Faking at Level 1

How Digital Twins Save Your PLCs

CyberDanube

CD Security Technologies GmbH | Hohenauergasse 21A/1,1190 Vienna | Email office@cyberdanube.com | 2022-07 | Version 1.0

Introduction

Focus on embedded/(I)IoT/OT related technologies

Speaker on conferences like HITB, BlackHat, IT-SECX, OMH,...

Published several security advisories regarding embedded devices

„WHO AM I ?“

Thomas Weber

Outline

Foundation

Typical OT Security Assessment

Digital Twin Construction

Security Testing

Conclusion

Foundations

OT - Operational Technology

- Devices on different levels are: RTU, PLC, HMI, Eng. Station, SCADA server, Historian,…

IoT - Internet of Things

- Devices: IP Camera, Printer, Router, Smart Fridge, Smart Watch,…

IIoT - Industrial Internet of Things

- Devices: Industrial Router/Switch, Sensors/Actuators in industrial environments,…

Digital Twins

- During this session: a (sometimes) full functional emulation from the operating system of the embedded device in scope, excluding physical I/Os.

„Digital Twin“

…there are different definitions of Digital Twin!

Foundations - How OT Became “Smarter”

In early days:

- Fieldbus technology - Modbus, PROFIBUS-PA/DP, CAN, ASI bus, …
- PLCs with one programming interface: a COM port (RS232) and limited memory
- Supervision via analog technology (e.g. via light signaling)

Foundations - How OT Became “Smarter”

In early days:

- Fieldbus technology - Modbus, PROFIBUS-PA/DP, CAN, ASI bus, …
- PLCs with one programming interface: a COM port (RS232) and limited memory
- Supervision via analog technology (e.g. via light signaling)

Nowadays:

- PLCs with Ethernet connection, much more computational power and memory
- Manageable Ethernet switches
- Routers, Firewalls and other network infrastructure devices
- Shift from traditional fieldbus technology to the TCP/IP stack
- Peripheral devices - Industrial Internet of Things (IIoT) like humidity/heat/light/proximity/… sensors

IT/OT Differences

Foundations

Foundations - IT/OT Differences

IT

- A lot of network traffic / high bandwidth
- Deals with business-related information
- Soft real-time due to not time-critical calculation
- Short system failure results in data-loss
- Updates during running operation
- Startup of whole IT system needs minutes/hours
- ...

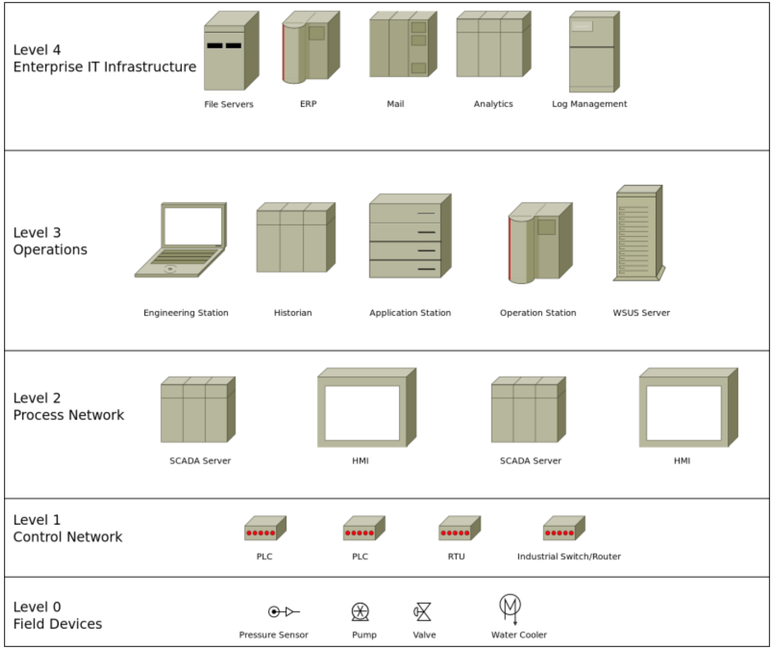
OT

- Medium network traffic / low bandwidth
- Deals with industrial-related information
- Hard real-time due to time-critical calculation
- Short system failure may pose a critical business risk
- Upgrades only during (yearly) maintanance windows
- Startup of whole OT system may need days/weeks
- ...

Typical OT Security Assessment

- Be careful!
- Log all network traffic!
- Do not(!) use automated security scanner for IT!
- Be careful!

Typical OT Security Assessment – Purdue



OT networks are often structured according the Purdue model.

A representative model can is viewed here …

Typical OT Security Assessment - Steps

Information Gathering / Passive Testing:

- Review network blueprints
- Collect information about all systems including the software/firmware version
- Sniffing network traffic using Tcpdump/Wireshark to monitor for devices/protocols

Active Testing:

- Do not forget to log with Tcpdum/Wireshark!
- Scanning for devices with ICMP in the network. Afterwards for selected ports (80, 443, 23 ,...)
- Testing for typical vulnerabilities in accordance with the customer (to not affect crit. systems)

Reporting:

- Listing vulnerabilities and their probability/impact
- Listing mitigation measures for each vulnerability

tenable.ot

Typical OT Security Assessment - Problems

Risks during active testing:

- Denial of service (can hit the whole factory) with potential long duration
- Destroyed devices due to wrong/malicious I/O
- Affecting power/water supply if done in critical infrastructure
- Affecting human life

Typical OT Security Assessment - Problems

Risks during active testing:

- Denial of service (can hit the whole factory) with potential long duration
- Destroyed devices due to wrong/malicious I/O
- Affecting power/water supply if done in critical infrastructure
- Affecting human life

Issues ?

maybe less harmful if OT scanning software is used …… but what if such issues still arise?

Typical OT Security Assessment - Solution

A possible solution to (partially) overcome the latter explained problems are digital copies of the OT network in scope. These can cover the whole network or selected parts, that have been left out as outage of one device can result in much bigger problems.

Such technique is also known as virtual pentesting, but it comes with the following implications:

- A virtualization always has a certain gap
- Not all devices/networks can be virtualized
- The effort to create virtualizations can differ a lot

Despite all the difficulties, it still pays off.

Digital Twin Construction – General

Digital twins of OT/IIoT/IoT/embedded devices (in terms of firmware virtualization) are usually created by using the following steps.

- Extracting/downloading the firmware of interest
- Analyzing the firmware and prepare it for virtualization
- Start the desired virtualization environment to create the digital twin
- Run the digital twin

Digital Twin Construction – Tools

FIRMADYNE

EMUX (ARMX)

- Linux-base firmware emulation
- Open-Source
- ARM/MIPS (QEMU)
- Command-line interface

Qiling Framework

- Binary instrumentation framework
- Open-Source
- x86/x64/ARM/MIPS (Unicorn)
- Command-line interface

MEDUSA

- Linux-based firmware emulation
- Propritary
- ARM/MIPS/PPC/SPARC/SH4/x86/x64 (QEMU)
- Web-interface

FIRMADYNE

- Linux-based firmware emulation
- Open-Source
- ARM/MIPS (QEMU)
- Command-line interface

EMUX ON DOCKER

MEDUSA

QILING.IO

FIRMADYNE

Digital Twin Construction – Gap Analysis

Physical Device

- Chipset
- I/Os
- Firmware

Digital Twin

- Emulated Chips
- Spare I/Os
- Emulated Firmware

Virtualizations of devices help to get a big picture of the specific embedded system!

Digital Twin Construction – Pro & Con

FIRMADYNE

Pro

- No risk at all by using Digital Twins
- Parallel tests can be performed
- Live debugging possible
- Device hardware not needed – high flexibility for the tester
- Also possible to test communication to fat clients
- Patches can be tested on virtual devices before rollout

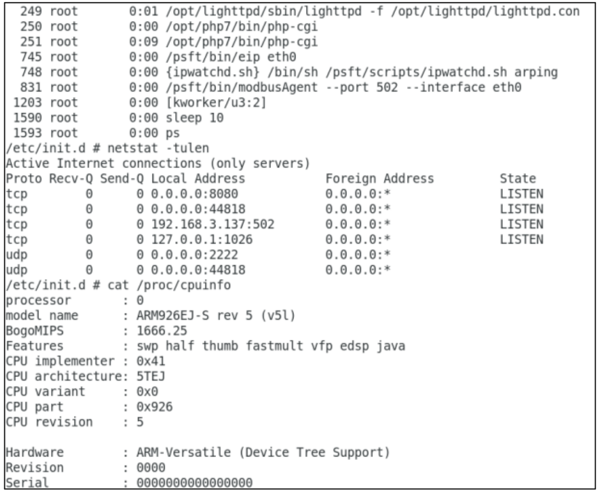
Con

- Virtualization/Cloning process can be hard and time consuming
- Not possible for all OT devices
- 100% clones are rarely possible
- Only feasible for bigger OT networks (50+ different devices)

Security Testing

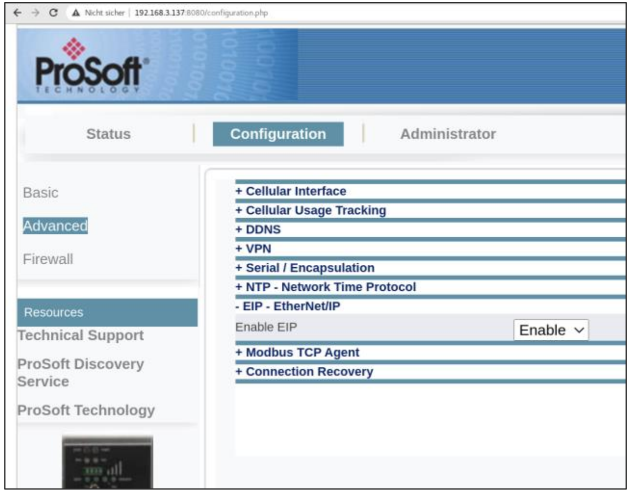
Hacking devices at Level 1

Security Testing – Examples / Demo



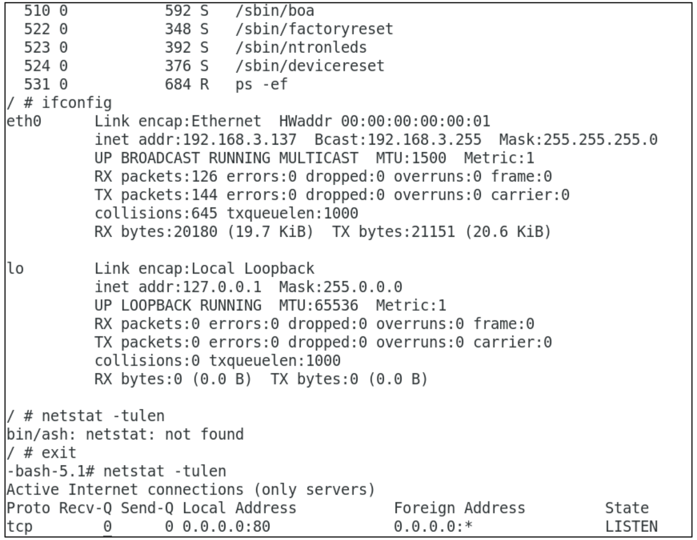
```
  249 root       0:01 /opt/lighttpd/sbin/lighttpd -f /opt/lighttpd/lighttpd.con
  250 root       0:00 /opt/php7/bin/php-cgi
  251 root       0:09 /opt/php7/bin/php-cgi
  745 root       0:00 /psft/bin/eip eth0
  748 root       0:00 {ipwatchd.sh} /bin/sh /psft/scripts/ipwatchd.sh arping
  831 root       0:00 /psft/bin/modbusAgent --port 502 --interface eth0
 1203 root       0:00 [kworker/u3:2]
 1590 root       0:00 sleep 10
 1593 root       0:00 ps
/etc/init.d # netstat -tulen
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:8080            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:44818           0.0.0.0:*               LISTEN
tcp        0      0 192.168.3.137:502       0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:1026          0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:2222            0.0.0.0:*
udp        0      0 0.0.0.0:44818           0.0.0.0:*
/etc/init.d # cat /proc/cpuinfo
processor       : 0
model name      : ARM926EJ-S rev 5 (v5l)
BogoMIPS        : 1666.25
Features        : swp half thumb fastmult vfp edsp java
CPU implementer : 0x41
CPU architecture: 5TEJ
CPU variant     : 0x0
CPU part        : 0x926
CPU revision    : 5

Hardware        : ARM-Versatile (Device Tree Support)
Revision        : 0000
Serial          : 0000000000000000
```



Enable EIP: Enable

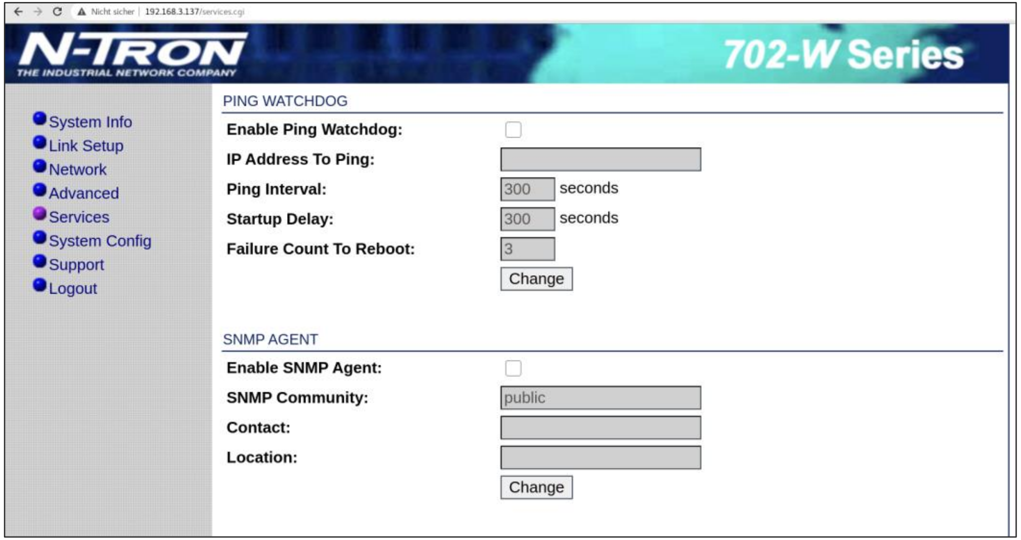
Security Testing – Examples / Demo



```
  510 0          592 S   /sbin/boa
  522 0          348 S   /sbin/factoryreset
  523 0          392 S   /sbin/ntronleds
  524 0          376 S   /sbin/devicereset
  531 0          684 R   ps -ef
/ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:00:00:00:00:01
          inet addr:192.168.3.137  Bcast:192.168.3.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:126 errors:0 dropped:0 overruns:0 frame:0
          TX packets:144 errors:0 dropped:0 overruns:0 carrier:0
          collisions:645 txqueuelen:1000
          RX bytes:20180 (19.7 KiB)  TX bytes:21151 (20.6 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

/ # netstat -tulen
bin/ash: netstat: not found
/ # exit
-bash-5.1# netstat -tulen
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
```



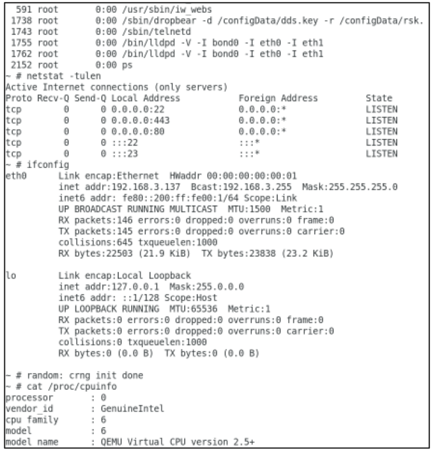
PING WATCHDOG

Enable Ping Watchdog:	□
IP Address To Ping:	
Ping Interval:	300 seconds
Startup Delay:	300 seconds
Failure Count To Reboot:	3
	Change

SNMP AGENT

Enable SNMP Agent:	□
SNMP Community:	public
Contact:	
Location:	
	Change

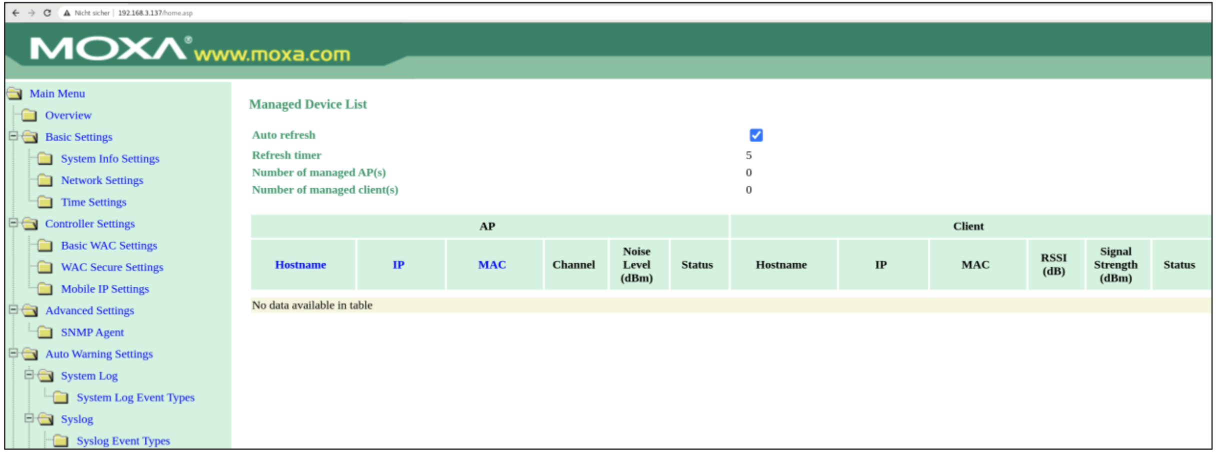
Security Testing – Examples / Demo



```
  591 root       0:00 /usr/sbin/iw_webs
 1738 root       0:00 /sbin/dropbear -d /configData/dds.key -r /configData/rsk.
 1743 root       0:00 /sbin/telnetd
 1755 root       0:00 /bin/lldpd -V -I bond0 -I eth0 -I eth1
 1762 root       0:00 /bin/lldpd -V -I bond0 -I eth0 -I eth1
 2152 root       0:00 ps
~ # netstat -tulen
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 :::22                   :::*                    LISTEN
tcp        0      0 :::23                   :::*                    LISTEN
~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 00:00:00:00:00:01
          inet addr:192.168.3.137  Bcast:192.168.3.255  Mask:255.255.255.0
          inet6 addr: fe80::200:ff:fe00:1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:146 errors:0 dropped:0 overruns:0 frame:0
          TX packets:145 errors:0 dropped:0 overruns:0 carrier:0
          collisions:645 txqueuelen:1000
          RX bytes:22503 (21.9 KiB)  TX bytes:23838 (23.2 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

~ # random: crng init done
~ # cat /proc/cpuinfo
processor       : 0
vendor_id       : GenuineIntel
cpu family      : 6
model           : 6
model name      : QEMU Virtual CPU version 2.5+
```



Managed Device List

Auto refresh ☑

Refresh timer 5

Number of managed AP(s) 0

Number of managed client(s) 0

AP						Client					
Hostname	IP	MAC	Channel	Noise Level (dBm)	Status	Hostname	IP	MAC	RSSI (dB)	Signal Strength (dBm)	Status
No data available in table											

Security Testing - Disclosed Vulnerabilities

Already Public:

- Red Lion N-Tron industrial access point
- Nexans industrial switch series
- Korenix industrial swich/access point/media converter device series
- Pepperl+Fuchs industrial swich/access point/IO-Link device series
- Phoenix Contact TC Router/Switch (industrial cellular device) series
- Altus Sistemas de Automacao / Beijer PLC series

Currently Pending:

- Delta Electronics
- Hirschmann

Security Testing – Reactions

Well known:

- Deny
- No reaction
- Endless ping-pong (even worse for OT)

Special case for Digital Twins:

- Vulnerabilities on application level get not accepted "…it's your controlled environment…"

Lessons learned

… do not mention that you’ve tested on a digital twin in the first message!

Conclusion … to sum it up!

# Comprehensive OT security assessments are always challenging

# Digital Twins enables the pentester to build a (more or less precise) clone

# OT Devices and networks can be emulated/virtualized by this technique

# OT Devices and networks are not harmed as the digital twins are completely seperated

# New vulnerabilities on OT devices can be found much easier on digital twins

# No big news: there are responsibly and absolutely not responsibly vendors

Any gaps in knowledge … ?

You can reach us at any time at
office@cyberdanube.com

CyberDanube

Austria - Vienna [HQ]

CD Security Technologies GmbH
Hohenauergasse 21A/1, A-1190 Vienna
Tel +43 (0) 677 637 562 21
Email office@cyberdanube.com

Austria - St. Pölten

CD Security Technologies GmbH
Dr.-Steger-Gasse 3, 3140 St. Pölten
Email office-stp@cyberdanube.com