Orchestrating a fire sale

Bringing Dutch alarm systems to their knees

Wilco Baan Hofman

Wilco Baan Hofman

about me

- Reverse engineer
- Working at Nikhef
- Free / open source software developer
- Co-founder and treasurer of Bitlair

Background

or how I got involved

- Why are alarms only visible at the receiving centre?
- We wanted notifications and logs of all events, not just alarms
- Let's reverse engineer the protocols!

Protocol landscape

or what's out there

- Legacy/Analog:
  - ANSI SIA
  - ANSI X/SIA
  - Ademco ContactID
- IP:
  - SIA-HS (Alphatronics proprietary)
  - Vebon SecIP (Proposed Dutch standard)
  - Chiron protocol (Chiron proprietary)
  - Ademco IP protocol (Pitt/Ademco/Honeywell proprietary)
  - ANSI/SIA IP DC-09 (USA standard)
  - VDS 2465-S2 (German standard)

The problem

or how hard is it to crack?

- Fatal assumptions are made
- Fatal mistakes are made

Assumption 1

The internet can be secured by certifying ISPs

Assumption 2

Internet source addresses can be trusted

Assumption 3

In a session, every packet is from the same peer

Assumption 4

Nobody can decode obfuscated packets

“... IP protocol fitted with text in a data format with dynamic data encryption which makes it ***impossible*** *to decipher the message.”*
--- Alphatronics Product Catalog

Assumption 5

If my product is certified, it is secure

“Alphatronics emphasizes that the uncovered vulnerabilities do not influence the product certification.”
--- Alphatronics security bulletin to customers

Assumption 6

If nobody knows the protocol format, nobody can decipher the messages

Assumption 7

If my peer speaks the same protocol, it must be valid peer

Assumption 8

Encryption is enough to make a connection secure

Assumption 9

Giving an alarm receiving centre the option to disable encryption will not lead to insecure deployments

Assumption 10

Alarm system electronics engineers can design secure internet protocols

Alarm dialer basics

or what's that word again?

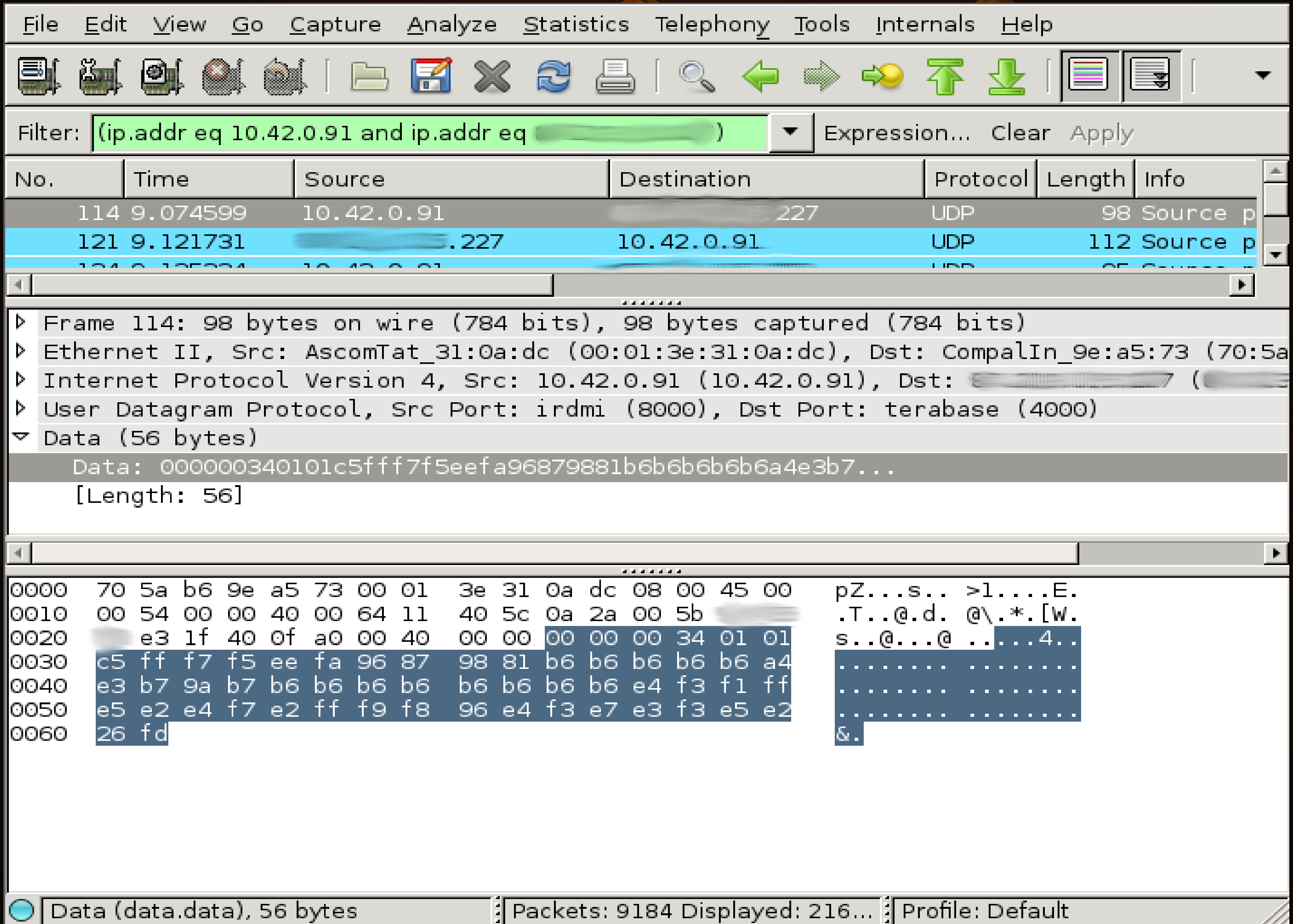
- ATE: Alarm Transmit Equipment
- ARC: Alarm Receiving Centre
- PROM: Unique account code for a building
- ATE sends alarms, ARC sends ACKs
- SIA codes
  - BA: Burglary Alarm, BR Burglary restore, etc

SIA-HS

or SIA "highly secure"

- Protocol by Alphatronics
- Impossible to decipher according to the catalog
- Let's see how secure it really is...?

The packet



Filter: (ip.addr eq 10.42.0.91 and ip.addr eq [redacted])

No.	Time	Source	Destination	Protocol	Length	Info
114	9.074599	10.42.0.91	[redacted].227	UDP	98	Source p
121	9.121731	[redacted].227	10.42.0.91	UDP	112	Source p

```
▷ Frame 114: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
▷ Ethernet II, Src: AscomTat_31:0a:dc (00:01:3e:31:0a:dc), Dst: CompalIn_9e:a5:73 (70:5a
▷ Internet Protocol Version 4, Src: 10.42.0.91 (10.42.0.91), Dst: [redacted] ([redacted]
▷ User Datagram Protocol, Src Port: irdmi (8000), Dst Port: terabase (4000)
▽ Data (56 bytes)
    Data: 000000340101c5fff7f5eefa96879881b6b6b6b6a4e3b7...
    [Length: 56]
```

```
0000  70 5a b6 9e a5 73 00 01  3e 31 0a dc 08 00 45 00   pZ...s.. >1....E.
0010  00 54 00 00 40 00 64 11  40 5c 0a 2a 00 5b [redacted]   .T..@.d. @\.*.[W.
0020  [redacted] e3 1f 40 0f a0 00 40  00 00 00 00 00 34 01 01   s..@...@ ....4..
0030  c5 ff f7 f5 ee fa 96 87  98 81 b6 b6 b6 b6 b6 a4   ........ ........
0040  e3 b7 9a b7 b6 b6 b6 b6  b6 b6 b6 b6 e4 f3 f1 ff   ........ ........
0050  e5 e2 e4 f7 e2 ff f9 f8  96 e4 f3 e7 e3 f3 e5 e2   ........ ........
0060  26 fd                                              &.
```

Data (data.data), 56 bytes | Packets: 9184 Displayed: 216... | Profile: Default

XOR 0xB6?

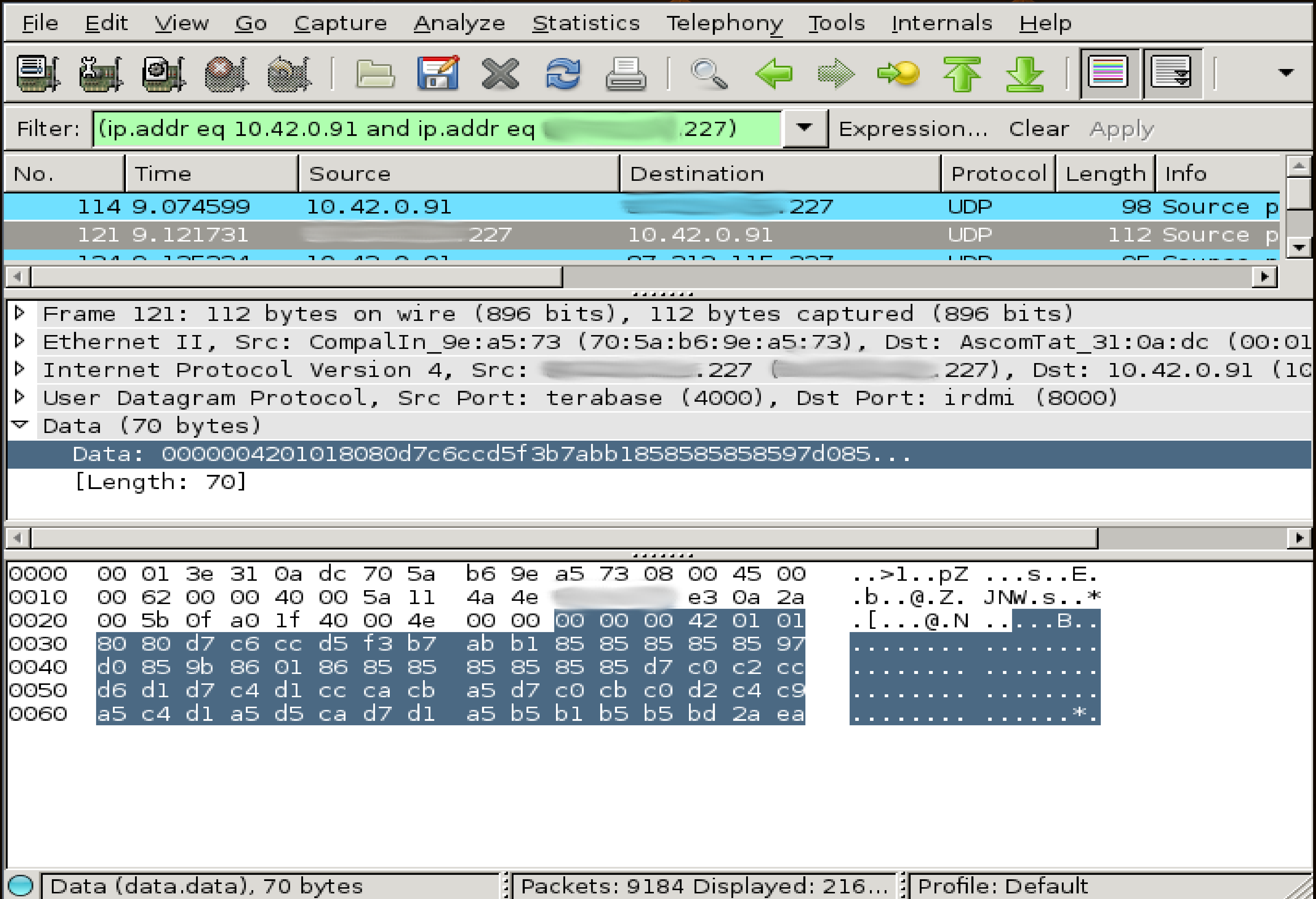
```
#!/usr/bin/env python

bytes =
bytearray("000000340101c5fff7f5eefa96879881b6b6b6b6b6a4e3b79ab7b6b6b6b
6b6b6b6b6e4f3f1ffe5e2e4f7e2fff9f896e4f3e7e3f3e5e226fd".decode('hex_cod
ec'))

for i in range(len(bytes)):
    bytes[i] ^= 0xB6

print bytes
print bytes.encode('hex_codec')
```

Why? Yes!

������sIACXL 1.7U,REGISTRATION REQUEST�K

```
b6b6b682b7b773494143584c20312e37000000
0000125501 2c010000000000000000000052454749
5354524154494f4e2052455155455354904b
```

But wait..


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply

Filter: (ip.addr eq 10.42.0.91 and ip.addr eq [redacted].227)

```
No.   Time      Source           Destination      Protocol Length Info
  114 9.074599  10.42.0.91       [redacted].227   UDP          98 Source p
  121 9.121731  [redacted].227   10.42.0.91       UDP         112 Source p
```

```
▷ Frame 121: 112 bytes on wire (896 bits), 112 bytes captured (896 bits)
▷ Ethernet II, Src: CompalIn_9e:a5:73 (70:5a:b6:9e:a5:73), Dst: AscomTat_31:0a:dc (00:01
▷ Internet Protocol Version 4, Src: [redacted].227 ([redacted].227), Dst: 10.42.0.91 (10
▷ User Datagram Protocol, Src Port: terabase (4000), Dst Port: irdmi (8000)
▽ Data (70 bytes)
    Data: 0000004201018080d7c6ccd5f3b7abb18585858585 97d085...
    [Length: 70]
```

```
0000  00 01 3e 31 0a dc 70 5a  b6 9e a5 73 08 00 45 00   ..>1..pZ ...s..E.
0010  00 62 00 00 40 00 5a 11  4a 4e [redacted] e3 0a 2a   .b..@.Z. JNW.s..*
0020  00 5b 0f a0 1f 40 00 4e  00 00 00 00 00 42 01 01   .[...@.N .....B..
0030  80 80 d7 c6 cc d5 f3 b7  ab b1 85 85 85 85 85 97   ........ ........
0040  d0 85 9b 86 01 86 85 85  85 85 85 85 d7 c0 c2 cc   ........ ........
0050  d6 d1 d7 c4 d1 cc ca cb  a5 d7 c0 cb c0 d2 c4 c9   ........ ........
0060  a5 c4 d1 a5 d5 ca d7 d1  a5 b5 b1 b5 b5 bd 2a ea   ........ ......*.
```

Data (data.data), 70 bytes | Packets: 9184 Displayed: 216... | Profile: Default

XOR 0x85?

- Yes indeed:

  ���DŽ�RCIPv2.4U�REGISTRATION RENEWAL AT PORT 04008�o

  858585c7848405055243495076322e340000000
  00001255001e0384030000000000000052454749
  5354524154494f4e2052454e4557414c204154
  20504f525420303430303038af6f

Recap

- So we have:
  - UnXORed packet length
  - Device name
  - Decimal PROM number encoded as if it were hex
  - Message
  - Checksum

The checksum

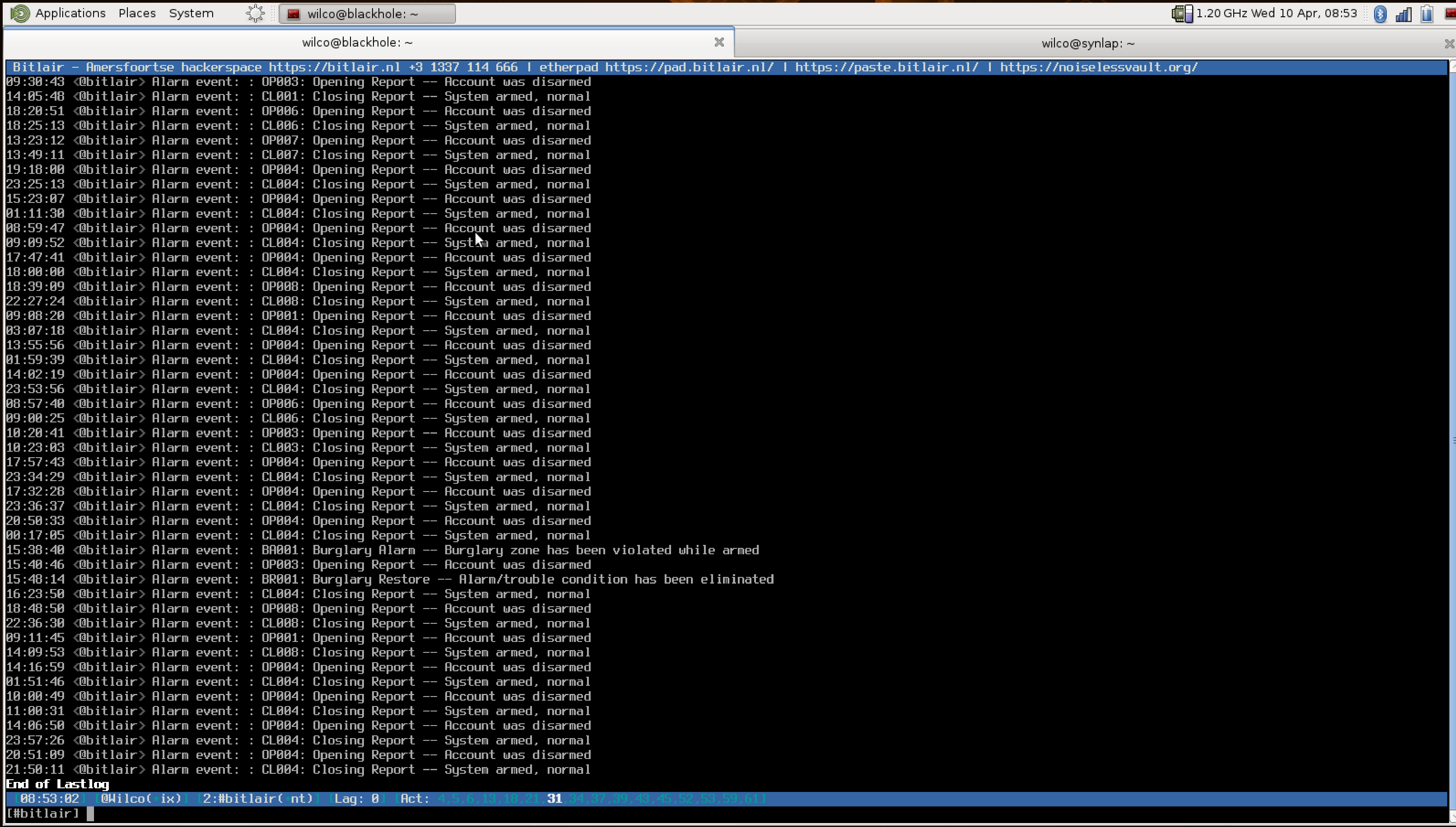
- Days of trying different algorithms...
  - I tried every known CRC-10 to CRC-16 algorithm
  - Different preseed values
- But wait..
  - longer packets give generally higher checksums
    - … Must be multiplication or addition
  - OMFG? Really!? 16-bit sum of all preceeding bytes
- D'OH!

My implementation

Bitlair's siahsd

- Full SIA-HS ARC implementation
- Full Vebon SecIP ARC implementation
- Pluggable handlers:
    - Database event logging
    - JSONBOT IRC Event notification
- Chiron IrisTouch implementation in progress

IRC in action



```
 Bitlair - Amersfoortse hackerspace https://bitlair.nl +3 1337 114 666 | etherpad https://pad.bitlair.nl/ | https://paste.bitlair.nl/ | https://noiselessvault.org/
09:30:43 <@bitlair> Alarm event: : OP003: Opening Report -- Account was disarmed
14:05:48 <@bitlair> Alarm event: : CL001: Closing Report -- System armed, normal
18:20:51 <@bitlair> Alarm event: : OP006: Opening Report -- Account was disarmed
18:25:13 <@bitlair> Alarm event: : CL006: Closing Report -- System armed, normal
13:23:12 <@bitlair> Alarm event: : OP007: Opening Report -- Account was disarmed
13:49:11 <@bitlair> Alarm event: : CL007: Closing Report -- System armed, normal
19:18:00 <@bitlair> Alarm event: : OP004: Opening Report -- Account was disarmed
23:25:13 <@bitlair> Alarm event: : CL004: Closing Report -- System armed, normal
15:23:07 <@bitlair> Alarm event: : OP004: Opening Report -- Account was disarmed
01:11:30 <@bitlair> Alarm event: : CL004: Closing Report -- System armed, normal
08:59:47 <@bitlair> Alarm event: : OP004: Opening Report -- Account was disarmed
09:09:52 <@bitlair> Alarm event: : CL004: Closing Report -- System armed, normal
17:47:41 <@bitlair> Alarm event: : OP004: Opening Report -- Account was disarmed
18:00:00 <@bitlair> Alarm event: : CL004: Closing Report -- System armed, normal
18:39:09 <@bitlair> Alarm event: : OP008: Opening Report -- Account was disarmed
22:27:24 <@bitlair> Alarm event: : CL008: Closing Report -- System armed, normal
09:08:20 <@bitlair> Alarm event: : OP001: Opening Report -- Account was disarmed
03:07:18 <@bitlair> Alarm event: : CL004: Closing Report -- System armed, normal
13:55:56 <@bitlair> Alarm event: : OP004: Opening Report -- Account was disarmed
01:59:39 <@bitlair> Alarm event: : CL004: Closing Report -- System armed, normal
14:02:19 <@bitlair> Alarm event: : OP004: Opening Report -- Account was disarmed
23:53:56 <@bitlair> Alarm event: : CL004: Closing Report -- System armed, normal
08:57:40 <@bitlair> Alarm event: : OP006: Opening Report -- Account was disarmed
09:00:25 <@bitlair> Alarm event: : CL006: Closing Report -- System armed, normal
10:20:41 <@bitlair> Alarm event: : OP003: Opening Report -- Account was disarmed
10:23:03 <@bitlair> Alarm event: : CL003: Closing Report -- System armed, normal
17:57:43 <@bitlair> Alarm event: : OP004: Opening Report -- Account was disarmed
23:34:29 <@bitlair> Alarm event: : CL004: Closing Report -- System armed, normal
17:32:28 <@bitlair> Alarm event: : OP004: Opening Report -- Account was disarmed
23:36:37 <@bitlair> Alarm event: : CL004: Closing Report -- System armed, normal
20:50:33 <@bitlair> Alarm event: : OP004: Opening Report -- Account was disarmed
00:17:05 <@bitlair> Alarm event: : CL004: Closing Report -- System armed, normal
15:38:40 <@bitlair> Alarm event: : BA001: Burglary Alarm -- Burglary zone has been violated while armed
15:40:46 <@bitlair> Alarm event: : OP003: Opening Report -- Account was disarmed
15:48:14 <@bitlair> Alarm event: : BR001: Burglary Restore -- Alarm/trouble condition has been eliminated
16:23:50 <@bitlair> Alarm event: : CL004: Closing Report -- System armed, normal
18:48:50 <@bitlair> Alarm event: : OP008: Opening Report -- Account was disarmed
22:36:30 <@bitlair> Alarm event: : CL008: Closing Report -- System armed, normal
09:11:45 <@bitlair> Alarm event: : OP001: Opening Report -- Account was disarmed
14:09:53 <@bitlair> Alarm event: : CL008: Closing Report -- System armed, normal
14:16:59 <@bitlair> Alarm event: : OP004: Opening Report -- Account was disarmed
01:51:46 <@bitlair> Alarm event: : CL004: Closing Report -- System armed, normal
10:00:49 <@bitlair> Alarm event: : OP004: Opening Report -- Account was disarmed
11:00:31 <@bitlair> Alarm event: : CL004: Closing Report -- System armed, normal
14:06:50 <@bitlair> Alarm event: : OP004: Opening Report -- Account was disarmed
23:57:26 <@bitlair> Alarm event: : CL004: Closing Report -- System armed, normal
20:51:09 <@bitlair> Alarm event: : OP004: Opening Report -- Account was disarmed
21:50:11 <@bitlair> Alarm event: : CL004: Closing Report -- System armed, normal
End of Lastlog
 [08:53:02] [@Wilco(+ix)] [2:#bitlair(+nt)] [Lag: 0] [Act: 4,5,6,13,18,21,31,34,37,39,43,45,52,53,59,61]
[#bitlair]
```

Protocol design

or how to make it secure?

Remember, protocol security requires at least:

- Protection from packet injection
- Strong cipher
- Identity verification
- Forward secrecy

Security

How bad can it be?

- No identity verification
- No session protection
- Predictable interaction between ARC and ATE
    - UDP packet's source easy to spoof
- Predictable PROM codes
    - Sequential, True for all protocols

Implications

or what can I do with this?

- Man-in-the-middle
- Send false alarms
  - … while remaining anonymous
- Denial of Service on the alarm centre ops
- Denial of Service on the police response
- Fire Sale?!

SIA-HS Security

The verdict

Everyone can trigger alarms for ALL of the ARC's customers without revealing their own IP

Vebon SecIP

Attempts to do it better

- Handshake:
  - RSA 1024 bit, public key sent to the ATE
  - ATE uses the public key to transfer the AES-128 session key
  - AES communication channel is up
- Secure, right?

Not really

- If done correctly, there'd be a secure channel
- … but to whom?

Vebon SecIP

The verdict

- No identity verification
  - Man in the Middle attack
  - Send false alarms from anywhere
- Insecure cryptographic padding
  - Chosen cipher-text attack
- No forward secrecy
  - Have the private key, decrypt entire event history

Responses

Or what happened since the report

- First report for SIA-HS august 2012: no response
- First report for SecIP in september 2012: no response
- Small scale publication at hitr2ndb
- Then in January 2013
  - Asked NCSC for help
  - NCSC assigned a coordinator
  - Alphatronics asked me to remove publication
  - Vebon and ENAI responded well, hired Certified Secure and Pine Security to fix SecIP
  - Chiron offered a properly configured ARC to aid testing

So what now?

Or how to fix?

- Upgrading all the firmwares
- Mitigating attacks by isolating customers on insecure protocols

Summary

- Code on github: http://github.com/bitlair/siahsd
- Ask me for more specs on other protocols!
- Give me more dialers with different protocols!

Thank you

- Please check out other projects I'm working on
  - Spacefed → Federated authentication for hackerspaces
  - Bitlair → Hackerspace Amersfoort
  - OHM2013 → The next big Dutch hacker camp