

Faking at Level 1

How Digital Twins Save Your PLCs



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



Introduction

"WHO AM I ?"

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

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

Published several security advisories regarding embedded devices



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.



...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

Cyber**Danube**

. . .

. . .



Typical OT Security Assessment

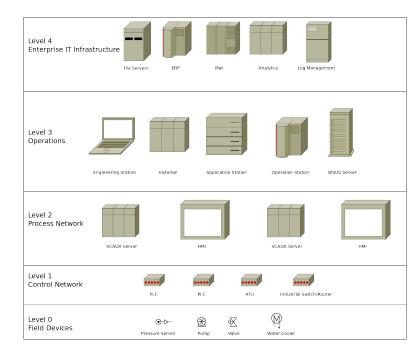
- Be careful!
- Log all network traffic!
- Do not(!) use automated

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 Tcpdump/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





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



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



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



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)

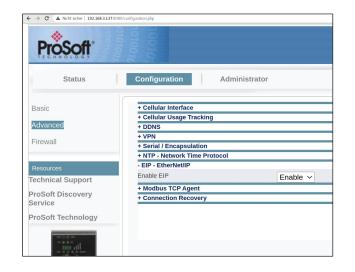
Security Testing

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/bp7/bin/php-cgi 745 root 0:00 /opt/bp7/bin/php-cgi 745 root 0:00 /psft/bin/mobusAgent -port 502interface eth0 1203 root 0:00 /psft/bin/mobusAgent -port 502interface eth0 1203 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:* LISTEN tcp 0 0.0.0.0:* LISTEN tcp 0 0.0.0.0:* LISTEN tcp 0 0.0.0:* LISTEN tcp 0 0.0.0:* LISTEN tcp 0 0.0.0:* LISTEN udp 0 0.0.0:* LISTEN vdp 0 0.0.0:* LISTEN tcp 0 0.0:0:* LISTEN tcp 0 0.0:0:* LISTEN udp 0 0.0:0:* LISTEN </th <th>249 root</th> <th>0.01 (opt/lighttpd/chip/li</th> <th>abttpd f (opt/lighttpd/</th> <th>lighttnd con</th>	249 root	0.01 (opt/lighttpd/chip/li	abttpd f (opt/lighttpd/	lighttnd con				
251 root 0:09 /opt/bin/bin/pin-cii 745 root 0:00 /opt/bin/sicip eth0 1203 root 0:00 /sicip eth0 1393 root 0:00 ps /etc/init.d # netstat -tulen Active Internet connections (only servers) Proto Recv-0 Send-0 Local Address Foreign Address State 0 0.0.0.0:8080 0.0.0.0:8 tcp 0 0.0.0.0:8080 0.0.0.0:8 LISTEN tcp 0 0.0.0.0:84818 0.0.0.0:8 LISTEN tcp 0 0.0.0.0:84818 0.0.0:8:* LISTEN tcp 0 0.0				tighttpu.com				
745 root 0:00 /pst/bin/eip eih0 748 root 0:00 (jpwatchd.sh /pst/scripts/jpwatchd.sh arping 831 root 0:00 /pst/bin/modbusAgent -port 502interface 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 Intermet connections (only servers) Proto Recv-0 Send-O Local Address tcp 0 0.0.0.0:44818 0 0.10.0.0:44818 0.0.0.0:* tcp 0 0.0.0.0:44818 udp 0 0.0.0.0:* udp 0 0.0.0.0:44818 0 0.0.0.0:* LISTEN tcp 0 0.0.0.0:* LISTEN udp 0 0.0.0.0:44818 0.0.0.0:* udp 0 0.0.0.0:44818 0.0.0.0:* vectrinit.d # cat/proc/cpuinfo processor : processor : 0 model.name cpurchitecture: Stat : UP orchitecture: Stat : UP orchitecture: Stat : <tr< td=""><td></td><td></td><td></td><td></td></tr<>								
748 root 0:00 (1pwatchd.sh) /bin/sh /psft/scripts/1pwatchd.sh arping 831 root 0:00 /psft/bin/mobusAgentport 502interface 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 0.0.0.0:44818 0.0.0.0:* tcp 0 0.0.0.0:44818 0.0.0.0:* LISTEN tcp 0 0.0.0.0:44818 0.0.0.0:* LISTEN tcp 0 0.0.0.0:44818 0.0.0.0:* LISTEN udp 0 0.0.0.0:44818 0.0.0.0:* LISTEN tcp 0 0.0.0.0:2222 0.0.0.0:* LISTEN udp 0 0.0.0.0:2222 0.0.0.0:* USTEN udp 0 0.0.0.0:4818 0.0.0:* USTEN udp 0 0.0.0.0:4818 0.0.0:* USTEN vdp (rocscor : 0 0 0.0.0:* USTEN gogMIPS : 1566.25 Stat								
831 root 0:00 /pst/bin/modbusAgentport 502interface eth0 1203 root 0:00 [kworker/u3:2] 1590 root 0:00 sleep 10 1593 root 0:00 ps /etc/init.d # netstat -tulen /etc/init.d # netstat -tulen Active Internet connections (only servers) Proto Recv-0 Send-0 Local Address Foreign Address State tcp 0 0.0.0.0:* LISTEN tcp tcp 0 0.0.0.0:* LISTEN tcp 0 0.0.0.0:* LISTEN tcp 0 0.0.0.0:* LISTEN tcp 0 0.0.0.0:* LISTEN tcp 0 0.0.0:* LISTEN tcp 0 0.0.0.0:* LISTEN 0.0.0:* LISTEN Udp 0 0.0.0:* LISTEN udp 0 0.0.0.0:*				- hand a se				
1203 root 0:00 [kworker/u3:2] 1590 root 0:00 bleep 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 0.0.0.8080 0.0.0.0.8* LISTEN tcp 0 0.0.0.8080 0.0.0.8* tcp 0 0.0.0.8080 0.0.0.8* tcp 0 0.0.0.8137:502 0.0.0.8* LISTEN tcp 0 0.0.0.8:222 0.0.0.8* LISTEN udp 0 0.0.0.8:222 0.0.0.8* LISTEN udp 0 0.0.0.8:222 0.0.0.8* LISTEN udp 0 0.0.0.8:4218 0.0.0.8* LISTEN processor : 0 model.5:5 model name : RM926EJ-S rev 5 (v51) BogoMIPS : 166:0.25 : State CPU architecture: STEJ CPU architecture: : : State CPU architecture: STEJ CPU architecture: : :								
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 0.0.0.8080 0.0.0.0.* LISTEN tcp 0 0.0.0.8080 0.0.0.0.* LISTEN tcp 0 0.0.0.1.812 0.0.0.* LISTEN tcp 0 0.0.0.1.812 0.0.0.0.* LISTEN tcp 0 0.0.0.1.8222 0.0.0.0.* LISTEN udp 0 0.0.0.44818 0.0.0.0								
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 0.0.0.8080 0.0.0.0.8:* LISTEN tcp 0 0.0.0.8080 0.0.0.0.8:* LISTEN tcp 0 0.0.0.1820 0.0.0.0.8:* LISTEN tcp 0 0.0.0.18222 0.0.0.0.8:* LISTEN udp 0 0.0.0.0.11026 0.0.0.0.8:* LISTEN processor :0 0.0.0.0.12222 0.0.0.0.8:* LISTEN udp 0 0.0.0.0.44818 0.0.0.0.8:* LISTEN processor :0 model name : RM926EJ-S rev 5 (v51) BogoMIPS : I666.25 Features : Swp half thumb fastmult vfp edsp java CPU architecture: STEJ CPU architecture: STEJ CPU architecture: STEJ CPU apart : 0x926 : : State : CPU part : 0x926 : : : : Hardware : ARM-Versatile (Device Tree Support) : : <td></td> <td></td> <td></td> <td></td>								
<pre>/etc/init.d # netstat -tulen Active Internet connections (only servers) Proto Recv-Q Send-Q Local Address Foreign Address State tcp 0 0 0.0.0.8:4818 0.0.0.0.8:* LISTEN tcp 0 0 192.168.3.137:502 0.0.0.0.8:* LISTEN tcp 0 0 192.168.3.137:502 0.0.0.0.8:* LISTEN tcp 0 0 127.0.0.1:1026 0.0.0.0.8:* LISTEN tcp 0 0 0.0.0.8:2222 0.0.0.0.8:* USTEN udp 0 0 0.0.0.8:2222 0.0.0.0.8:* USTEN udp 0 0 0.0.0.8:4818 0.0.0.6:* / /etc/init.d # cat /proc/puinfo processor : 0 model name : ARM926EJ-S rev 5 (v51) Bog0MIPS : 1666.25 Features : swp half thumb fastmult vfp edsp java CPU implementer : 0x41 CPU architecture: STEJ CPU variant : 0x00 CPU part : 0x926 CPU revision : 5 Hardware : ARM-Versatile (Device Tree Support) Revision : 0000</pre>								
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 0 102.168.3.137:502 0.0.0.0:* LISTEN tcp 0 0 102.168.3.137:502 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0.1:1025 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0.1:1025 0.0.0.0:* LISTEN tcp 0 0 0.0.0.0.0:2222 0.0.0.0.0:* udp 0 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 (v51) BogoMIP5 : 1666.25 Features : swp half thumb fastmult vfp edsp java CPU implementer : 0x04 CPU architecture: STEJ CPU variant : 0x00 CPU part : 0x926 CPU revision : 5 Hardware : ARM-Versatile (Device Tree Support) Revision : 0000								
Proto Recv-Q Send-Q Local Address Foreign Address State tcp 0 0.0.0.8080 0.0.0.8.9 ILSTEN tcp 0 0.0.0.8080 0.0.0.8.9 ILSTEN tcp 0 0.0.0.81800 0.0.0.8.9 ILSTEN tcp 0 0.0.0.813137:502 0.0.0.8.9 ILSTEN tcp 0 0.127.8.0.1:1026 0.0.0.8.9 LISTEN udp 0 0.0.0.8.137:502 0.0.0.8.9 LISTEN udp 0 0.0.8.137:502 0.0.0.8.9 LISTEN udp 0 0.0.8.1812 0.0.8.9 ILSTEN udp 0 0.8.0.8.1812 0.8.8.9 ILSTEN processor 0 model.8.1812 0.8.8.9 ILSTEN BogoMIPS 1666.25 restarmes restarmes ILSTEN CPU architecture: STEJ restarmes restarmes ILSTEN CPU architecture: STEJ restarmes restarmes restarmes CPU parchitecture: <								
tcp 0 0.0.0.0.8080 0.0.0.0.* LISTEN tcp 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 0.12.168.3.137:502 0.0.0.0.* LISTEN tcp 0 0.0.0.0.0:222 0.0.0.0.0.* LISTEN udp 0 0.0.0.0.0:222 0.0.0.0.0.* LISTEN udp 0 0.0.0.0.44818 0.0.0.0.* LISTEN udp 0 0.0.0.0.0.0.0. 0.0.0.0.* LISTEN udp 0 0.0.0.0.0.0.0.0.0. 0.0.0.0.* LISTEN vdc1/dt #ct/int.dt #ct/int.dt #ct/int.dt LISTEN wodel name : 0 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.								
tcp 0 0.0.0.0.44818 0.0.0.0.* LISTEN tcp 0 0.21.68.3.137:502 0.0.0.0.0.* LISTEN tcp 0 0.27.0.0.1:1026 0.0.0.0.0.* LISTEN udp 0 0.0.0.0.22222 0.0.0.0.* LISTEN udp 0 0.0.0.0.0.2222 0.0.0.0.* Udp porcessor 0 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.								
tcp 0 192.168.3.137:502 0.0.0.0:* LISTEN tcp 0 0.27.0.0.1:1026 0.0.0.0:* LISTEN udp 0 0.0.0.0:12222 0.0.0.0.0:* LISTEN udp 0 0.0.0.0:44818 0.0.0.0:* LISTEN vdc/init.df *cl/proc/cpuinfo processor :0 model name RM926E1-S rev 5 (v51) BogoMIPS :1666.25 Features :swp half thumb fastmult vfp edsp java CPU architecture: STEJ CPU architecture: Sv0 CPU part :0x0 CPU part :0x0 CPU revision :5 Hardware : ARM-Versatile (Device Tree Support) Revision :0000								
tcp 0 0127.0.0.1:1026 0.0.0.0.0:* LISTEN udp 0 0.0.0.0:222 0.0.0.0.0:* Vector /etc/init.d # cat /proc/cpuinfo 0.0.0.0:* Vector Vector processor :0 0 0.0.0.0:* Vector BogoMIPS :1666.25 Features :swp half thumb fastmult vfp edsp java CPU architecture: Stat CPU architecture: :Sw0 CPU architecture: Stat CPU concerned CPU concerned CPU architecture: :Stat :Sw0 CPU revision :Sw0 CPU revision :Sw0 CPU revision :S Sw0 :Sw0 :Sw0 :Sw0 :Sw0 CPU revision :Sw0 :Sw0 :Sw0 :Sw0 :Sw0 :Sw0 :Sw0 CPU revision :Sw0 :Sw0 <td< td=""><td></td><td></td><td></td><td></td></td<>								
udp 0 0.0.0.0:2222 0.0.0.0:* vdp 0 0.0.0:44818 0.0.0.0:* vetc/init.d # cat /proc/cpuinfo processor :0 processor :0 0 0.0.0:* model name :RAM926EJ-S rev 5 (v51) 0.0.000000000000000000000000000000000								
udp 0 0.0.0.2.44818 0.0.0.0:* /etc/init.d # cat /proc/cpuinfo processor :0 model name : ARM926EJ-S rev 5 (v51) BogoMIPS : I666.25 Features : Swp half thumb fastmult vfp edsp java CPU implementer : SwA1 CPU varchitecture: STEJ CPU varchitecture: : Sv0 CPU part : 0x926 CPU revision : 5 Hardware : ARM-Versatile (Device Tree Support) Revision : 0000				LISTEN				
/etc/init.d # cat /proc/cpuinfo processor : 0 model name : RRM926EJ-S rev 5 (v5l) BogoNIPS : 1666.25 Features : swp half thumb fastmult vfp edsp java CPU implementer : 0x41 CPU architecture: STEJ CPU variant : 0x00 CPU part : 0x926 CPU part : 5 Hardware : ARM-Versatile (Device Tree Support) Revision : 0000								
processor : o model name : RAM026E1-S rev 5 (v5l) BogoMIPS : 1666.25 Features : swp half thumb fastmult vfp edsp java CPU implementer : 8v41 CPU architecture: STEJ CPU variant : 8v8 CPU part : 8v926 CPU part : 8v926 CPU revision : 5 Hardware : ARM-Versatile (Device Tree Support) Revision : 0000			0.0.0:*					
model name : ARM926EJ-S rev 5 (v5l) BogoNIPS : 1666.25 Features : swp half thumb fastmult vfp edsp java CPU implementer : 0x41 CPU architecture: STEJ CPU variant : 0x00 CPU part : 0x926 CPU part : 0x926 CPU revision : 5 Hardware : ARM-Versatile (Device Tree Support) Revision : 0000	/etc/init.d # cat	/proc/cpuinfo						
BogOMIPS : 1666.25 Features : swp half thumb fastmult vfp edsp java CPU implementer : 0x41 CPU architecture: STEJ CPU variant : 0x00 CPU part : 0x926 CPU revision : 5 Hardware : ARM-Versatile (Device Tree Support) Revision : 0000	processor :	0						
Features : swp half thumb fastmult vfp edsp java CPU implementer : 0x41 CPU architecture: STEJ CPU variant : 0x0 CPU part : 0x926 CPU revision : 5 Hardware : ARM-Versatile (Device Tree Support) Revision : 0000	model name :	ARM926EJ-S rev 5 (v5l)						
CPU implementer : 0x41 CPU architecture: STEJ CPU variant : 0x00 CPU part : 0x926 CPU revision : 5 Hardware : ARM-Versatile (Device Tree Support) Revision : 0000	BogoMIPS :	1666.25						
CPU architecture: STEJ CPU variant : 0x0 CPU part : 0x926 CPU revision : 5 Hardware : ARM-Versatile (Device Tree Support) Revision : 0000	Features :	swp half thumb fastmult v	fp edsp java					
CPU variant : 0x0 CPU part : 0x926 CPU revision : 5 Hardware : ARM-Versatile (Device Tree Support) Revision : 0000	CPU implementer :	0x41						
CPU part : 0x926 CPU revision : 5 Hardware : ARM-Versatile (Device Tree Support) Revision : 0000	CPU architecture:	5TEJ						
CPU revision : 5 Hardware : ARM-Versatile (Device Tree Support) Revision : 0000	CPU variant :	0×0						
Hardware : ARM-Versatile (Device Tree Support) Revision : 0000	CPU part :	0x926						
Revision : 0000	CPU revision :	5						
Revision : 0000								
Revision : 0000	Hardware :	ARM-Versatile (Device Tre	e Support)					
Serial : 00000000000000			245 B					
	Serial :	0000000000000000						





Security Testing – Examples / Demo

510 0 592 S /sbin/boa	← → C ▲ Nicht sicher 192.168.3.	137/services.cgi	
522 0 348 S /sbin/factoryreset			
523 0 392 S /sbin/ntronleds	N-IRC		702-W Series
524 0 376 S /sbin/devicereset	THE INDUSTRIAL NETWORK C	OMPANY	
531 0 684 R ps -ef / # ifconfig		PING WATCHDOG	
eth0 Link encap:Ethernet HWaddr 00:00:00:00:00:01	System Info	Enable Ping Watchdog:	
inet addr:192.168.3.137 Bcast:192.168.3.255 Mask:255.255.255.0	Link Setup	Enable Fing Waterluog.	
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1	Network	IP Address To Ping:	
RX packets:126 errors:0 dropped:0 overruns:0 frame:0 TX packets:144 errors:0 dropped:0 overruns:0 carrier:0	Advanced	Ping Interval:	300 seconds
collisions:645 txqueuelen:1000	Services	Startup Delay:	300 seconds
RX bytes:20180 (19.7 KiB) TX bytes:21151 (20.6 KiB)	System Config		
le link encenderel keenbeek	Support	Failure Count To Reboot:	3
lo Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0			Change
UP LOOPBACK RUNNING MTU:65536 Metric:1	Logout		
RX packets:0 errors:0 dropped:0 overruns:0 frame:0			
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0		SNMP AGENT	
collisions:0 txqueuelen:1000		Enable SNMP Agent:	\square
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)		-	
/ # netstat -tulen		SNMP Community:	public
p # netstat -tuten bin/ash: netstat: not found		Contact:	
/ # exit		I south an	
-bash-5.1# netstat -tulen		Location:	
Active Internet connections (only servers)			Change
Proto Recv-Q Send-Q Local Address Foreign Address State			
tcp 0 0 0.0.0.80 0.0.0.0:* LISTEN			



Security Testing – Examples / Demo

591 root 0:00 /usr/sbin/iw_webs ← → C	A Nicht sicher 192.168.3.137/home.asp												
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		IOAE.COIII											
- # netstat -tulen													
Antice Tetranet executions (enly execute)													
Proto Recv-Q Send-Q Local Address Foreign Address State	Menu												
	Ma	anaged Device Lis	t										
tcp 0 0 0.0.0:443 0.0.0.0:* LISTEN	verview												
								-					
tcp 0 0 0000000 00000 00000 00000 00000 0000	sic Settings Au	uto refresh						~					
	De	efresh timer						5					
- # ifconfig	System mo Settings							5					
	Nu	umber of managed A	P(s)					0					
inet addr:192.168.3.137 Bcast:192.168.3.255 Mask:255.255.255.0	Network Settings	0											
		umber of managed c	lient(s)					0					
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1	Time Settings												
	ntroller Settings			AP						Client			
TX packets:145 errors:0 dropped:0 overruns:0 carrier:0													
collisions:645 txqueuelen:1000	Basic WAC Settings					Noise						Signal	
RX bytes:22503 (21.9 KiB) TX bytes:23838 (23.2 KiB)		100000000000000000000000000000000000000		1000			-				RSSI		
	WAC Secure Settings	Hostname	IP	MAC	Channel	Level	Status	Hostname	IP	MAC	(dB)	Strength	Status
lo Link encap:Local Loopback						(dBm)					(ub)	(dBm)	
inet addr:127.0.0.1 Mask:255.0.0.0	Mobile IP Settings												
inet6 addr: ::1/128 Scope:Host	N	o data available in tab	1.										
UP LOOPBACK RUNNING MTU:65536 Metric:1	Ivanced Settings INO	b data available in tab	ae										
RX packets:0 errors:0 dropped:0 overruns:0 frame:0													
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0	SNMP Agent												
collisions:0 txqueuelen:1000													
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)	to Warning Settings												
~ # random: crng init done	System Log												
~ # cat /proc/cpuinfo													
processor : 0	System Log Event Types												
vendor id · GenuineIntel	and the second												
cpu family : 6	Syslog												
model : 6													
model name : OEMU Virtual CPU version 2.5+	Syslog Event Types												



Security Testing - Disclosed Vulnerabilities

Already Public:

- Red Lion N-Tron industrial access point
- Nexans industrial switch series
- Korenix industrial switch/access point/media converter device series
- PepperI+Fuchs industrial switch/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



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

Cyber Danube

Title: HITB 2022 – CyberDanube - Faking at Level 1 | Responsible: T. Weber | Version / Date: V1.0/2022-07 | Confidentiality Class: public