Common problems in SCADA

D.S. Ljungmark

Date
2016-11-28

MODIO

Who’s this guy?

D.S. Ljungmark

- Kernel
- Distributions
- GNOME
- etc.

Systems nerd
Security fellow
Free Software Fan
Opinionated Unixbeard
Social Justice Aficionado

https://twitter.com/spidler
https://github.com/Spindel/
https://gitlab.com/Spindel

MODIO

Embedded systems

Hardware that's difficult to reach

Sometimes online, sometimes not

- "Lights out Management"
- Train Engine Controller
- SSD wear level controller

Some have stability requirements, others not

- Network hardware (Switches)
- USB connected 3G Modems

Some are constrained, others not

- 8bit PIC
- 16bit DOS (Canon EOS cameras)
- 32bit mips systems with 4Gigs RAM (routers, etc.)

MODIO

Our Embedded Systems

Beefy little machines

- Fair bit of RAM
- Quite fast ARMv7 cores
- Plenty of Storage
- Connected

In hard to reach places

- Behind locked doors
- Buildings 200km away
- Datacentres

The network is hostile

- Random networks
- No administration
- Bare firewalling

MODIO

Threats in our business

- Networked access is easy
  - Always on public internet
  - Assume reachable
- Network should not harm neighbours
  - DDoS, reflection, etc.
- Physical access is hard
  - Locked rooms
  - Not public knowledge
- Physical access can do worse
  - No point protecting against physical attacks
- Physical access should not harm other infrastructure
  - No shared credentials
  - No undesirable shared access

MODIO

Other threats to keep in mind

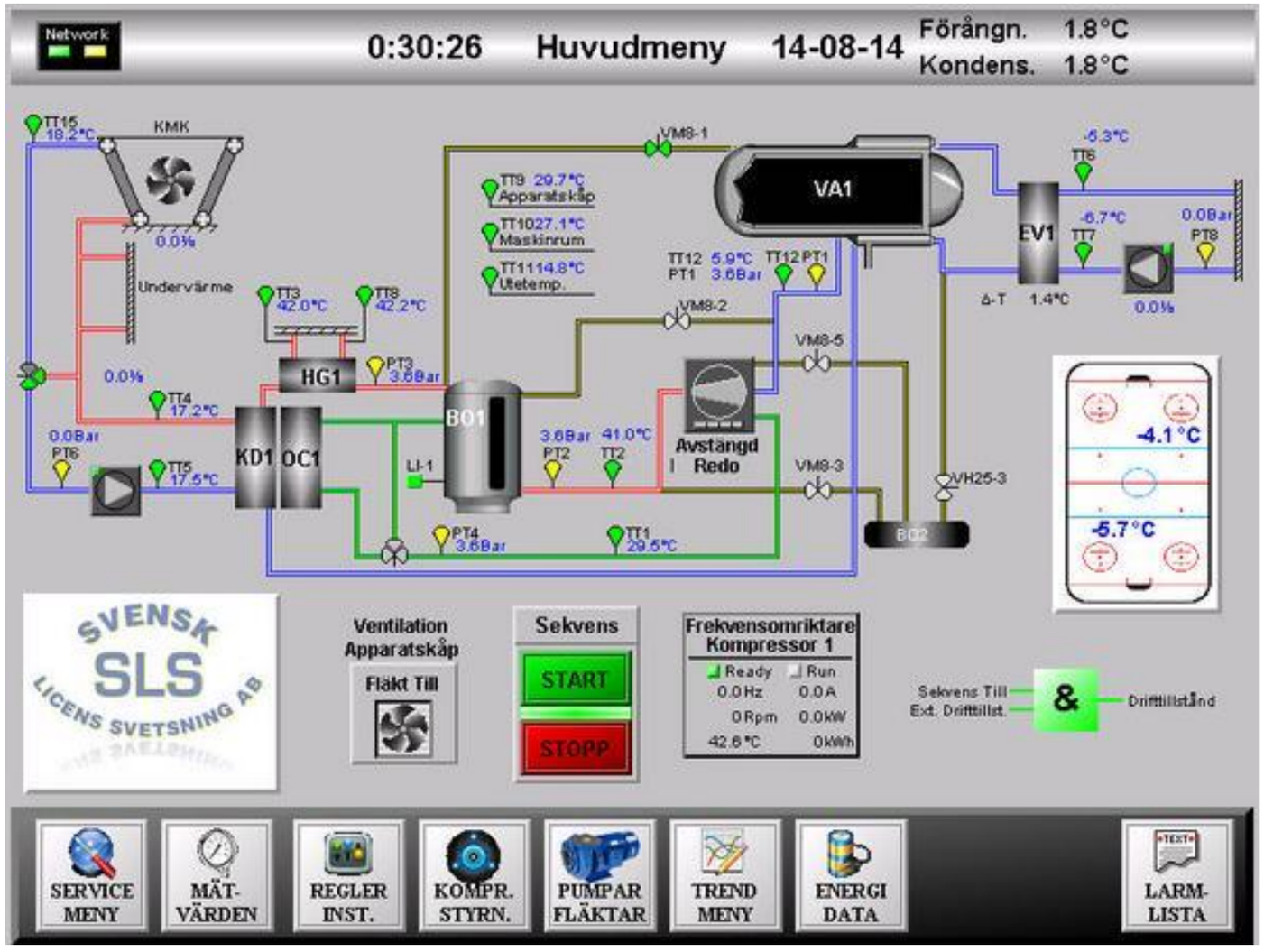
- Many sources of input
  - Network
  - User
  - Hardware
- Hostile environment
  - Internet is not friendly
  - Facility networks are quirky
- Protect from yourself
  - Internet parts should not bring down SCADA part

Do strict validation!

Performance? Meh. Until DoS

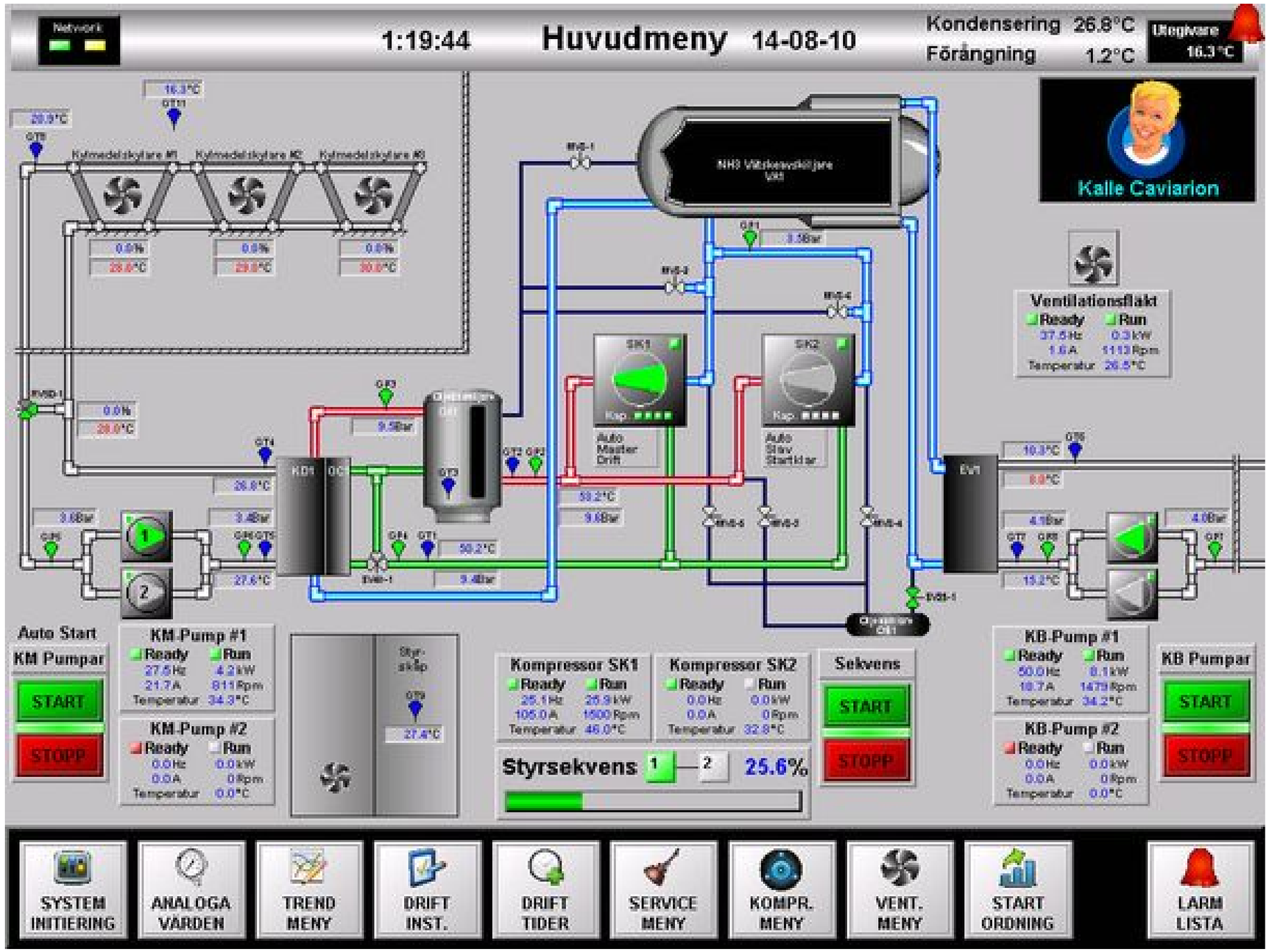
MODIO

Same as always, but Online



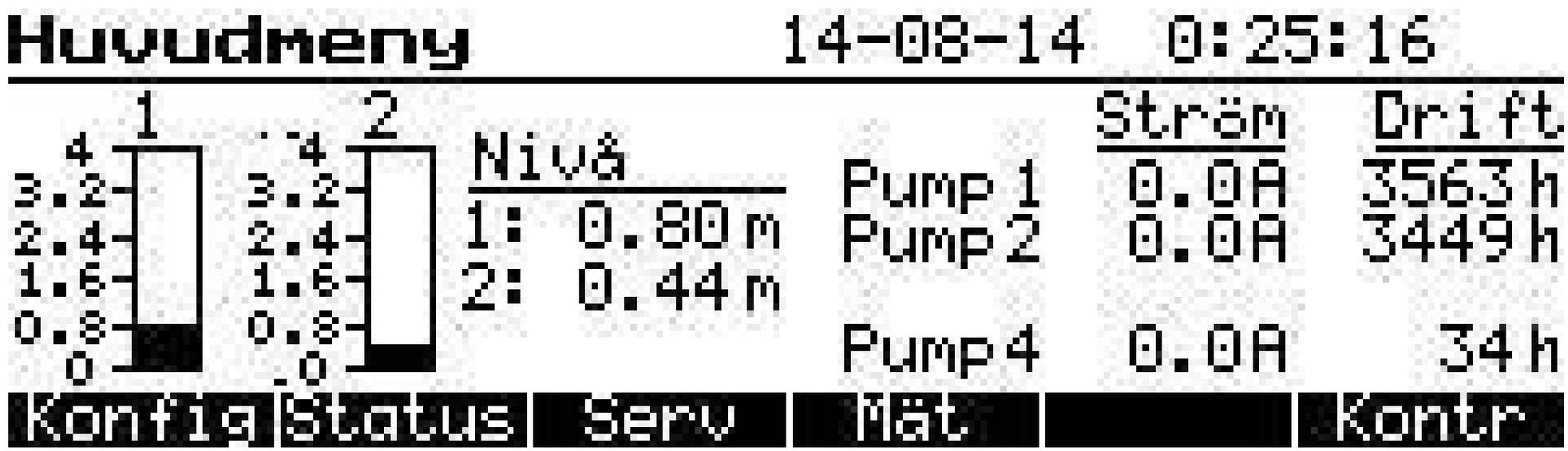
MODIO

The Same, but Online mk2



MODIO

“It’s not a computer”



MODIO

Hardcoded or default credentials

Wireshark · Follow TCP Stream (tcp.stream eq 27) · cameradome-20161118-04

```
............LocalHost login: ..........P..........rootroot

Password: xmhdipc

.[1;32mWelcome to Monitor Tech..[0;39m
# enable
enable
system
shell
sh
-sh: enable: not found
# /bin/busybox ECCHI
system
-sh: system: not found
# shell
-sh: shell: not found
# sh
# /bin/busybox ECCHI
ECCHI: applet not found
# /bin/busybox ps; /bin/busybox ECCHI
/bin/busybox ps; /bin/busybox ECCHI
  PID USER       VSZ STAT COMMAND
    1 root      1240 S    init
    2 root         0 SW   [kthreadd]
    3 root         0 SW   [ksoftirqd/0]
    4 root         0 SW   [kworker/0:0]
```

428 client pkt(s), 1,988 server pkt(s), 852 turns.

Entire conversation (813 kB) | Show data as ASCII | Stream 27

Find: | Find Next

Hide this stream | Print | Save as... | Close | Help

MODIO

Configuration bugs

Conversations: traffic.pcap16

Ethernet: 1 | Fibre Channel | FDDI | IPv4: 150 | IPv6 | IPX | JXTA | NCP | RSVP | SCTP | TCP | Token Ring | UDP: 164 | USB | WLAN

UDP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B	Rel Start	Duration	bps A→B	bps
118.69.250.27	ntp	192.168.0.3	http	14 758	7 113 356	14 758	7 113 356	0	0	0.001695000	9.9336	5728731.60	
85.111.0.148	ntp	192.168.0.3	http	12 562	6 054 884	12 562	6 054 884	0	0	0.010440000	9.5057	5095776.66	
202.10.82.10	ntp	192.168.0.3	http	11 252	5 423 464	11 252	5 423 464	0	0	0.004325000	10.0466	4318663.93	
222.255.125.126	ntp	192.168.0.3	http	10 114	4 874 948	10 114	4 874 948	0	0	0.003535000	9.9577	3916521.37	
208.118.234.238	ntp	192.168.0.3	http	9 154	4 412 228	9 154	4 412 228	0	0	0.000286000	9.6962	3640372.55	
94.20.20.40	ntp	192.168.0.3	http	8 880	4 280 160	8 880	4 280 160	0	0	0.016930000	9.6400	3552004.05	
80.82.78.2	ntp	192.168.0.3	http	8 862	4 271 484	8 862	4 271 484	0	0	0.003076000	9.5534	3576928.16	
193.110.75.146	ntp	192.168.0.3	http	8 861	4 271 002	8 861	4 271 002	0	0	0.009293000	9.1673	3727171.77	
59.53.64.2	ntp	192.168.0.3	http	8 854	4 267 628	8 854	4 267 628	0	0	0.000683000	9.9346	3436571.05	
24.124.0.251	ntp	192.168.0.3	http	8 830	4 256 060	8 830	4 256 060	0	0	0.014518000	9.6221	3538557.34	
212.227.126.37	ntp	192.168.0.3	http	8 793	4 238 226	8 793	4 238 226	0	0	0.004970000	9.4317	3594888.75	
201.17.1.233	ntp	192.168.0.3	http	8 781	4 232 442	8 781	4 232 442	0	0	0.000130000	9.7165	3484729.30	
206.197.60.7	ntp	192.168.0.3	http	8 498	4 096 036	8 498	4 096 036	0	0	0.000149000	9.4364	3472536.81	
212.227.126.49	ntp	192.168.0.3	http	8 452	4 073 864	8 452	4 073 864	0	0	0.000010000	9.5564	3410359.75	
176.43.250.1	ntp	192.168.0.3	http	8 103	3 905 646	8 103	3 905 646	0	0	0.000000000	8.5763	3643178.66	
200.52.196.166	ntp	192.168.0.3	http	7 581	3 654 042	7 581	3 654 042	0	0	0.000537000	9.1761	3185720.39	
122.193.101.138	ntp	192.168.0.3	http	7 572	3 649 704	7 572	3 649 704	0	0	0.012389000	9.9591	2931746.13	
200.75.3.254	ntp	192.168.0.3	http	7 489	3 609 698	7 489	3 609 698	0	0	0.006899000	9.2697	3115251.51	
195.10.10.67	ntp	192.168.0.3	http	7 399	3 566 318	7 399	3 566 318	0	0	0.013891000	8.4222	3387521.64	
40.136.209.102	ntp	192.168.0.3	http	7 373	3 553 786	7 373	3 553 786	0	0	0.059239000	10.9231	2602772.83	
76.8.155.55	ntp	192.168.0.3	http	7 369	3 542 066	7 369	3 542 066	0	0	0.018782000	9.2379	3067421.28	
200.52.174.70	ntp	192.168.0.3	http	7 185	3 463 170	7 185	3 463 170	0	0	0.007794000	9.6491	2871292.53	
217.12.178.249	ntp	192.168.0.3	http	7 181	3 461 242	7 181	3 461 242	0	0	0.002297000	9.0337	3065196.74	

☑ Name resolution ☐ Limit to display filter

Help | Copy | Follow Stream | Graph A→B | Graph B→A | Close

MODIO

Software Vulnerabilities

```
Bootstrap Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x9772a11e
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.139.12 (192.168.139.12)
    Next server IP address: 192.168.139.128 (192.168.139.128)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Vmware_d0:6d:08 (00:0c:29:d0:6d:08)
    Client hardware address padding: 00000000000000000000
    Server host name: () { :; }; echo sname1
    Boot file name not given
    Magic cookie: DHCP
  ⊞ Option: (53) DHCP Message Type (ACK)

0000  ff ff ff ff ff ff 00 0c  29 d9 98 a6 08 00 45 00   ........ )......E.
0010  01 5c 0d e0 00 00 80 11  df 88 c0 a8 8b 80 ff ff   .\...... ........
0020  ff ff 04 10 00 44 01 48  a8 ad 02 01 06 00 97 72   .....D.H .......r
0030  a1 1e 00 00 00 00 00 00  00 00 c0 a8 8b 0c c0 a8   ........ ........
0040  8b 80 00 00 00 00 00 0c  29 d0 6d 08 00 00 00 00   ........ ).m.....
0050  00 00 00 00 00 00 28 29  20 7b 20 3a 3b 20 7d 3b   ......() { :; };
0060  20 65 63 68 6f 20 73 6e  61 6d 65 31 00 00 00 00    echo sn ame1....
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

Threats faced, summary

- Same as old, without updating threat model
  - From Physical availability to Global availability
- Same as old, but with a pin/password!
  - Fast brute forced
  - Very common
- It’s broken but we can’t update it
  - Build systems
  - PLC
  - Manual update (screwdriver + programmer)
- Networked, but not designed for Internet
  - Combination of above problems
  - Configuration errors allowing UDP amplification
- Pure bugs & Security bugs
  - Heartbleed
  - Shellshock

MODIO

Security as a process

- No instant security
- No simple checklist
- Some easy fixes
- Process changes
- Purchaser awareness
- No magic devices

MODIO

Fixes that don’t work

Tell user to change password

Not documenting the root password

Tell user they need a separate firewall

Tell user device should not be on internet

Tell user to update software

Crypto

MODIO

Fixes: Credentials

No backdoor accounts

No remote accessible defaults

Generate on first startup

Force physical interaction to reset

Rate limit

Hop limit / TTL

(2FA)

MODIO

Fixes: Legacy

Enable updates

Keep building

Social problem, documentation problem

Support software for expected hardware lifetime

Postel’s principle is wrong

Windows XP of the future

MODIO

Fixes: Bugs

Enable online & unattended updates

Reduce scope

Secure languages / environments

Disarm classes of bugs

(ASLR, Rust, Modern C++ , canaries.)

Enable online configuration changes

MODIO

Questions?

Modio team

Simon Oest
Sales/
Project management

Take Aanstoot
CEO

Dennis Ljungmark
Security expert/
developer

At Modio we know IT-security, we love embeded systems and want them to be secure on the Internet. Our porfolio consists of a number of services that helps our customers and partners to have full control of their solutions through a common web browser at any device. Through our REST-API data can be fetched and included in your web portal or distributed to third parties. Combining secure connections with customer value, so to speak.

MODIO