

Getting security objectives wrong

A cautionary tale of an Industrial Control System

Simon Foley
NTNU IIK Gjøvik
<mailto:simon.foley@ntnu.no>

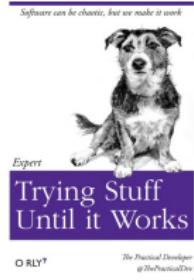
17 September, 2019

Getting security objectives wrong

A cautionary tale of an Industrial Control System

Simon Foley
NTNU IIK Gjøvik
<mailto:simon.foley@ntnu.no>

17 September, 2019



Outline of Talk

Networking recap

Motivation

The cautionary tale

Threat Management

Conclusion

Extra

TCP/IP Recap

[IP] A source system wants to send a message to a destination system.

Msg 1 : *Source → Destination : message*

The IP-address of the source and destination are contained in the Network header of the packets exchanged. The message data is contained in the application header.

However, when multiple messages are sent it is possible that they may arrive at the destination out-of-sequence or are even lost.

[TCP] facilitates correct ordering of data arriving reliably at destination socket connection.

Source system establishes a TCP connection to a port on a destination system, whereupon the source can send any amount of data and be sure that the destination application (associated with that port) receives the data in the correct order.

Network Application Example

For example, `sendmail` is a Unix application that is used to route, send and receive email messages. It runs on a server, 'listening' on Port 25 for requests from other systems.

For example, a user on `cosmos.ucc.ie` sends a request to the application running on `smtp.ucc.ie`:

```
> telnet smtp.ucc.ie 25
he1o cosmos.ucc.ie
mail from: <taoiseach@gov.ie>
rcpt to: <s.foley@cs.ucc.ie>
data
.....
```

The data related to the request (above) is contained within the application data of the packet.

Application does not provide authentication of sender: no check whether user/system sending request corresponds to originating email address.

Network Application Example

Inspecting packet sent from `cosmos.ucc.ie` to Port 25 on `smtp.cs.ucc.ie`, yields the following data (organized by header):

Physical	HWaddr (cosmos) 00:10:5A:4B:09:32, ...
Network	from 143.239.75.206 to 143.239.153.184 ...
Transport	... to port 25, ...
Application	mail from: <taoiseach@gov.ie> rcpt to: <s.foley@cs.ucc.ie> data

When the packet arrives at `smtp.ucc.ie`, a daemon, such as `xinetd` in Unix, knows that a packet arriving on Port 25 should be directed to the `sendmail` process. The `sendmail` process running on `smtp.ucc.ie` effectively receives the application data portion of this packet.

`sendmail` implements the SMTP protocol (an “application layer protocol”).

Sample Network Packet Content

tcpdump -A display traffic on a network (run here on smtp.cs.ucc.ie)

```
sudo tcpdump -A port smtp
[...]
09:25:45.143837 IP 143.239.74.165.50483 > neptune.cs.ucc.ie.smtp:
    P 1:21(20) ack 35 win 65535 <nop,nop,timestamp 157409668 291916037>
        U.....w.....J.....3.....a...fI.helo cosmos.ucc.ie
[...]
09:25:45.144090 IP neptune.cs.ucc.ie.smtp > 143.239.74.165.50483:
    P 35:55(20) ack 21 win 5792 <nop,nop,timestamp 291932278 157409668>
        U.....J....3.f.va..250 neptune.ucc.ie
[...]
09:26:23.078507 IP 143.239.74.165.50483 > neptune.cs.ucc.ie.smtp:
    P 21:48(27) ack 55 win 65535 <nop,nop,timestamp 157410047 291932278>
        U.....~.....J.....3.....a...f.vmail from: <taoiseach@gov.ie>
[...]
09:26:44.486250 IP 143.239.74.165.50483 > neptune.cs.ucc.ie.smtp:
    P 48:77(29) ack 69 win 65535 <nop,nop,timestamp 157410261 291970212>
        U.....J.....3.....a...g..rcpt to <s.foley@cs.ucc.ie>
```

Shodan

Searching for sites based on Internet header data

SHODAN port:25

TOTAL RESULTS: 8,055,444

TOP COUNTRIES:

Country	Results
United States	3,131,784
Japan	658,748
Germany	653,729
France	368,825
China	366,492

TOP ORGANIZATIONS:

Organization	Results
Google Cloud	801,022
Tencent cloud computing	235,398
DHV SAS	186,634
Unified Layer	178,631
home.pt webhosting farm - static abc...o...	164,071

TOP OPERATING SYSTEMS:

OS	Results
Linux 3.x	3,133
Windows 7 or 8	482
Linux 2.x	237
FreeBSD 8.x	108
Windows XP	65

TOP PRODUCERS:

Producer	Results
Postfix	1,830,620
Exim smtpd	761,147
Microsoft Exchange smtpd	212,496
Sendmail	176,849
MicrosoftExchange smtpd	147,203

48.43.198.105

Port:25

SSL Certificate

Issued By: NTT

Subject: 229-mail.studisiglapfahel1.it ESMTP Mdaemon 18.0.1; Med, 11 Sep 2018 12:26:17 +0200
229-mail.studisiglapfahel1.it Hello 241.248.192.224 (241.248.192.224), pleased to meet you
229-ETRN
229-UTH LOGIN CRAM-MD5 PLAIN
229-BESTMATCH
229-ENHANCEDSTATUSCODES
229-STEHTLS
229-SIZE
229-DRAFT
229-OPEN
229-LOGFILE
229-MAILERNAME
229-DSR
229-SMTPUTF8

83.211.193.32

Port:25

SSL Certificate

Issued By: mail.studisiglapfahel1.it
Common Name: mail.studisiglapfahel1.it
Organization: Studio Legato Fiduci
Issued To: studiolegato.it
Alternative Name: studisiglapfahel1.it
Organization: Studio Legato Fiduci

185.248.203.59

Port:25

SSL Certificate

Issued By: Saitama Consulting Co., Ltd
Common Name: www.saitama-consulting.com
Organization: Saitama Consulting Co., Ltd
Issued To: www.saitama-consulting.com

109.206.225.154

Port:25

SSL Certificate

Issued By: NTT

Subject: 229-dast09.soft-com.hiz ESMTP Postfix
229-dast09.soft-com.hiz
229-PGM1LN1K
229-ENHANCEDSTATUSCODES
229-CCTN
229-UTH PLAIN LOGIN DIGEST-MD5 CRAM-MD5
229-UTH PLAIN LOGIN DIGEST-MD5 CRAM-MD5
229-ENHANCEDSTATUSCODES
229-CRIME
229-DSR

46.43.198.105

Port:25

SSL Certificate

Issued By: NTT

Subject: 229-Fortuneland.co.jp ESMTP Postfix
229-Fortuneland.co.jp

Shodan

Searching for sites based on Internet header data

The screenshot shows the Shodan search interface with a search query of "port:25". The results are displayed under several categories:

- TOTAL RESULTS:** 2
- TOP COUNTRIES:** A world map showing the distribution of results.
- TOP CITIES:** A list of cities with their respective result counts:
 - 220 - Berlin, Germany
 - 200 - New York City, USA
 - 250 - SINGAPORE
 - 250 - BELGRADE
 - 250 - PENTING
 - 250 - DUBLIN
 - 250 - HELP
- TOP ORGANIZATIONS:** A list of organizations with their respective result counts:
 - 220 - Mail
 - 250 - Mail
 - 250 - Email
- TOP PRODUCTS:** A list of products with their respective result counts:
 - 5 - Sendmail
 - 5 - Exim 4.81

Each result entry includes a small thumbnail image of a server or device, a timestamp, and a brief description. At the bottom of the page, there is a copyright notice: "© 2013-2019, All Rights Reserved - Shodan®".

Shodan

Searching for sites based on Internet header data

The screenshot shows the Shodan search interface. At the top, there's a navigation bar with links for "Module", "Developer", "Dashboard", "View All", "Help Center", "My Account", and "Upgrade". Below the navigation is a search bar with a magnifying glass icon and a dropdown menu. To the right of the search bar are links for "Explore", "Downloads", "Reports", "Pricing", and "Enterprise Access".

The main area features a large map of the world with green and grey regions, representing different network segments or countries. Below the map, there are several search results:

- 143.** (with a globe icon) - This section includes fields for "City", "Country", "Organization", and "ISP". It also shows the "Last Update" as "2019-08-28T17:24:31.178019".
- Ports** (with a server icon) - Shows a count of 25 ports.
- Services** (with a gear icon) - Shows a count of 25 services. One service listed is "Sendmail" with the version "8.14.4B.54.6". The log entry for this service reads:

```
228-mail4 : ESMTP Sendmail 8.14.4/8.14.4; Wed, 28 Aug 2019 18:24:27 +0100
258-mail4 : Hello 237.111.7.85 [237.111.7.85], pleased to meet you
258 ENHANCEDSTATUSCODES
```

At the bottom of the page, there's a footer with the text "© 2013-2019, All Rights Reserved - Shodan®" and a series of navigation icons for back, forward, and search.

Shodan

Searching for sites based on Internet header data

The screenshot shows a Google search results page with the following details:

- Search Query:** ESMTP Sendmail 8.14.4/8.14.4
- Results:** About 5,890 results (0.33 seconds)
- Privacy Reminder:** A box from Google says "A privacy reminder from Google" with buttons for "REMIND ME LATER" and "REVIEW".
- First Result:**
 - Title:** Pentestit Lab v11 - ClamAV Token (9/12) - Jack Hacks
 - Link:** <https://jhalon.github.io/pentestit-lab-11-clamav-token/>
 - Text:** Sep 27, 2017 - root@cali-pentestit:~# 192.168.11.5 25 220 811-192.168.11.5-mail-dev
ESMTP Sendmail 8.14.4/8.14.4/Debian-8+deb8u2, Thu, 27 Jul 2017 ...
- Second Result:**
 - Title:** pentestit lab v11 Guide Part 7 | Innogen security Pentesting
 - Link:** <https://innogen-security.com/pentestit-lab-v11-guide-part-7/>
 - Text:** Aug 7, 2017 - 111-192-168-11-5-mail-dev ESMTP Sendmail 8.14.4/8.14.4/Debian-8+deb8u2.
After connecting to the smtp port a few times it was noticed ...
- Third Result:**
 - Title:** Using mail() for Remote Code Execution - Sogei ESEC Pentest
 - Link:** <https://www.cvedetails.com/posts/20111103/using-mail-for-remote-cod.../>
 - Text:** Nov 3, 2011 - The sendmail program provides several parameters and options which are ... 220 self.com ESMTP Sendmail 8.14.4/8.14.4/Debian-2ubuntu1.
- Fourth Result:**
 - Title:** Sendmail Sendmail version 8.14.4 : Security vulnerabilities
 - Link:** https://www.cvedetails.com/product/16-45/version_id-167023/Send.../
 - Text:** Jun 4, 2014 - Security vulnerabilities of Sendmail Sendmail version 8.14.4 List of cve security vulnerabilities related to this exact version. You can filter results ...
- Fifth Result:**
 - Title:** Sendmail SMTP HELO Argument Buffer Overflow Vulnerability
 - Link:** <https://www.securityfocus.com/bid/>
 - Text:** Apr 1, 1998 - Vulnerable: Sendmail Consortium Sendmail 8.14.4, Sendmail Consortium Sendmail 8.14.3, Sendmail Consortium Sendmail 8.13.8, Sendmail ...

Shodan

Searching for sites based on Internet header data

CVE Details

The ultimate security vulnerability datasource

Last 30 days

Home
Browse :
Vendors
Threats
Vulnerabilities By Date
Vulnerabilities By Type

Reports

CVE Score Report
CVSS Score Distribution
Search Reports

Vendor Search
Product Search
Virus Search
Vulnerability Search
Related References

Top 40 :

Vendors
Vendor CVE Scores
Products
Related CVE Scores
Vulnerabilities

Other :

Hackers Database
Attack Archives
CVSS Database
About & Contact
Feedback
CVE News
FAQ
Articles

External Links :

NVD Website

CVE Web Site

View CVE :

(e.g.: CVE-2009-1234 or
2010-1234 or 20111234)

View RDP :

(e.g.: 12345)

Search By Microsoft Reference ID :

(e.g.: m10-091 or

Vulnerability Details : [CVE-2014-3956](#)

The sm_close_on_exec function in confic in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.

(n.e.: DB-2008-1234 or 2010-1234 or 20111234)

View CVE

[Vulnerability Feed & Widgets](#)

[www.Iseeeds.com](#)

CVE@Score & Vulnerability Types

CVSS Score

6.6

Confidentiality Impact
Partial (There is considerable informational disclosure.)

Integrity Impact
None (There is no impact to the integrity of the system.)

Availability Impact
None (There is no impact to the availability of the system.)

Access Complexity
Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit.)

Authentication
Not required (Authentication is not required to exploit the vulnerability.)

Generic Access
None

Vulnerability Type(s)
Obtain Information

200

CWE ID

- Related OVAL Definitions

Title
Definition ID
Class Family

SUSE-SU-2014:0972-1 – Security update for sendmail
[oval.org/references/oval/2008](#)

oval (Open Vulnerability and Assessment Language) definitions define exactly what should be done to verify a vulnerability or a missing patch. Check out the OVAL definitions if you want to learn what you should do to verify a vulnerability.

- Products Affected By CVE-2014-3956

#	Product	Type	Vendor	Product	Version	Update	Edition	Language
1	OS	Operating System	Ubuntu	Ubuntu	20			Version Details Vulnerabilities
2	OS	Operating System	Ubuntu	Ubuntu	9.2	-		Version Details Vulnerabilities
3	Application	IF	None	None	8.11.31			Version Details Vulnerabilities
4	Application	Sendmail	Sendmail	Sendmail	8.6.7			Version Details Vulnerabilities
5	Application	Sendmail	Sendmail	Sendmail	8.7.6			Version Details Vulnerabilities
6	Application	Sendmail	Sendmail	Sendmail	8.7.7			Version Details Vulnerabilities
7	Application	Sendmail	Sendmail	Sendmail	8.7.8			Version Details Vulnerabilities
8	Application	Sendmail	Sendmail	Sendmail	8.7.9			Version Details Vulnerabilities
9	Application	Sendmail	Sendmail	Sendmail	8.7.10			Version Details Vulnerabilities
10	Application	Sendmail	Sendmail	Sendmail	8.8.8			Version Details Vulnerabilities

Shodan

Searching for sites based on Internet header data

The screenshot shows the Shodan search interface with the query "http.cookie". The results page displays various network nodes, each with a small thumbnail image and some identifying information.

Search Results:

- Ports:** 228 (vsFTPD 3.6.3), 558 (Login incorrect), 231 (Protocol login with USER and PASS), 231+features (SFTP, EPSF, NVTM, PASV, RECENT STREAM, ST25, TTFB, 211 End)
- Services:** 23 (OpenSSH - Version 7.4p1 Debian 10, Key type: ssh-rsa, cipher: 3des-ede-cbc@openssh.com, MAC: hmac-sha1@openssh.com, Kex: diffie-hellman-group-exchange-sha256, dh-group1-sha512, dh-group1-sha256, dh-group1-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group14-sha256, diffie-hellman-group1-sha512, diffie-hellman-group1-sha256, diffie-hellman-group1-sha1)
- OpenSSH - Version 7.4p1 Debian 10:** 559-2.0-OpenSSH_7.4p1 Debian 10

Vulnerabilities:

- CVE-2019-0116**: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.36. When the path component of a request URL contains multiple consecutive slashes ('//'), directives such as Location-Match and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse these.
- CVE-2019-0220**: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.36. When the path component of a request URL contains multiple consecutive slashes ('//'), directives such as Location-Match and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse these.
- CVE-2019-0217**: In Apache HTTP Server 2.4 release 2.4.36 or prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
- CVE-2019-0197**: A vulnerability was found in Apache HTTP Server 2.4.36 to 2.4.38. When a client sends a request for a https host or https://grade with encrypted session ticket, an upgrade request is sent to the https host over the encrypted connection. This could lead to a reconnection and crash. Server that never enabled the h2 protocol or that only enabled it for https and did not set "H2Upgrade on" by this issue.
- CVE-2019-0215**: In Apache HTTP Server 2.4 release 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions.
- CVE-2019-0211**: In Apache HTTP Server 2.4 release 2.4.17 to 2.4.36, with NMPM event, worker or prefork, code executing in less privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

Shodan

Searching for sites based on Internet header data

The screenshot shows a ZDNet article titled "Millions of Exim servers vulnerable to root-granting exploit". The article discusses a major security bug impacting the internet's most popular email server. It includes a photo of a server rack and links to other stories by the same author.

Millions of Exim servers vulnerable to root-granting exploit

The internet's most popular email server impacted by second major bug this summer



By Catalin Cimpanu for Zero Day | September 7, 2019 -- 2039 GMT (3:39 PDT) | Topic: Security

The screenshot shows two program banners from IE School of Business & Technology. The top banner is for the "Master in Visual and Digital Media" (October, English, 10 months, Full-time) with a "Discover More" button. The bottom banner is for the "Master in Business Analytics & Big Data" (April/October, English, 10 Months, Full-Time) with a "Discover More" button. Below the banners is a section titled "MORE FROM CATALIN CIAMPANU" featuring a link to a story about Google Chrome 77.



Manage Settings

Outline of Talk

Networking recap

Motivation

The cautionary tale

Threat Management

Conclusion

Extra

The Shodan search interface shows a search bar with the query "Industrial Control Systems". Below the search bar, there are navigation links for Explore, Downloads, Reports, Pricing, Enterprise Access, My Account, and Upgrade. The main content area displays a large image of an industrial facility with various pipes, tanks, and structures. A sidebar on the left lists search filters: Network, Port, OS, and Service.

Industrial Control Systems

Spotlight

XZERES Wind Turbine

XZERES Wind designs & manufactures wind energy systems for small wind turbine market designed for powering homes farms or businesses with clean energy.

[Explore](#)

What Are They?

In a nutshell, Industrial control systems (ICS) are computers that control the world around you. They're responsible for managing the air conditioning in your office, the turbines at a power plant, the lighting at the theatre or the robots at a factory.



PIPS Automated License Plate Reader

The PIPS AutoPlate Secure ALPR Access Control System catalogs all vehicles entering or exiting an access point to a site or facility.

[Explore](#)

Common Terms

ICS Industrial Control System

SCADA Supervisory Control and Data Acquisition

PLC Programmable Logic Controller

DCS Distributed Control System

Protocols

The following protocols are some of the languages that the industrial control systems use to communicate across the Internet. Many of them were developed before the Internet became widely used, which is why Internet-accessible ICS devices don't always require authentication - it isn't part of the protocol!



Modbus is a popular protocol for industrial control systems (ICS). It provides easy, raw access to the control system without requiring any authentication.

[Explore Modbus](#)[Explore Siemens S7](#)[Explore DNP3](#)

EtherNet/IP

The Fox protocol, developed as part of the Niagara framework from Tridium, is most commonly seen in building automation systems (offices, libraries, Universities, etc.)

[Explore Niagara Fox](#)

BACnet is a communications protocol for building automation and control networks. It was designed to allow communication of building automation and control systems for applications such as heating, air-conditioning, lighting, and fire detection systems.

[Explore BACnet](#)[Explore EtherNet/IP](#)

PHOENIX CONTACT

Service Request Transport Protocol (GE-SRTP) protocol is developed by GE Intelligent Platforms (earlier GE Fanuc) for transfer of data from PLCs.

[Explore GE-SRTP](#)

The HART Communications Protocol (Highway Addressable Remote Transducer Protocol) is an early implementation of Fieldbus, a digital industrial automation protocol. Its most notable advantage is that it can communicate over legacy wiring.

[Explore HART-IP](#)

PCWorx is a protocol and program by Phoenix Contact used by a wide range of industries.

[Explore PCWorx](#)

MELSEC-Q Series use a proprietary network protocol for communication. The devices are used by equipment and manufacturing facilities to provide high-speed, large volume data processing and machine control.

[Explore MELSEC-Q](#)

FINS, Factory Interface Network Service, is a network protocol used by Omron PLCs, over different physical networks like Ethernet, Controller Link, DeviceNet and RS-232C.

[Explore OMRON FINS](#)

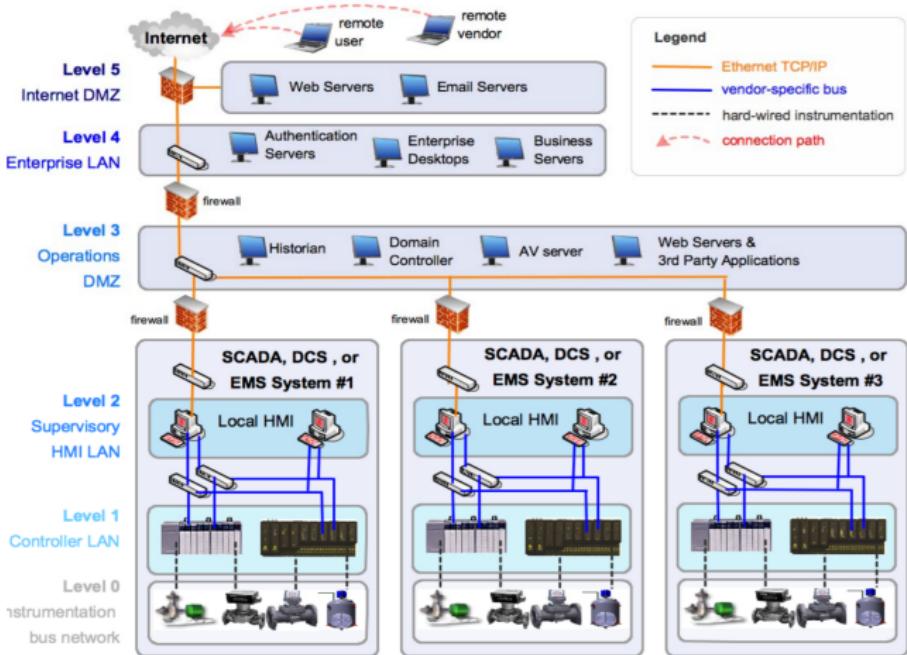
The protocol the Crimson v3.0 desktop software uses when communicating with the Red Lion Controls G3064 human machine interface (HMI).

[Explore Crimson v3](#)



SCADA / Industrial Control Systems

Supervisory Control and Data Acquisition

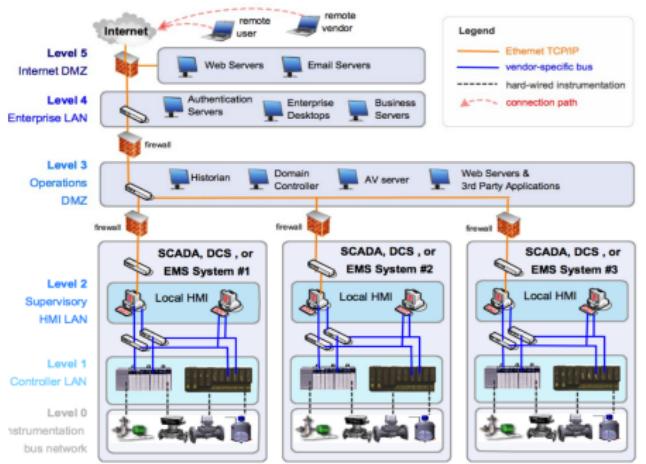


SCADA over public networks

One seemingly simple security objective

[...] SCADA communications should be encrypted and routed through a VPN tunnel through corporate IT or other non-critical networks. [...]"

[Securing the move to IP-based SCADA/PLC networks, UK Centre for the Protection of National Infrastructure (CPNI), 2011]



Use shodan to search for a use case

Siemens S7comm protocol over TCP/TSAP on Port 102

Shodan Developers Book View All... Show API Key

SHODAN port:102 Explore Downloads Reports Enterprise Access Contact Us My Account Upgrade

Exploits Maps Like 5 Download Results Create Report

TOP COUNTRIES

Country	Count
Poland	898
Germany	519
Italy	294
United States	252
Spain	230

Total results: 3,618
37.84.36.184
 Deutsche Telekom AG
 Action on: 2016-03-23 14:40:47 GMT
 Germany
[Details](#)

89.113.3.164
 VimperCom
 Action on: 2016-03-23 14:35:09 GMT
 Russian Federation
[Details](#)

81.165.25.69
 telekom-nw
 Action on: 2016-03-23 14:17:01 GMT
 Belgium, Ranst
[Details](#)

Copyright: Original Siemens Equipment
 PLC name: SIMATIC 300 (1)
 Module type: CPU 313C-2 DP
 Unknown (129): Boot Loader A
 Module: 6ES7 313-6CF03-0AB0 v.0.2
 Basic Firmware: v.2.6.4
 Module name: CPU 313C-2 DP
 Serial number of module: 5 C-VOH756222987
 Plant identification:
 Basic Hardware: 6...

217.92.140.217
 iperfectconnect.de
 Deutsche Telekom AG
 Action on: 2016-03-23 14:16:56 GMT
 Germany
[Details](#)

Basic Hardware: 6ES7 315-2AG10-0AB0 v.0.4
 Module: 6ES7 315-2AG10-0AB0 v.0.4
 Basic Firmware: v.2.0.11

The ICS use case

Siemens S7comm protocol over TCP/TSAP on Port 102

Shodan Developers Book View All... Explore Downloads Reports Enterprise Access Contact Us My Account Upgrade

86.4 [REDACTED] Ports

86.4 [REDACTED]

wtd.eircom.net

City [REDACTED]

Country Ireland

Organization Eircom

ISP Eircom

Last Update 2016-03-09T19:51:16.830084

Hostnames [REDACTED] wtd.eircom.net

ASN [REDACTED]

Ports

102 1723 2000 7547

Services

102 Basic Hardware: 6E57 315-2AG10-BAB0 v.0.5
1723 Basic Firmware: v.2.0.12
S7

1723 Firmware: 0 Hostname: Vendor: Microsoft
tcp pptp

7547 Ntp http

HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="Huawei@OneGateway",nonce="e8f536c11a5554b"
9ffef73899e633f808, qop="auth", algorithm="H05"
Content-Length: 0

What have we found?

Google search results for "6es7 315-2ag10-0ab0".

Privacy reminder from Google:

- REMIND ME LATER
- REVIEW

Data sheet 6ES7315-2AG10-0AB0 - Industry Support Siemens
<https://support.industry.siemens.com/tedservices/DatasheetService?DataSheetId=6ES7315-2AG10-0AB0>

May 9, 2019 · 6ES7315-2AG10-0AB0, ***Spare part*** SIMATIC S7-300, CPU 315-2DP Central processing unit with MPI Integr. power supply 24 V DC Work ...

Product Details - Industry Mail ...
<https://mail.industry.siemens.com/mall/Catalog/6ES7315-2AG10-0AB0>

6ES7315-2AG10-0AB0, Product, ***Spare part*** SIMATIC S7-300, CPU 315-2DP Central processing unit with MPI Integr. power supply 24 V DC Work memory ...

People also search for
 6es7 315-2ag10-0ab0 price 6es7 315-2ah14-0ab0

Network port and service monitoring interface.

Ports:

- 102 (TCP)
- 1723 (TCP)
- 2000 (TCP)
- 7547 (TCP)

Services:

102	Basic Hardware: 6ES7 315-2AG10-BAB0 v.0.5
tcp	Module: 6ES7 315-2AG10-BAB0 v.0.5
67	Basic Firmware: v.2.0.12

1723 (TCP): Firmware: 0, Hostname: , Vendor: Microsoft

7547 (TCP): http

HTTP/1.1 401 Unauthorized
 Connection: Keep-Alive
 WWW-Authenticate: Digest realm="SubstationControlArea",nonce="e8f536c11a554b96fe739996533f08",qop="auth",algorithm="MD5"

What have we found?

Google search results for "6es7 315-2ag10-0ab0":

- A privacy reminder from Google**
- REMIND ME LATER** **REVIEW**
- [PDF] Data sheet 6ES7315-2AG10-0AB0 - Industry Support Siemens**
<https://support.industry.siemens.com/tedsservices/DatasheetService/Detail...>
 May 9, 2019 · 6ES7315-2AG10-0AB0, ***Spare part*** SIMATIC 37-300, CPU 315-2DP Central processing unit with MPI Integr. power supply 24 V DC Work ...
- 6ES7315-2AG10-0AB0 - Product Details - Industry Mail ...**
<https://mail.industry.siemens.com/mall/catalog/6ES7315-2AG10-0AB0> • 6ES7315-2AG10-0AB0, Product, ***Spare part*** SIMATIC 37-300, CPU 315-2DP Central processing unit with MPI Integr. power supply 24 V DC Work memory ...
- People also search for**
 6es7 315-2ag10-0ab0 price 6es7 315-2ah14-0ab0



Network port scanning results:

Port	Protocol	Module	Firmware
102	tcp	6ES7 315-2AG10-0AB0 v.0.5	Basic Firmware: v.2.0.12
1723	tcp		
2000	tcp		
7547	tcp		
7547	http		

Services:

Port	Protocol	Module	Firmware	Hostname	Vendor
102	tcp	6ES7 315-2AG10-0AB0 v.0.5	Basic Firmware: v.2.0.12		
1723	tcp				
2000	tcp				
7547	tcp				
7547	http				

HTTP Headers (Port 102):

```

HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="Siemens@192.168.1.10",nonce="e8f536c1a554b
f96fe73999e633f08",qop="auth",algorithm="MD5"
Content-Type: application/digest-nego
Content-Length: 0
Date: Mon, 10 Jun 2019 10:45:20 GMT

```

Are there any published vulnerabilities?

Search the CVE vulnerability database via CVE details



Are there any published vulnerabilities?

Search the CVE vulnerability database via CVE details

CVE Details
The ultimate security vulnerability database

Search: Search | View CSV | Vulnerability Feed & Migrations | www.cvedetails.com

Siemens S7-300

Current CVSS Score Distribution for All Vulnerabilities

Distribution of all vulnerabilities by CVSS Score.

CVSS Score Range	Count	CVSS Score Range	Count
0.0 - 3.9	834	6.0 - 6.9	1
4.0 - 6.9	102	7.0 - 7.9	1
7.0 - 7.9	675	8.0 - 8.9	1
8.0 - 8.9	482	9.0 - 9.9	1
9.0 - 9.9	200	10.0	1
Total	2320		

CVSS Score Range Legend:

- 0.0 - 3.9
- 4.0 - 6.9
- 7.0 - 7.9
- 8.0 - 8.9
- 9.0 - 9.9
- 10.0

Weighted Average CVSS Score: 8.40

Looking for OVAL (Open Vulnerability and Assessment Language) definitions? <https://www.cvedetails.com> allows you to view exact details of OVAL/Open Vulnerability and Assessment Language definition and see exactly what you should do to verify a vulnerability. It is fully integrated with cvedetails so you will be able to see related definitions related to a product or a CVE entry.

Additional Links:

- [OVAL](#)
- [RSS](#)
- [Atom](#)
- [JSON](#)
- [HTML](#)

Siemens SIMATIC S7-300 Firmware - CVE security vulnerabilities ...
<https://www.cvedetails.com/references/Siemens-S7-300-Firmware-CVE/>

Siemens SIMATIC S7-300 Firmware security vulnerabilities, exploits, mitigations, modules, vulnerability statistics and list of versions.

Siemens SIMATIC S7-300 Firmware - List of security vulnerabilities

View all security vulnerabilities for Siemens SIMATIC S7-300 Firmware. List of all related CVE security vulnerabilities, CVSS Scores, vulnerability details and links to full details.

CVE-2010-0159 - A vulnerability has been identified in SIMATIC S7...
<https://www.cvedetails.com/cve/CVE-2010-0159/>
Jan 26, 2010 - A vulnerability has been identified in SIMATIC S7-300 CPU family, SIMATIC S7-400 V8 and earlier CPU family, SIMATIC S7-400 V7 CPU family.

CVE-2010-2177 - Siemens SIMATIC S7-300 CPU devices allow ...
<https://www.cvedetails.com/cve/CVE-2010-2177/>
Jan 1, 2010 - Siemens SIMATIC S7-300 CPU devices allow remote attackers to cause a denial of service (buffer mode transition) via crafted packets on TIA.

CVE-2010-1661 - A vulnerability has been identified in SIMATIC S7...
<https://www.cvedetails.com/cve/CVE-2010-1661/>
Apr 10, 2010 - A vulnerability has been identified in SIMATIC S7-300 CPU (All versions > V3.0, V4). The affected CPUs improperly validate S7 communication.

CVE-2010-0150 - A vulnerability has been identified in SIMATIC S7-300 CPU family ...
<https://www.cvedetails.com/cve/CVE-2010-0150/>
Jan 26, 2010 - A vulnerability has been identified in SIMATIC S7-300 CPU family, SIMATIC S7-400 V8 and earlier CPU family, SIMATIC S7-400 V7 CPU family.

CVE-2010-2176 - A vulnerability has been identified in SIMATIC S7-300 CPU family ...
<https://www.cvedetails.com/cve/CVE-2010-2176/>

CVE-2010-3469 - Siemens SIMATIC S7-300 Profinet-enabled CPU ...
<https://www.cvedetails.com/cve/CVE-2010-3469/>
Aug 1, 2010 - Siemens SIMATIC S7-300 Profinet-enabled CPU devices with firmware before 3.2.12 and SIMATIC S7-300 Profinet-enabled CPU devices with v0.1.

CVE-2010-0672 - The integrated web server on Siemens SIMATIC ...
<https://www.cvedetails.com/cve/CVE-2010-0672/>

Are there any published vulnerabilities?

Search the CVE vulnerability database via CVE details

CVE Details
The ultimate security vulnerability database

Siemens S7-300

Current CVSS Score Distribution For All Vulnerabilities

CVSS Score Range	Number of Vulnerabilities
0-10	~2500
11-20	~1500
21-30	~1000
31-40	~500
41-50	~200
51-60	~100
61-70	~50
71-80	~20
81-90	~10
91-100	~5
Total	~5500

Avg CVSS Score: 15.30

Looking for XNA? (Open Vulnerability and Assessment Language) definitions? <https://www.cvedetails.com> allows you to store exact details of XNA/Open Vulnerability and Assessment Language definition and exactly what you should do to verify a vulnerability. It is fully integrated with cvedetails so you will be able to search definitions related to a product or a CPE name.

Search CVE entry with XNA definitions - [CVE-2007-0001](https://www.cvedetails.com)

CVE Details
The ultimate security vulnerability database

Siemens, Siemens S7-300 Firmware - CVE security vulnerabilities ...

Siemens S7-300 Firmware security vulnerabilities, exploits, mitigations, modules, vulnerability statistics and list of versions.

Siemens, Siemens S7-300 Firmware - List of security vulnerabilities

View Details | View History | View Issues | View References | View CVSS | View CVN | View CVN ID | View CVN URL | View CVN File | View CVN PDF

Security vulnerabilities of Siemens S7-300 Firmware - List of all related CVE security vulnerabilities. CVE Issues, vulnerability details and links to full details.

CVE-2018-0159 - A vulnerability has been identified in SIMATIC S7 ...

Apr 10, 2018 - A vulnerability has been identified in SIMATIC S7-300 CPU family, SIMATIC 3T-400 V8 and earlier CPU family, SIMATIC 3T-400 V7 CPU family.

CVE-2019-2177 - Siemens SIMATIC S7-300 CPU devices allow ...

Jan 23, 2019 - A vulnerability has been identified in SIMATIC S7-300 CPU devices allowing remote attackers to cause a denial of service (denial mode transition) via crafted packets on (1) TCP port 302 or (2) UDP port 302.

CVE-2018-1661 - A vulnerability has been identified in SIMATIC S7 ...

Apr 10, 2018 - A vulnerability has been identified in SIMATIC S7-300 CPU (All versions < v3.0. 1). The affected CPUs improperly validate S7 communication.

CVE-2018-0158 - A vulnerability has been identified in SIMATIC S7 ...

Apr 10, 2018 - A vulnerability has been identified in SIMATIC S7-300 CPU family, SIMATIC 3T-400 V8 and earlier CPU family, SIMATIC 3T-400 V7 CPU family.

CVE-2018-3469 - Siemens SIMATIC S7-300 Profinet-enabled CPU ...

Aug 10, 2018 - Siemens SIMATIC S7-300 Profinet-enabled CPU devices with firmware before 3.2.12 and SIMATIC S7-300 Profinet-enabled CPU devices with v3.0.1.

CVE-2018-0172 - The integrated web server on Siemens SIMATIC ...

Aug 10, 2018 - The integrated web server on Siemens SIMATIC...

CVE Details
The ultimate security vulnerability database

CVE-2019-2177 - Siemens SIMATIC S7-300 CPU devices allow remote attackers to cause a denial of service (denial-mode transition) via crafted packets on (1) TCP port 302 or (2) UDP port 302.

Published Date : 2019-01-23 Last Update Date : 2019-01-01

Vulnerability Details - CVE-2019-2177

Siemens SIMATIC S7-300 CPU devices allow remote attackers to cause a denial of service (denial-mode transition) via crafted packets on (1) TCP port 302 or (2) UDP port 302.

Links

- Get Details
- Report ID
- CVSS Score Result
- CVSS Score Distribution
- Details
- Vendor Search
- Product Search
- Version Search
- Vendor Details
- Product Details
- Version Details
- Vendor Details
- Product Details
- Version Details
- Product Details
- External Links
- References
- Metasploit Modules Related To CVE-2019-2177

CVSS Scores & Vulnerability Types

Type	CVSS Score	Confidentiality, Integrity, Availability Impact	CVSS Score	Confidentiality, Integrity, Availability Impact
Information Disclosure	6.1	None (There is no impact to the confidentiality of the system.)	6.1	None (There is no impact to the integrity of the system.)
Denial of Service	7.8	Complete (There is a total loss of the affected resource.)	7.8	Complete (The attacker can render the resource completely unavailable.)
Access Complexity	Low	Low (Exploitation requires little knowledge or skill and is required to exploit.)	Low	Low (Exploitation requires little knowledge or skill and is required to exploit.)
Authentication	Required	Required (Authentication is not required to exploit the vulnerability.)	Required	Required (Authentication is not required to exploit the vulnerability.)
Confidentiality	None	None	None	None
Integrity	None	None	None	None
Availability	High	High (A significant portion of the affected resource is lost or becomes unavailable.)	High	High (A significant portion of the affected resource is lost or becomes unavailable.)

Products Affected By CVE-2019-2177

Product Type	Vendor	Product	Version	Update	Edition	Language
Industrial	Siemens	SIMATIC 3T-300 CPU	v3.0.0			
Industrial	Siemens	SIMATIC 3T-300 CPU Firmware	v3.0.0			

Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
Siemens	SIMATIC 3T-300 CPU	1
Siemens	SIMATIC 3T-300 CPU Firmware	1

References For CVE-2019-2177

- <https://www.siemens.com/cve/1633290> SECURITY 1633290
- <https://www.siemens.com/cve/1635202> EXPLOIT-01-4498
- https://www.siemens.com/innovation/assets/der/technologies/der-security_advisory_sse-M7628.pdf CONFIRM
- <https://www.metasploit.com/modules/search/?q=S7-300-284-04>

There are not any metasploit modules related to this CVE entry. (Please visit www.metasploit.com for more information.)

How Does It Work? Known Vulnerabilities & Technical Details

A denial of service vulnerability

(at least for this version v.0.5/v.2.0.12)

ICS Advisory (ICSA-15-064-04)

Siemens SIMATIC S7-300 CPU Denial-of-Service Vulnerability

Original release date: March 05, 2015 | Last revised: August 22, 2018

Legal Notice

All information products included in <http://ics-cert.us-cert.gov> are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within DHS sites. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see <http://www.us-cert.gov/tlp>.

OVERVIEW

Johannes Klick, Christian Pfleßl, Martin Gebert, and Lucas Jacob from Freie Universität Berlin's work team SCADACS have identified a Denial-of-Service (DoS) vulnerability in Siemens SIMATIC S7-300 CPUs. Siemens has developed mitigations for this vulnerability.

This vulnerability could be exploited remotely.

AFFECTED PRODUCTS

The following SIMATIC S7-300 CPUs are affected:

- SIMATIC S7-300 CPU family: all versions.

IMPACT

This vulnerability could allow attackers to perform a DoS attack over the network without prior authentication against S7-300 CPUs under certain conditions. A cold restart is required to recover the system.

Impact to individual organizations depends on many factors that are unique to each organization. NCCIC/ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

BACKGROUND

Siemens is a multinational company headquartered in Munich, Germany.

The affected product, SIMATIC S7-300 CPU, have been designed for process control in industrial environments. This product is deployed across several sectors including Chemical, Energy, Food and Agriculture, and Water and Wastewater Systems. Siemens estimates that these products are used primarily in the United States and Europe with a small percentage in Asia.

VULNERABILITY OVERVIEW

DENIAL-OF-SERVICE ATTACK^a

Specifically crafted packets sent to Port 102/TCP (ISO-TSAP) or via Profibus could cause the affected device to go into defect mode. A cold restart is required to recover the system.

CVE-2015-2177^b has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (R/2.0/A/C1.4/C/N/I/N/A/C).^c

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

Crafting a working exploit for this vulnerability would be difficult.

MITIGATION

Siemens recommends the following mitigations:

- Apply protection-level 3 (Read/Write protection),
- Apply cell protection concept.^d
- Use VPN to protecting network communication between cells, and
- Apply Defense-in-Depth.^e

For more information on these vulnerabilities and detailed instructions, please see Siemens Security Advisory SSA-981029 at the following location:

<http://www.siemens.com/cert/advisories/0>

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.

ICS-CERT also provides a section for control systems security recommended practices on the ICS-CERT web page at: <http://ics-cert.us-cert.gov/content/recommended-practices>. Several recommended practices are available for reading and download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*. ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, [ICS-TIP-12-246-01B - Targeted Cyber Intrusion Detection and Mitigation Strategies](http://ics-cert.us-cert.gov/content/recommended-practices), that is available for download from the ICS-CERT web site (<http://ics-cert.us-cert.gov>).

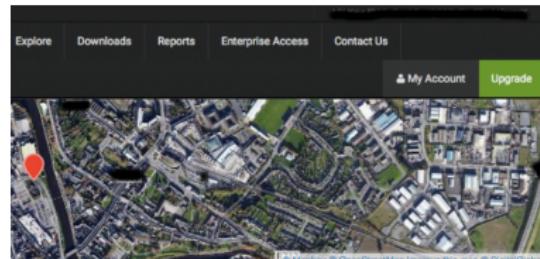
Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

Vulnerabilities

S7comm on Port 102

CVE-2015-2177 Denial of service;
Preset userid/password Basisk;



Ports

102 1723 2000 7547

Services

102 Basic Hardware: 6E57 315-2AG18-0AB0 v.0.5
tcp Module: 6E57 315-2AG18-0AB0 v.0.5
s7 Basic Firmware: v.2.0.12

1723 Firmware: 0
tcp Hostname:
pptp Vendor: Microsoft

7547
tcp
http

HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="e8f536c11a5554bf96fe73099e63f80",qop="auth",algorithm="MD5"
Content-Length: 0

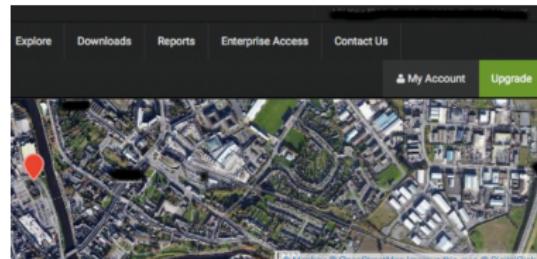
Vulnerabilities

S7comm on Port 102

CVE-2015-2177 Denial of service;
Preset userid/password Basisk;

PPTP on Port 1723

MS Security Advisory 2743314:
MS-CHAPv2 weakness; . . .



Ports

102 1723 2000 7547

Services

102 Basic Hardware: 6E57 315-2AG1B-0AB0 v.0.5
tcp Module: 6E57 315-2AG1B-0AB0 v.0.5
s7 Basic Firmware: v.2.0.12

1723 Firmware: 0
tcp Hostname:
pptp Vendor: Microsoft

7547
tcp
http

HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="e0f536c11a5554bf96fe73099e63f80",qop="auth",algorithm="MD5"
Content-Length: 0

Vulnerabilities

S7comm on Port 102

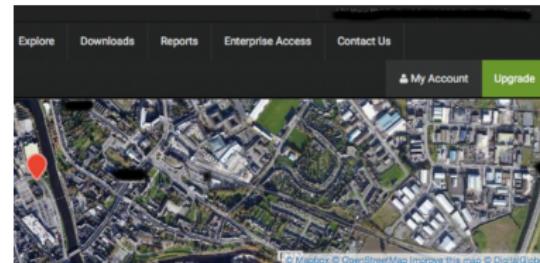
CVE-2015-2177 Denial of service;
Preset userid/password Basisk;

PPTP on Port 1723

MS Security Advisory 2743314:
MS-CHAPv2 weakness; . . .

CWMP over HTTP

CVE-2014-9222, CVE-2014-9223:
misfortune cookie vulnerability; . . .



Vulnerabilities

S7comm on Port 102

CVE-2015-2177 Denial of service;
Preset userid/password Basisk;

PPTP on Port 1723

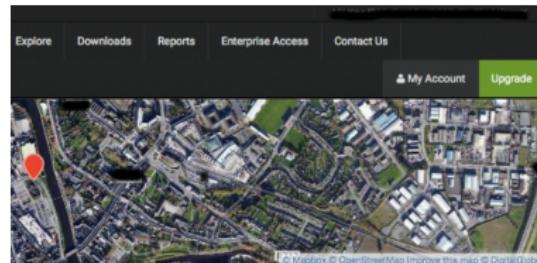
MS Security Advisory 2743314:
MS-CHAPv2 weakness; . . .

CWMP over HTTP

CVE-2014-9222, CVE-2014-9223:
misfortune cookie vulnerability; . . .

Huawei home gateway

CVE-2015-7254 path traversal;
CVE-2013-6786 embedded web
server XSS; . . .



Vulnerabilities

S7comm on Port 102

CVE-2015-2177 Denial of service;
Preset userid/password Basisk;

PPTP on Port 1723

MS Security Advisory 2743314:
MS-CHAPv2 weakness; ...

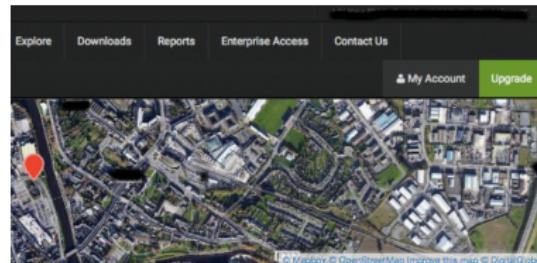
CWMP over HTTP

CVE-2014-9222, CVE-2014-9223:
misfortune cookie vulnerability; ...

Huawei home gateway

CVE-2015-7254 path traversal;
CVE-2013-6786 embedded web
server XSS; ...

At least there's no SCADA
embedded webserver!



What exactly are the objectives?

The security expert's view

- Security properties, ...
- Setup a VPN, use a firewall, punch a hole for VPN traffic, ...



What exactly are the objectives?

The security expert's view

- Security properties, ...
- Setup a VPN, use a firewall, punch a hole for VPN traffic, ...



Convoluted Systems: the user's view

- Configuration efficacy based on user expertise and best practices.
- Dealing with multiple objectives is difficult.



Outline of Talk

Networking recap

Motivation

The cautionary tale

Threat Management

Conclusion

Extra

The ICS use case

Siemens S7comm protocol over TCP/TSAP on Port 102

Shodan Developers Book View All... Explore Downloads Reports Enterprise Access Contact Us My Account Upgrade

86.4 [REDACTED] Ports

86.4 [REDACTED]

wtd.eircom.net

City [REDACTED]

Country Ireland

Organization Eircom

ISP Eircom

Last Update 2016-03-09T19:51:16.830084

Hostnames [REDACTED] wtd.eircom.net

ASN [REDACTED]

Ports

102 1723 2000 7547

Services

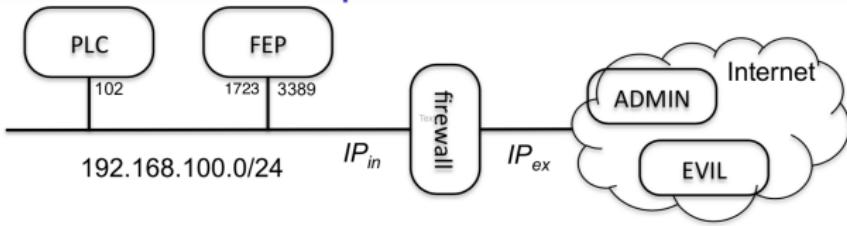
102 Basic Hardware: 6E57 315-2AG10-BAB0 v.0.5
102 Basic Firmware: v.2.0.12

1723 Firmware: 0 Hostname:
tcp Vendor: Microsoft
pptp

7547 Ntp http

HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="Huawei@OneGateway",nonce="e8f536c11a5554b"
f96fe73899e633f808, qop="auth", algorithm="H05"
Content-Length: 0

Possible setup behind the scenes?



Use a Virtual Private Network



Siemens FAQ8970169

"Port 102 is blocked by default in routers and firewalls and must be enabled for the complete transfer route"

Original firewall policy

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	≥ 1024	PLC	102	ALLOW
2	...	*.*.*.*	≥ 1024	FEP	1723	ALLOW

From: Simon Foley
Subject: XXX Cyber Physical System
Date: March 23, 2016 at 12:02:31 PM GMT+1
To: XXX

Dear XXX,

[...] In preparing a talk on Cyber Physical Systems security I came across an issue on a system which, if I was to guess, is operated by XXX, and wanted to draw your attention to this, in your capacity as [...]

A screenshot with the details is attached and Shodan reports the address of the building as XXX, which, looking at Google Streetview, seems to have some relationship with XXX. In case you're not familiar with it, Shodan.io is an Internet search engine that [...]

Of concern is that Port 102 on the system is reported as open to the Internet. Siemens' S7comm protocol runs over Port 102 and is used for communications between programmable logic controllers and SCADA systems. Looking at the header information it looks like there's a Siemens SIMATIC S7-300 PLC (315-2DP CPU) controller at this address. For example, CVE-2015-2177 [1] notes that versions of the SIMATIC S7-300 is vulnerable to denial of service attack via this protocol as described by Beresford [2], who also discovered a hardcoded userid/password ('Basisk') for internal diagnostic functions [3].

I'm speculating here about the connected system, based on the Shodan report, and no attempt was made to access/test the system.

Best practices, for example [4], recommend that the controller and PLCs should be deployed on an internal control network and a VPN tunnel used when accessing the controller over the Internet/public network. VPN access to the local Control Network does appear to be provided via PPTP on Port 1723 on the system, however, it looks like the S7comm Port (102) has been (perhaps accidentally) left open. The S7comm service on Port 102 should not be directly accessible over a public network.

If this is not a XXX controlled system then perhaps you might be able to suggest who the owner might be so that I can contact them?

Best regards,

Simon Foley

Postscript - March 2016

SHODAN Developers Book View All... Show API Key My Account Upgrade

86 [REDACTED]

City	[REDACTED]
Country	Ireland
Organization	Eircom
ISP	Eircom
Last Update	2016-03-25T12:35:41.030138
Hostnames	86-[REDACTED]
ASN	AS5466

Ports

102 1723 2000 3389 7547

Services

102 Basic Hardware: 6E57 315-2AG1B-0A8B v.0.5
Module: 6E57 315-2AG1B-0A8B v.0.5
s7 Basic Firmware: v.2.0.12

1723 Firmware: 0
Hostname:
Vendor: Microsoft
tcp
ppp

3389 Remote Desktop Protocol
tcp
rdp
\x03\x00\x00\x00\x00\x00\x00\x00\x124\x00

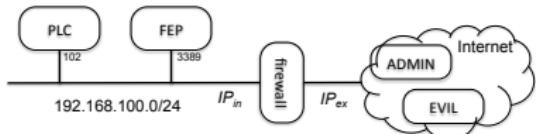
7547
tcp
http

HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="e0f536c11a5554bf96fe73099e633f80",qop="auth",algorithm="MD5"
Content-Length: 0

[Navigation icons: back, forward, search, etc.]

Firewall policy objectives

(Keep things simple: VPN via Port 3389)

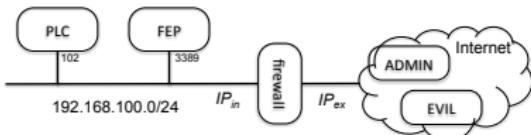


Initial policy *UPol*

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	≥ 1024	PLC	102	ALLOW
2	...	*.*.*.*	≥ 1024	FEP	3389	ALLOW

Firewall policy objectives

(Keep things simple: VPN via Port 3389)



Initial policy *UPol*

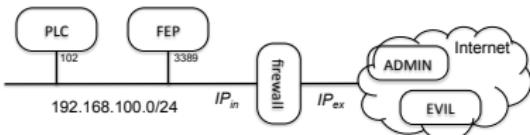
Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	≥ 1024	PLC	102	ALLOW
2	...	*.*.*.*	≥ 1024	FEP	3389	ALLOW

CPNI Recommendations: *CPNI*

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	192.168.100.0/24	≥ 1024	PLC	102	ALLOW
2	...	external IPs	*	PLC	102	DROP
3	...	external IPs	≥ 1024	FEP	3389	ALLOW

Firewall policy objectives

(Keep things simple: VPN via Port 3389)



Initial policy *UPol*

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	≥ 1024	PLC	102	ALLOW
2	...	*.*.*.*	≥ 1024	FEP	3389	ALLOW

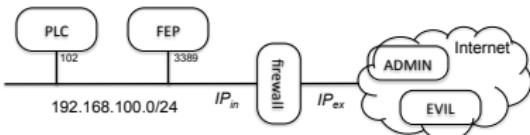
CPNI Recommendations: *CPNI*

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	192.168.100.0/24	≥ 1024	PLC	102	ALLOW
2	...	external IPs	*	PLC	102	DROP
3	...	external IPs	≥ 1024	FEP	3389	ALLOW

Remote Desktop Policy: *RPol*

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	ADMIN	≥ 1024	FEP	3389	ALLOW
2	...	*.*.*.*	*	FEP	3389	DROP

Composition of policy objectives

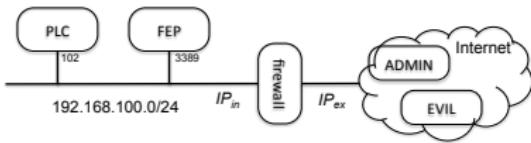


UPol;CPNI;RPol

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	≥ 1024	PLC	102	ALLOW
2	...	*.*.*.*	≥ 1024	FEP	3389	ALLOW
3	...	192.168.100.0/24	≥ 1024	PLC	102	ALLOW
4	...	external IPs	*	PLC	102	DROP
5	...	external	≥ 1024	FEP	3389	ALLOW
6	...	ADMIN	≥ 1024	FEP	3389	ALLOW
7	...	*.*.*.*	*	FEP	3389	DROP

Each firewall rule takes the form of a series of conditions on packet fields that must be met in order for that rule to be applicable, with a consequent action for the matching packet. Given a network packet, the rules are tested in the order in which they appear in the table. Once a packet has been successfully matched against a rule, no further rule tests are carried out for that packet.

Composition of policy objectives



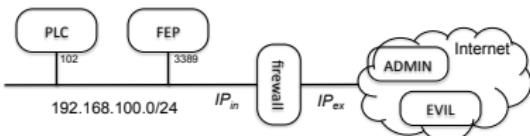
UPol;CPNI;RPol

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	≥ 1024	PLC	102	ALLOW
2	...	*.*.*.*	≥ 1024	FEP	3389	ALLOW
3	...	192.168.100.0/24	≥ 1024	PLC	102	ALLOW
4	...	external IPs		PLC	102	DROP
5	...	external		FEP	3389	ALLOW
6	...	ADMIN	≥ 1024	FEP	3389	ALLOW
7	...	*.*.*.*	*	FEP	3389	DROP

Each firewall rule takes the form of a series of conditions on packet fields that must be met in order for that rule to be applicable, with a consequent action for the matching packet. Given a network packet, the rules are tested in the order in which they appear in the table. Once a packet has been successfully matched against a rule, no further rule tests are carried out for that packet.

Composition of policy objectives

UPol;CPNI;RPol



Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*	≥ 1024	PLC	102	ALLOW
2	...	*.*.*	≥ 1024	FEP	3389	ALLOW
3	...	192.168.100.0/24	≥ 1024	PLC	102	ALLOW
4	...	external IPs	*	PLC	102	DROP
5	...	external	≥ 1024	FEP	3389	ALLOW
6	...	ADMIN	≥ 1024	FEP	3389	ALLOW
7	...	*.*.*	*	FEP	3389	DROP

A **redundancy** conflict occurs when two firewall rules can filter the same packets and those rules have the same target actions over those packets and that the removal of the redundant rule does not affect the semantics of the firewall configuration.

A **shadowing** conflict occurs when a rule is never matched due to a previous rule filtering the same kinds of packets (equivalence or subsumption) and both rules have different target actions.

Postscript - May 2016

Shodan Developers Book View All... Show API Key

port:102 country:'IE'

Exploits Maps Share Search Download Results Create Report Upgrade

TOP COUNTRIES

Ireland 4

TOP CITIES

Dublin 2

TOP ORGANIZATIONS

Organization	Count
Microsoft Azure	1
Amazon.com	1

23.102.62.210
Microsoft Azure
Added on 2016-06-13 05:57:12 GMT
Ireland, Dublin
[Details](#)

Location designation of a module:
Copyright: Original Siemens Equipment
Module type: IM151-8 PNP/DP CPU
PLC name: Techendrome
Module: v.8.0
Plant identification: Mouser Factory
OEM ID of a module:
Module name: Siemens, SIMATIC, ST-200
Serial number of module: 88111222

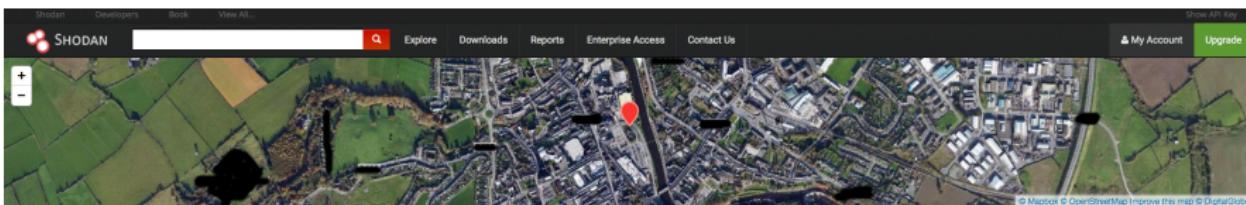
52.30.77.31
ec2-52-30-77-31.eu-west-1.compute.amazonaws.com
Amazon AWS
Added on 2016-06-06 10:59:38 GMT
Ireland, Dublin
[Details](#)

Location designation of a module:
Copyright: Original Siemens Equipment
Module type: IM151-8 PNP/DP CPU
PLC name: Techendrome
Module: v.8.0
Plant identification: Mouser Factory
OEM ID of a module:
Module name: Siemens, SIMATIC, ST-200
Serial number of module: 88111222

© 2013-2016, All Rights Reserved - Shodan®

Postscript - June 2016

SHODAN Show API Key Upgrade



86 [REDACTED]

Ports

102 3389 7547

Services

102 Copyright: Original Siemens Equipment
tcp PLC name:
s7 Module type: CPU 315-2 DP
Unknown (129) Boot Loader A
Module: 6E57 315-2AG10-0AB0 v.0.5
Basic Firmware: v.6.11
Module name: CPU 315-2 DP
Serial number of module:
Plant identification:
Basic Hardware: 6E57 315-2AG10-0AB0 v.0.5

3389 Remote Desktop Protocol
tcp \x83\x00\x00\x00\x00\x00\x00\x00\x124\x00
rdp

7547 7547
tcp http

HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="c0174e290311d5282df4bcba1d272262",qop="auth",alg="MD5"

[Navigation icons: back, forward, search, etc.]

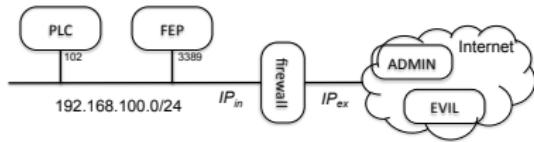
Postscript - October 2016

The screenshot displays a dual-pane interface. The left pane is a network analysis tool with the following data:

City	Ireland
Country	Ireland
Organization	Giscan
ISP	Giscan
Last Update	2016-10-25T16:46:41.375Z07
Hostnames	
ASN	AS5466

The right pane shows a Windows 7 Professional logon screen. The desktop background is a blue gradient with a yellow sunflower icon. The logon window is open, showing the user "Barry" logged on, a password field, and a "Cancel" button. The Windows logo and "Windows 7 Professional" are visible at the bottom.

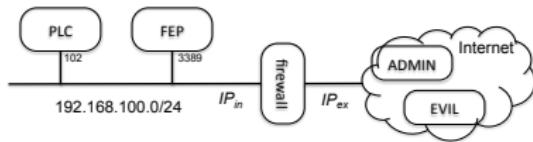
Composition of policy objectives



CPNI; RPol; UPol

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	192.168.100.0/24	≥ 1024	PLC	102	ALLOW
2	...	external IPs	*	PLC	102	DROP
3	...	external IPs	≥ 1024	FEP	3389	ALLOW
4	...	ADMIN	≥ 1024	FEP	3389	ALLOW
5	...	*.*.*.*	*	FEP	3389	DROP
6	...	*.*.*.*	≥ 1024	PLC	102	ALLOW
7	...	*.*.*.*	≥ 1024	FEP	3389	ALLOW

Composition of policy objectives



CPNI; RPol; UPol

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	192.168.100.0/24	≥ 1024	PLC	102	ALLOW
2	...	external IPs	*	PLC	102	DROP
3	...	external IPs	≥ 1024	FEP	3389	ALLOW
4	...	ADMIN	≥ 1024	FEP	3389	ALLOW
5	...	*.*.*.*	*	FEP	3389	DROP
6	...	*.*.*.*	≥ 1024	PLC	102	ALLOW
7	...	*.*.*.*	≥ 1024	FEP	3389	ALLOW

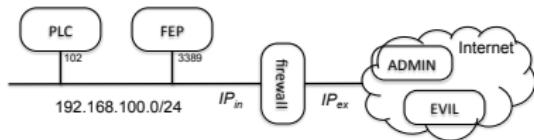
[Aside: **redundant** rules can promote policy update inconsistencies: revising one rule may not give the desired effect if there are other redundant rules, or changes become time-consuming as all applicable rules must be searched for and updated.]

Postscript - December 2016



City	
Country	Ireland
Organization	Giscan
ISP	Giscan
Last Update	2016-10-25T16:46:41.375Z07
Hostnames	
ASN	AS5466

Composition of policy objectives



RPol;CPNI;UPol

Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	ADMIN	≥ 1024	FEP	3389	ALLOW
2	...	*.*.*.*	*	FEP	3389	DROP
3	...	192.168.100.0/24	≥ 1024	PLC	102	ALLOW
4	...	external IPs	*	PLC	102	DROP
5	...	external IPs	≥ 1024	FEP	3389	ALLOW
6	...	*.*.*.*	≥ 1024	PLC	102	ALLOW
7	...	*.*.*.*	≥ 1024	FEP	3389	ALLOW

Wasn't (*RPol;CPNI;UPol*) obvious?

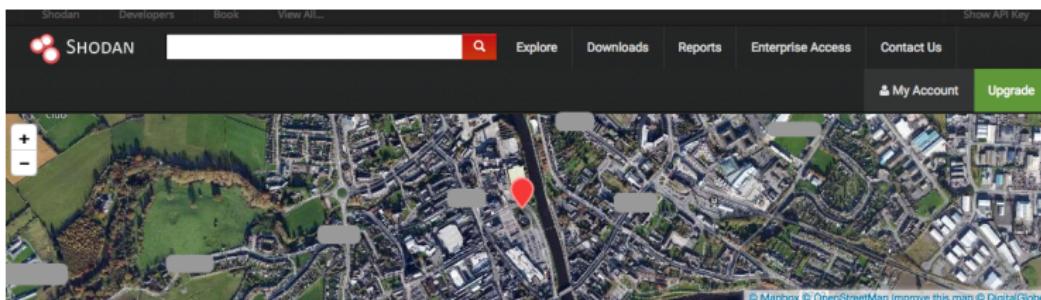
```
iptables -P FORWARD DROP
iptables -I 1 FORWARD -o eth0 -p icmp --icmp-type echo-request -j DROP
iptables -I 4 FORWARD -o eth0 -s 10.0.0.0/8 -j DROP
iptables -I 11 FORWARD -d PLC --dport 102 -j ACCEPT
iptables -I 1 OUTPUT -p icmp --icmp-type echo-request -j DROP
iptables -I 5 FORWARD -o eth0 -s 172.16.0.0/12 -j DROP
iptables -I 6 FORWARD -i eth0 -s 192.168.0.0/16 -j DROP
iptables -I 7 FORWARD -o eth0 -s 224.0.0.0/4 -j DROP
iptables -I 8 FORWARD -o eth0 -s 240.0.0.0/5 -j DROP
iptables -I 9 FORWARD -o eth0 -s 127.0.0.0/8 -j DROP
iptables -I 10 FORWARD -o eth0 -s 0.0.0.0/8 -j DROP
iptables -I 11 FORWARD -d FEP --dport 3398 -j ACCEPT
iptables -I 12 FORWARD -o eth0 -d 255.255.255.255 -j DROP
iptables -I 13 FORWARD -o eth0 -s 169.254.0.0/16 -j DROP
iptables -I 14 FORWARD -o eth0 -d 224.0.0.0/4 -j DROP
iptables -I 15 FORWARD -p tcp --tcp-flags ACK,URG URG -j DROP
iptables -I 16 FORWARD -p tcp --tcp-flags FIN,RST FIN,RST -j DROP
iptables -I 17 FORWARD -p tcp --tcp-flags SYN,FIN SYN,FIN -j DROP
iptables -I 19 FORWARD -p tcp --tcp-flags SYN,RST SYN,RST -j DROP
iptables -I 11 FORWARD -d PLC --dport 102 -j DROP
iptables -I 20 FORWARD -p tcp --tcp-flags ALL ALL -j DROP
iptables -I 21 FORWARD -p tcp --tcp-flags ALL NONE -j DROP
iptables -I 22 FORWARD -p tcp --tcp-flags ALL FIN,PSH,URG -j DROP
iptables -I 23 FORWARD -p tcp --tcp-flags ALL SYN,FIN,PSH,URG -j DROP
....  
...
```

Postscript - 03 March 2017

The screenshot shows the SHODAN search interface. At the top, there's a navigation bar with links for "Shodan", "Developers", "Book", "View All...", "Explore", "Downloads", "Reports", "Enterprise Access", "Contact Us", "My Account", and "Upgrade". Below the navigation is a map of a city area with a red location pin. A banner at the bottom of the map reads "© Mapbox © OpenStreetMap Improve this map © DigitalGlobe". On the left side, there's a summary card with a "86.4" rating, a progress bar, and sections for "City" (Ireland), "Country" (Ireland), "Organization" (Eircom), "ISP" (Eircom), "Last Update" (2017-03-01T11:43:16.867182), "Hostnames" (progress bar), and "ASN" (A5546). On the right side, there are two main sections: "Ports" showing "2000" and "7547" ports, and "Services" showing "7547" TCP services for "http-simple-new". Below the services section is a green button labeled "HTTP/1.1 401 Unauthorized" with a connection dump:

```
HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="1bb431991
a2c8436b30ae55cfeb5fd13", qop="auth", algorithm="MD5"
Content-Length: 0
```

Postscript - 03 March 2017



Ports

2000 7547

Services

7547
tcp
http-simple-new

HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest
a2c8436b30ae55feb5fd13'
Content-Length: 0

Remotely
Anywhere

Windows Authentication

Please enter your Windows username and password.

User name

Password

Login

Options

Go directly to Remote Control
Go directly to File Transfer & Synchronization
Go to Main Menu

Full interface (for DHTML capable browsers)
Light interface (for old browsers or slow connections)

Select language: English

<< Hide advanced options

Postscript - 03 March 2017

SHODAN Developers Book View All... Show API Key

My Account Upgrade



Mapbox © OpenStreetMap improve this map © DigitalGlobe

86.4

Ports

2000 7547

Services

7547 tcp http-simple-new

HTTP/1.1 401 Unauthorized

Connection: Keep-Alive

WWW-Authenticate: Digest

a2c8436b30ae55cfab5fd13'

Content-Length: 0

Remotely Anywhere

Website Identity

Website: 84-41.net.2000

Owner: This website does not supply ownership information.

Verified by: CN=Default CA,O=IE

View Certificate

Privacy & History

Have I visited this website prior to today? No

Is this website storing information (cookies) on my computer? No

View Cookies

Have I saved any passwords for this website? No

View Saved Passwords

Technical Details SHA1

Connection Encrypted (TLS_1_2, WITH_AES_256_GCM_SHA1)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone could read this page as it traveled across the network.

Postscript - 13 March 2017

Shodan Developers Book View All... Show API Key

SHODAN Explore Downloads Reports Enterprise Access Contact Us My Account Upgrade

Mapbox © OpenStreetMap Improve this map © DigitalGlobe

86.4

Ports

2000	3389	7547
------	------	------

Services

3389	tcp	rdp
------	-----	-----

Remote Desktop Protocol
\\x03\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x00\\x124\\x00

SSL Certificate

Certificate:

Data:
Version: 3 (0x2)
Serial Number:
5f:5e:5c:06:b7:a3:17:83:4a:06:f9:44:ce:e8:28:85

Postscript - 17 March 2017



86.

wtd.eircom.net

City [REDACTED]

Country Ireland

Organization Eircom

ISP Eircom

Last Update 2017-03-01T11:43:16.867182

Hostnames [REDACTED]

ASN AS5466

Ports

2000

7547

Services

7547

tcp

http-simple-new



HTTP/1.1 401 Unauthorized

Connection: Keep-Alive

WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="1bb431991a2c8436b

30ae55cfb5fd13",qop="auth",algorithm="MD5"

Content-Length: 0

Postscript - 20 March 2017

The screenshot shows a Shodan search result for the IP address 86.44.11.11. At the top, there's a navigation bar with links for "Shodan", "Developers", "Book", "View All...", "Explore", "Enterprise Access", "Contact Us", "New to Shodan?", and "Login or Register". Below the bar is a map of Ireland with a red dot indicating the location of the target IP. A copyright notice at the bottom right of the map area reads "© Mapbox © OpenStreetMap Improve this map © DigitalGlobe".

Ports

Port	Protocol
2000	tcp
3389	tcp
7547	tcp

Services

Port	Protocol	Service
3389	tcp	Remote Desktop Protocol
	rdp	

Details for the IP 86.44.11.11:

- City: [REDACTED]
- Country: Ireland
- Organization: Eircom
- ISP: Eircom
- Last Update: 2017-03-18T22:41:01.847452
- Hostnames: 86.44.11.11 [REDACTED]
- ASN: AS5466

A large screenshot of a Windows desktop environment is shown below the service details. The desktop background is blue, and a yellow sunflower icon is visible. The taskbar at the bottom shows icons for File Explorer, Task View, and other system utilities. The user profile "Barry" is visible.

Outline of Talk

Networking recap

Motivation

The cautionary tale

Threat Management

Conclusion

Extra

Conflicting control recommendations

- Setting up a VPN here implicitly means closing Port 102 at router

Conflicting control recommendations

- Setting up a VPN here implicitly means closing Port 102 at router
- However, for S7 service availability, suggestion is that Port 102 is open

The screenshot shows a ticket page from the Siemens Industry Online Support platform. The ticket number is 2010-044, and it has 10 likes and 10 comments. The subject of the ticket is "Which ports are used by the various services for state transfer via TCP and UDP and what should you watch out for when using routes and firewalls?".

The ticket content discusses the use of ports 102, 2000, and 4000 for various services. It notes that port 102 is used for S7 communication, while 2000 and 4000 are used for other services. It also mentions that port 102 is used for state transfer via TCP and UDP.

Related Links:

- SIMATIC Industrial Ethernet
- Configuring firewalls
- Firewall configuration
- Port forwarding
- My Projects
- Community
- FAQ
- Siemens Wiki
- Service info
- Events
- Contact Siemens

Product Information:

- SIMATIC Industrial Ethernet
- Configuring firewalls
- Firewall configuration
- Port forwarding
- My Projects
- Community
- FAQ
- Siemens Wiki
- Service info
- Events
- Contact Siemens

Topic pages for this entry:

- Firewalls - All discussions
- Industrial firewalls
- Set up your projects

Conflicting control recommendations

- Setting up a VPN here implicitly means closing Port 102 at router
- However, for S7 service availability, suggestion is that Port 102 is open

The screenshot shows a forum post from the Siemens Industry Online Support platform. The post is titled "Which ports are used by the various services for data transfer via TCP and UDP and what should you watch out for when using routes and firewalls?" It includes a poll asking if users enable port 102. Below the poll, there's a detailed technical explanation of port 102's use for S7 services like MPI, DP, and LPI, and its importance for remote programming. A red box highlights the following text:

RFC 1006 is based on the TCP protocol and permits a reliable connection between two systems.
RFC 1006 is used for standard connections in the SIMATIC environment.
Areas of application:

- STEP 7 remote programming via LAN
- STEP 7 remote programming via ISDN
- ISO-on-TCP connections
- S7 connections via Industrial Ethernet

The TCP Port 102 must be enabled in all areas of application.
Note
Port 102 is blocked by default in routers and firewalls and must be enabled for the complete transfer route.

Conflicting control recommendations

- Setting up a VPN here implicitly means closing Port 102 at router
- However, for S7 service availability, suggestion is that Port 102 is open
- When alerted to potential confusion, Siemens updated FAQ

The screenshot shows a Siemens Industry Online Support page. At the top, there's a video thumbnail of two men in a factory setting. Below the video, the page title is "Which ports are used by the various services for data transfer via TCP and UDP and what should you watch out for when using routes and firewalls?". The main content area contains several sections of text and tables. A red box highlights the "Note" section at the bottom right, which states:

Note

- Port 102 is blocked by default in routers and firewalls.
- Further information about the RFC1006 service is available in Entry [15048962](#).

Conflicting control recommendations

- Setting up a VPN here implicitly means closing Port 102 at router
- However, for S7 service availability, suggestion is that Port 102 is open
- When alerted to potential confusion, Siemens updated FAQ
- But, we also look for advice elsewhere.

The screenshot shows a forum thread titled "Which ports are used by the various services for data transfer via TCP and UDP and how can I open them?" The thread has two main posts:

Post #1 (User: Wizard, Jan 10 2008):

Hi there,
I would like to ask you the following question:
return ports are used by the various services for data transfer by means of TCP or UDP and what should you watch out for when using routers and firewalls?
Best regards,
Wizard

Post #2 (User: Diamond Member, Jan 10 2008):

Hi Wizard,
return ports are used by the various services for data transfer by means of TCP or UDP and what should you watch out for when using routers and firewalls?
Best regards,
Diamond Member

Post #3 (User: Wizard, Jan 10 2008):

Hi Diamond Member,
just to continue, to be more precise, in the my answer? Or is there any other problem that should take care of, regarding access to PLC?

Post #4 (User: Diamond Member, Jan 10 2008):

Hi Wizard, just to add
any port can be used on the host processor and provide a reliable connection.
Hence, port 102 is used for standard connection in the Ethernet based of applications:
102: EtherNet/Industrial Ethernet programming via SPP
102: EtherNet/Industrial Ethernet via TCP
102: EtherNet/Industrial Ethernet via UDP
102: Ethernet connection via Industrial Ethernet
Port 102 is blocked by default in routers and firewalls and must be enabled for the complete transparent access.

Conflicting control recommendations

- Setting up a VPN here implicitly means closing Port 102 at router
- However, for S7 service availability, suggestion is that Port 102 is open
- When alerted to potential confusion, Siemens updated FAQ
- But, we also look for advice elsewhere.

Following a control recommendation does not necessarily mean threat is mitigated.

Must also check the efficacy of the control at mitigating the threat.

The screenshot shows a forum thread titled "Which ports are used by the various services for data transfer via TCP and UDP and what should you watch out for when using routers and firewalls?" with three main posts:

- Post 1 (Siemens):** A screenshot of a Siemens FAQ page titled "FAQ: Which ports are used by the various services for data transfer via TCP and UDP and what should you watch out for when using routers and firewalls?". It lists several services and their ports, including "S7-Industrial Ethernet" using port 102.
- Post 2 (User):** A user asks if port 102 is used for the S7 service. The response suggests it's used for "various services" and advises watching for "confusion".
- Post 3 (Siemens):** A follow-up from Siemens clarifies that port 102 is used for "various services" and provides a detailed list of services and their ports, including "S7-Industrial Ethernet" using port 102.

Security threat management for the ICS use case

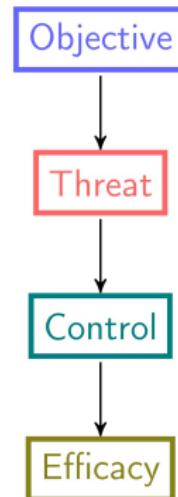
Objective: provide remote supervisory control to ICS

Threat: attacker accesses PLC

- CPNI: tunnel S7 traffic over VPN.
- Only admin IP may access via VPN.
- Software update mechanism.

Efficacy: are threats mitigated?

- Check VPN/firewall is configured.
- Audit HW/SW versions, run shodan, ...
- IDS checks for suspicious S7 packets on internal network.



Security threat management for the ICS use case

Objective: provide remote supervisory control to ICS

Threat: attacker accesses PLC

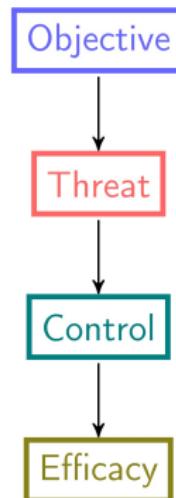
- CPNI: tunnel S7 traffic over VPN.
- Only admin IP may access via VPN.
- Software update mechanism.

Efficacy: are threats mitigated?

- Check VPN/firewall is configured.
- Audit HW/SW versions, run shodan, ...
- IDS checks for suspicious S7 packets on internal network.

Threat: PLC is unreachable

- FAQ: “[...] open Port 102 on router”



Outline of Talk

Networking recap

Motivation

The cautionary tale

Threat Management

Conclusion

Extra

Conclusion

- Security control selection does not necessarily mean system is secure: controls can conflict, be ineffective or missing.
- Assess the efficacy of threat mitigation: intrusion detection, ongoing audit, shodan investigation, ...
- Policy anomalies: what is meant by policy composition?
- Vulnerabilities are not limited to code.
- Studies help us to understand *why*.

Resources and further reading

- <https://shodan.io>
- “*Journalists warned system owners and Norwegian NSA of 2500 critical data flaws*”, Dagbladet, 06.01.2014.
- Dagbladet, NULL CTRL, <https://www.dagbladet.no/nullctrl>
- Front-end for CVE data <https://www.cvedetails.com>
- SN Foley, *Getting security objectives wrong: a cautionary tale of an Industrial Control System*, In proceedings of International Workshop on Security Protocols, Springer LNCS 10476, 2017.
- Robert Graham, FAQ: Firewall Forensics (What am I seeing?), Linux Security, 2000.

Outline of Talk

Networking recap

Motivation

The cautionary tale

Threat Management

Conclusion

Extra

Responsible disclosure

Give stakeholders opportunity to address issues

- Contacted owners of email sites about SMTP vulnerabilities.
- Contacted ICS owner about the Scada/other vulnerabilities.
- Contacted Siemens about the 'confusion' in FAQ 8970169.

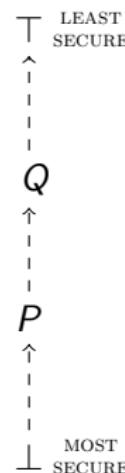
Shodan investigation only; did not visit/probe the sites

Security as comparison

Formalizing what we mean by composition of policy objectives

Secure Replacement $P \sqsubseteq Q$

- P is no less secure than Q .
- Currently upheld objective Q can be securely replaced by objective P .

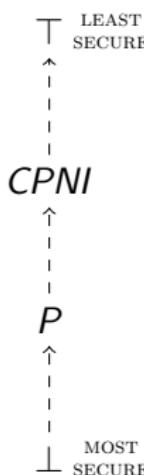


Security as comparison

Formalizing what we mean by composition of policy objectives

Secure Replacement $P \sqsubseteq Q$

- P is no less secure than Q .
- Currently upheld objective Q can be securely replaced by objective P .
- Compliance: $P \sqsubseteq CPNI$

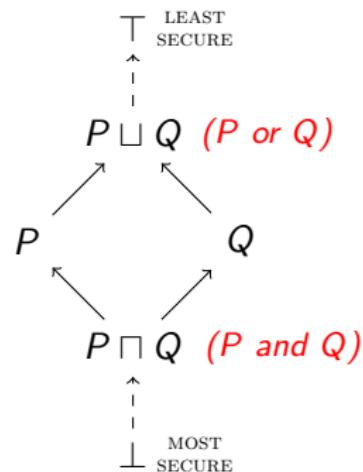


Security as comparison

Formalizing what we mean by composition of policy objectives

Secure Replacement $P \sqsubseteq Q$

- P is no less secure than Q .
- Currently upheld objective Q can be securely replaced by objective P .
- Compliance: $P \sqsubseteq CPNI$



Secure Composition $P \sqcap Q$, $P \sqcup Q$

- A lattice of policy objectives.
- Objective $P \sqcap Q$ as 'best' objective that is no less secure than P and Q .
- Replace P by $P \sqcap (CPNI \sqcup RFC5735)$

A (simplified) lattice of firewall policies

Secure Replacement $P \sqsubseteq Q$

Policy Q can be replaced by policy P , if P is no less restrictive than Q .

For all $P, Q : Policy$:

$$P \sqsubseteq Q \equiv (\text{accepts}(P) \subseteq \text{accepts}(Q)) \wedge (\text{denies}(P) \supseteq \text{denies}(Q))$$

$$P \sqcup Q \Leftrightarrow (\text{accepts}(P) \cup \text{accepts}(Q)) \wedge (\text{denies}(P) \cap \text{denies}(Q))$$

$$P \sqcap Q \Leftrightarrow (\text{accepts}(P) \cap \text{accepts}(Q)) \wedge (\text{denies}(P) \cup \text{denies}(Q))$$

Lattice of policies ($Policy, \sqsubseteq, \sqcup, \sqcap$)

A lattice under \sqsubseteq ; lowest upper bound \sqcup and greatest lower bound \sqcap .

Policy compositions

$$\begin{aligned} Pol &= UPol \sqcap (CPNI \sqcup RPol) \\ &= (RPol \circ CPNI \circ UPol); \end{aligned}$$

$$Pol' = Pol \sqcap RFC5735$$

Some sample Snort IDS rules

We could configure an IDS to look for any traffic that might suggest attempted use of the built-in Basisk Siemens account, for instance a Snort style rule that looks for any packet containing string "Basisk":

```
alert TCP any any -> any 102 \
  (msg:"access attempt using Basisk backdoor account"; \
  content:"Basisk"; )
```

However, this is a coarse-grained rule: we would like to be able to discriminate an attack on a vulnerable system (that could succeed), versus a unsuccessful attempt against a non-vulnerable system (that could not succeed).

It is also possible that access to this hard-coded account on legacy systems via the local network might be considered a necessary operation for certain legacy workflows.

Some Snort IDS rules for Simatic S7 can be found [here](#) and [here](#)

Some sample Snort IDS rules

Stateful rule attribute `flowbits` is used to track rule state during a transport protocol session. It's set to `backdoor` when it appears that there is a S7 connection attempt made using the backdoor Basisk userid/password.

```
alert TCP any any -> any 102 \
  (msg:"access attempt using Basisk backdoor account"; \
  content:"Basisk"; \
  flow:to_server,established; \
  flowbits:set,backdoor; )
```

If there is subsequent activity on the attempted Basisk TCP session then it could indicate that the login was successful. The following rule triggers an alert if it appears that there is an attempt to send a request to delete a block over that same session:

```
alert tcp any any -> any 102 \
  (msg:"Delete block requested via backdoor account"; \
  content:"|03 00|";offset:0;depth:2; \
  content:"|05 5f 44 45 4c 45|";sid:20; \
  flow:to_server,established; \
  flowbits:isset,backdoor; )
```

However, the correlation here is crude.