 96 11 8d 06 fb 95 9f 85 94 92  5v..._..........
```

2011 Security Explorations. All Rights Reserved.

```
0050:  45 c3 17 ce 3f 61 a0 ea 35 cc 50 fc 59 27 73 92  E...?a..5.P.Y's.
0060:  72 47 16 f4 a4 80 8f fc c9 1b 56 09 5e 38 47 d6  rG........V.^8G.
0070:  6a 29 f5 44 08 7b e6 56 cf 9d 7f 70 3b 2f 60 7e  j).D.{.V...p;/..
0080:  aa 4a 97 c2 3e 52 4e 8d 41 88 f8 90              .J..>RN.A...
```

The above message udates subscriber's set of entitlements by adding the following entry to it:

```
- "ITI VOD 2       "
   01.11.2011 - 30.11.2011  0x00000002
```

Conax EMM messages are usually directed to specific Conax cards identified upon their unique address. This address is composed of 7 bytes and starts at offset 0x10 of the EMM message. For the presented message this address is equal to "00 00 00 00 33 48 83". EMM messages also specify the key number, which should be used by the card to decrypt the body of the message. In the case of EMM messages, this key is different for every subscriber in order to avoid a replay attack reusing EMM messages directed to other users. In the case of our message, this key has index 0x10.

We suspect that the problem with blocking attack against EMM data has its origin from the Issue 22. Security Explorations observed that Conax card successfully released Control Words for the TV programming in a subscription period for which no new entitlements were received by the card yet. All TV programming could be watched as in the previous subscription period. In the case where the current subscription period is not replaced by the new one, old entitlements bits are still in effect. In the context of EMM blocking attack, this can allow potential attackers to prolonge their subscription periods to certain programming to which they should not be entitled any more.

About Security Explorations

Security Explorations (`http://www.security-explorations.com`) is a security start-up company from Poland, providing various services in the area of security and vulnerability research. The company came to life in a result of a true passion of its founder for breaking security of things and analyzing software for security defects. Adam Gowdiak is the company's founder and its CEO. Adam is an experienced Java Virtual Machine hacker, with over 50 security issues uncovered in the Java technology over the recent years. He is also the hacking contest co-winner and the man who has put Microsoft Windows to its knees (vide MS03-026). He was also the first one to present successful and widespread attack against mobile Java platform in 2004.

2011 Security Explorations. All Rights Reserved.