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

TCP/IP Recap

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

$$\text{Msg 1}: \quad \textit{Source} \rightarrow \textit{Destination}: \quad \textit{message}$$

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 on `cosmos.ucc.ie` sends a request to the application running on `smtp.ucc.ie`:

```
> telnet smtp.ucc.ie 25
helo 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").

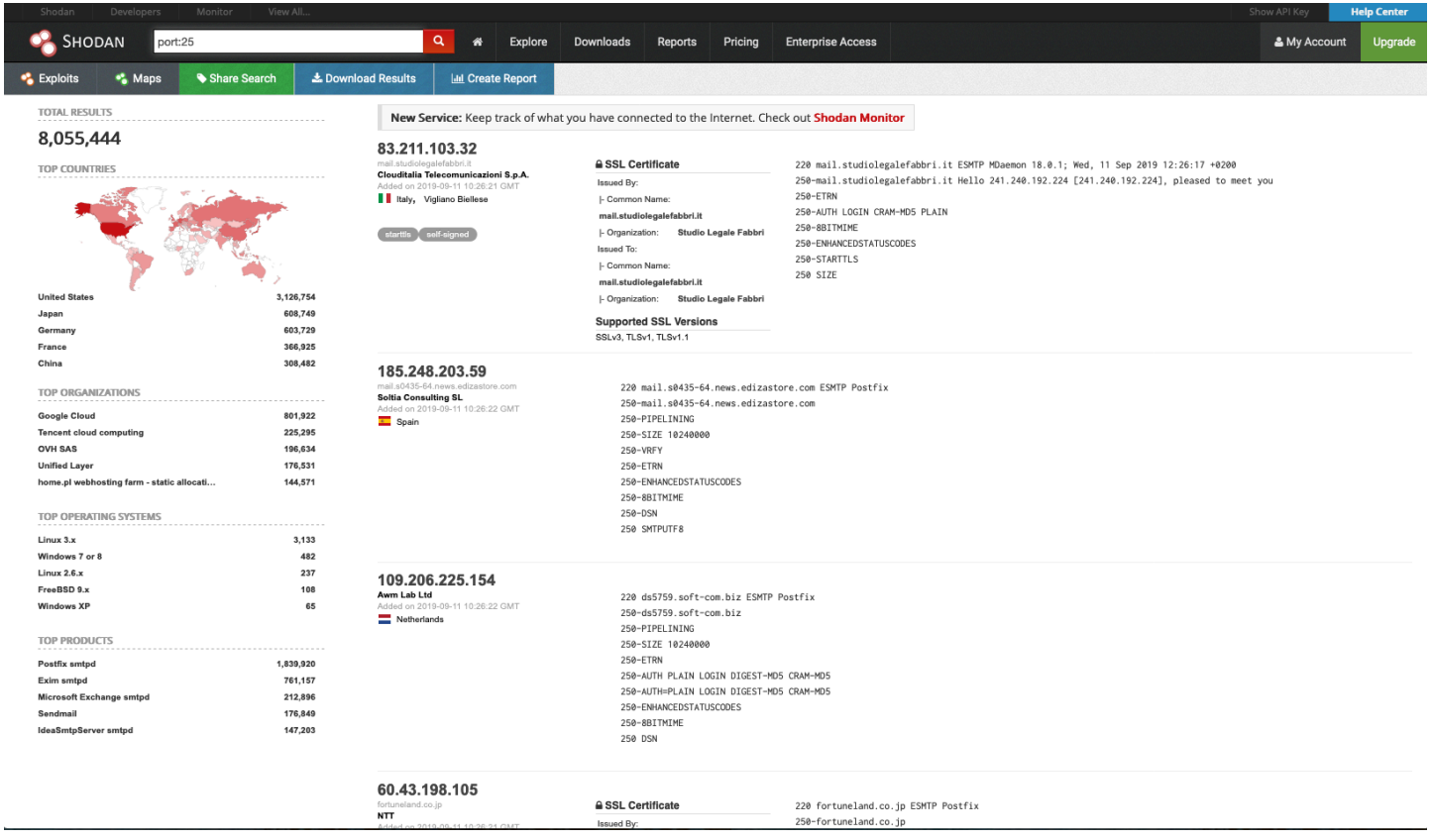
Sample Network Packet Content

`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>
```

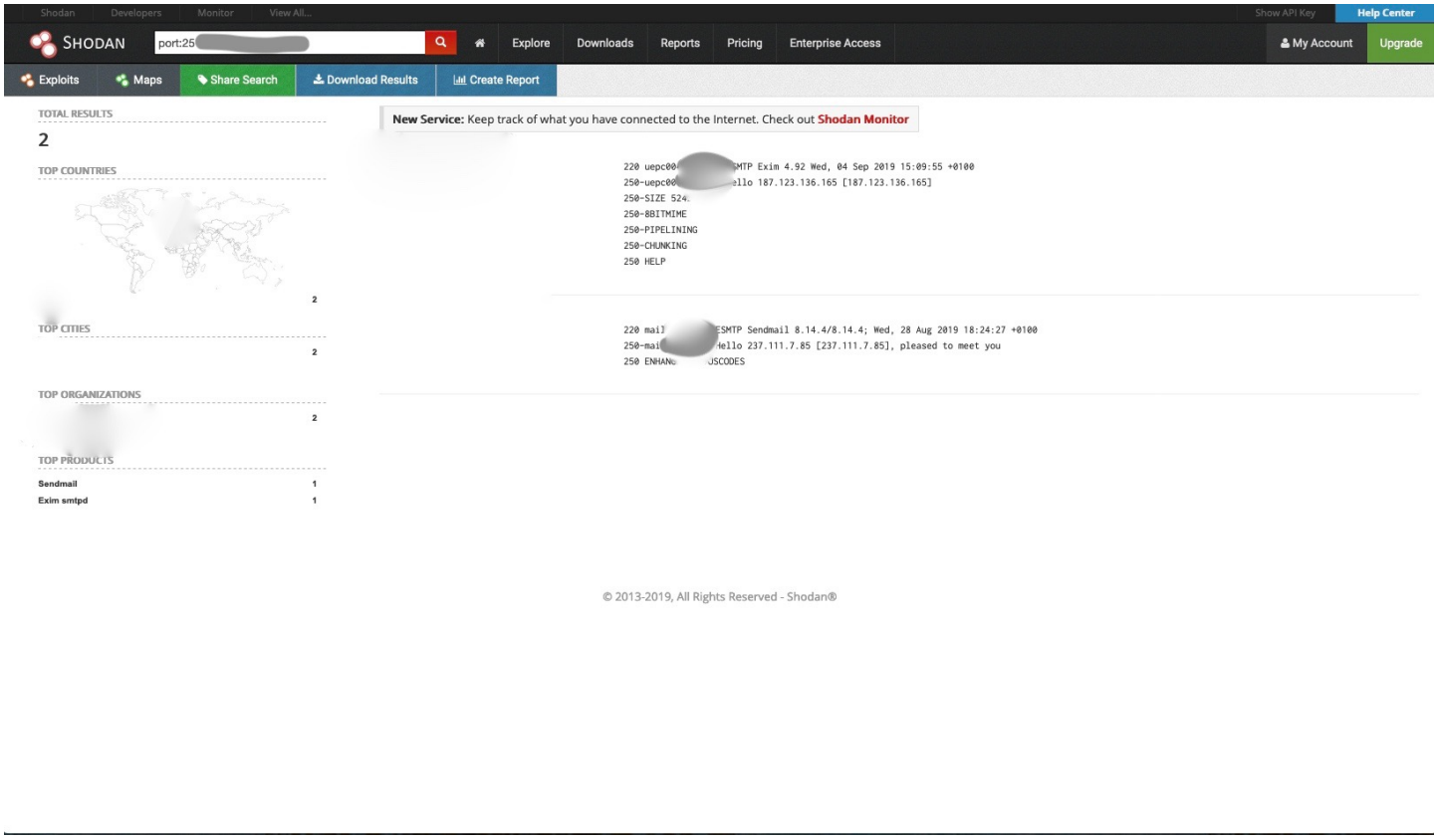
Shodan

Searching for sites based on Internet header data



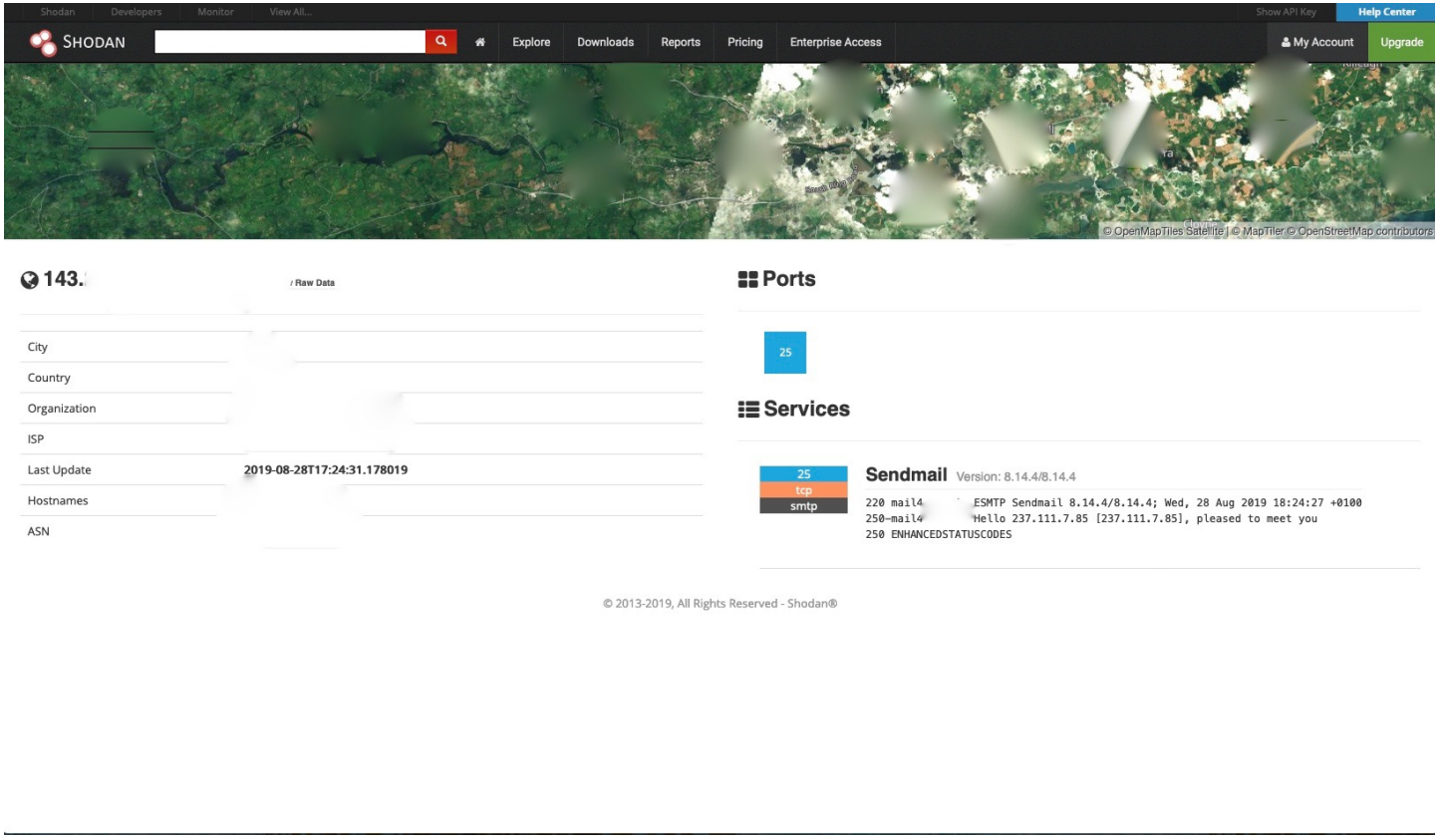
Shodan

Searching for sites based on Internet header data



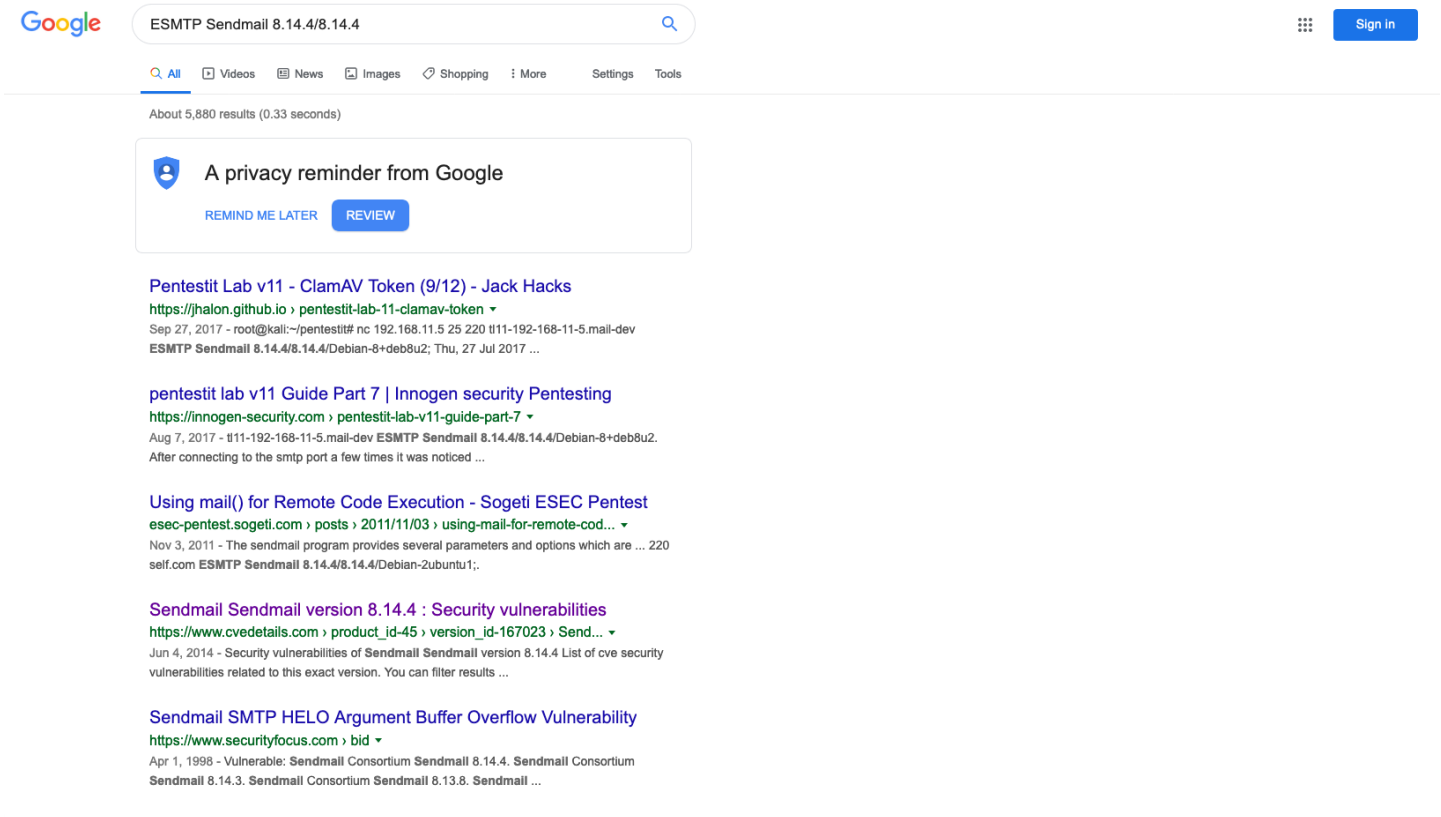
Shodan

Searching for sites based on Internet header data



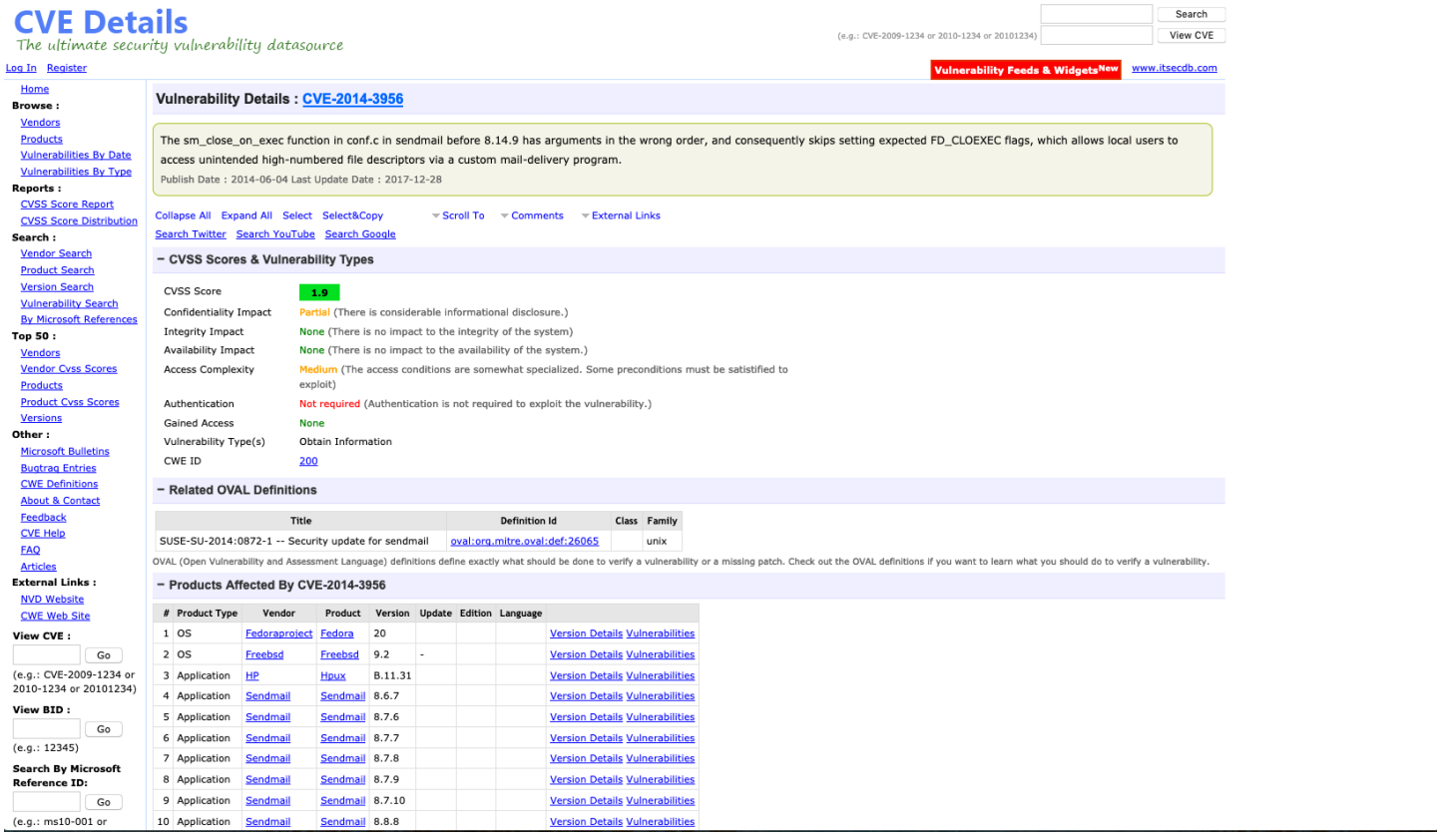
Shodan

Searching for sites based on Internet header data



Shodan

Searching for sites based on Internet header data



CVE Details
The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234) Search View CVE

Log In Register

Vulnerability Feeds & Widgets New www.itsecdb.com

Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
External Links :
NVD Website
CWE Web Site
View CVE :
Go
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)
View BID :
Go
(e.g.: 12345)
Search By Microsoft Reference ID:
Go
(e.g.: ms10-001 or

Vulnerability Details : CVE-2014-3956

The sm_close_on_exec function in conf.c 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.

Publish Date : 2014-06-04 Last Update Date : 2017-12-28

Collapse All Expand All Select Select&Copy Scroll To Comments External Links
Search Twitter Search YouTube Search Google

– CVSS Scores & Vulnerability Types

CVSS Score	1.9
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.)
Gained Access	None
Vulnerability Type(s)	Obtain Information
CWE ID	200

– Related OVAL Definitions

Title	Definition Id	Class	Family
SUSE-SU-2014:0872-1 -- Security update for sendmail	oval:org.mitre.oval:def:26065		unix

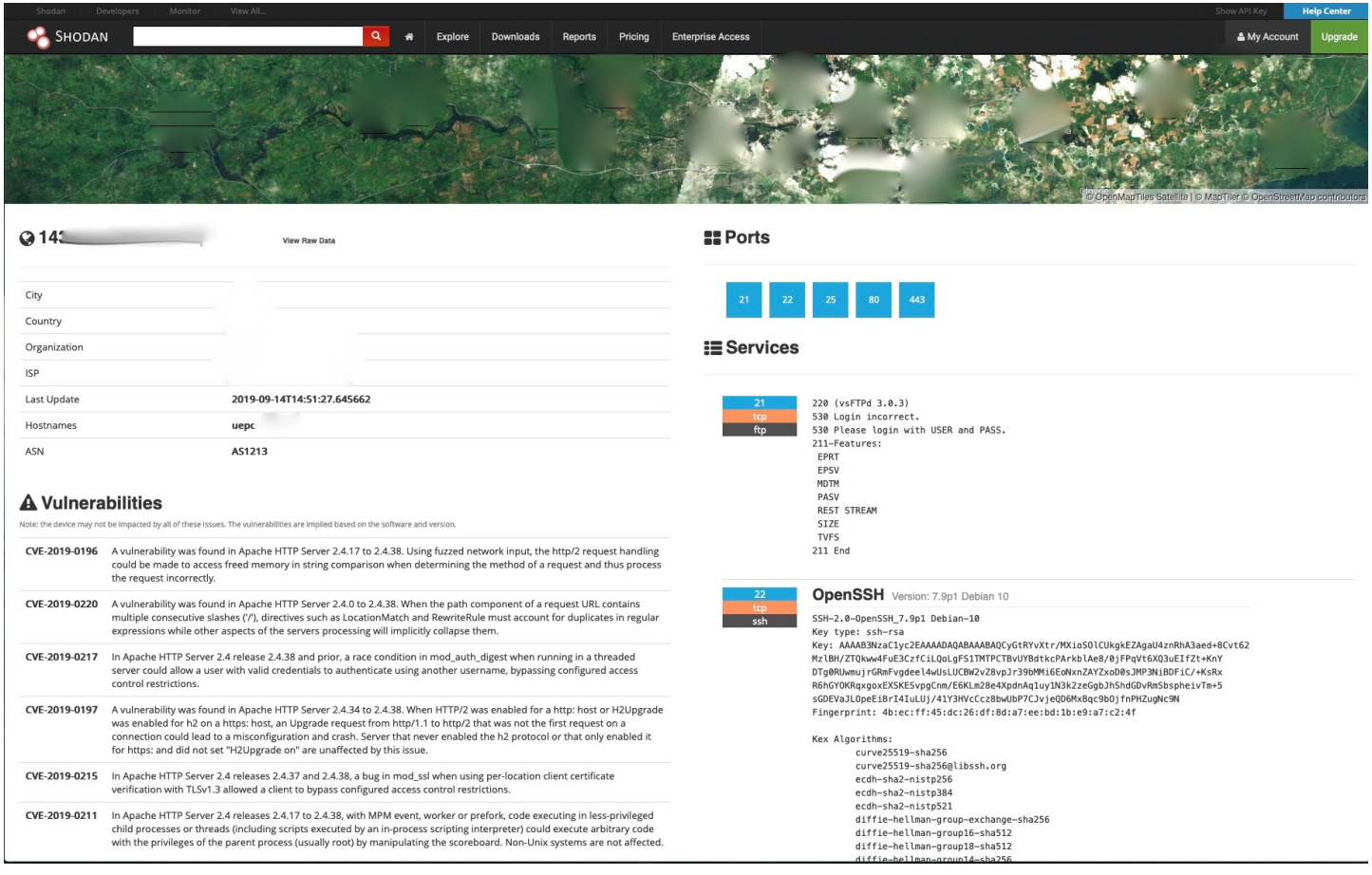
OVAL (Open Vulnerability and Assessment Language) definitions define exactly what should be done to verify a vulnerability or a missing patch. Check out the OVAL definitions if you want to learn what you should do to verify a vulnerability.

– Products Affected By CVE-2014-3956

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	OS	Fedoraproject	Fedora	20				Version Details Vulnerabilities
2	OS	Freebsd	Freebsd	9.2	-			Version Details Vulnerabilities
3	Application	HP	Hpux	B.11.31				Version Details Vulnerabilities
4	Application	Sendmail	Sendmail	8.6.7				Version Details Vulnerabilities
5	Application	Sendmail	Sendmail	8.7.6				Version Details Vulnerabilities
6	Application	Sendmail	Sendmail	8.7.7				Version Details Vulnerabilities
7	Application	Sendmail	Sendmail	8.7.8				Version Details Vulnerabilities
8	Application	Sendmail	Sendmail	8.7.9				Version Details Vulnerabilities
9	Application	Sendmail	Sendmail	8.7.10				Version Details Vulnerabilities
10	Application	Sendmail	Sendmail	8.8.8				Version Details Vulnerabilities

Shodan

Searching for sites based on Internet header data



Shodan

Searching for sites based on Internet header data

Outline of Talk

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

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

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.

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 dont always require authentication - it isnt 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

S7 (S7 Communication) is a Siemens proprietary protocol that runs between programmable logic controllers (PLCs) of the Siemens S7 family.

Explore Siemens S7

DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.

Explore DNP3

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

EtherNet/IP was introduced in 2001 and is an industrial Ethernet network solution available for manufacturing automation.

Explore EtherNet/IP

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.

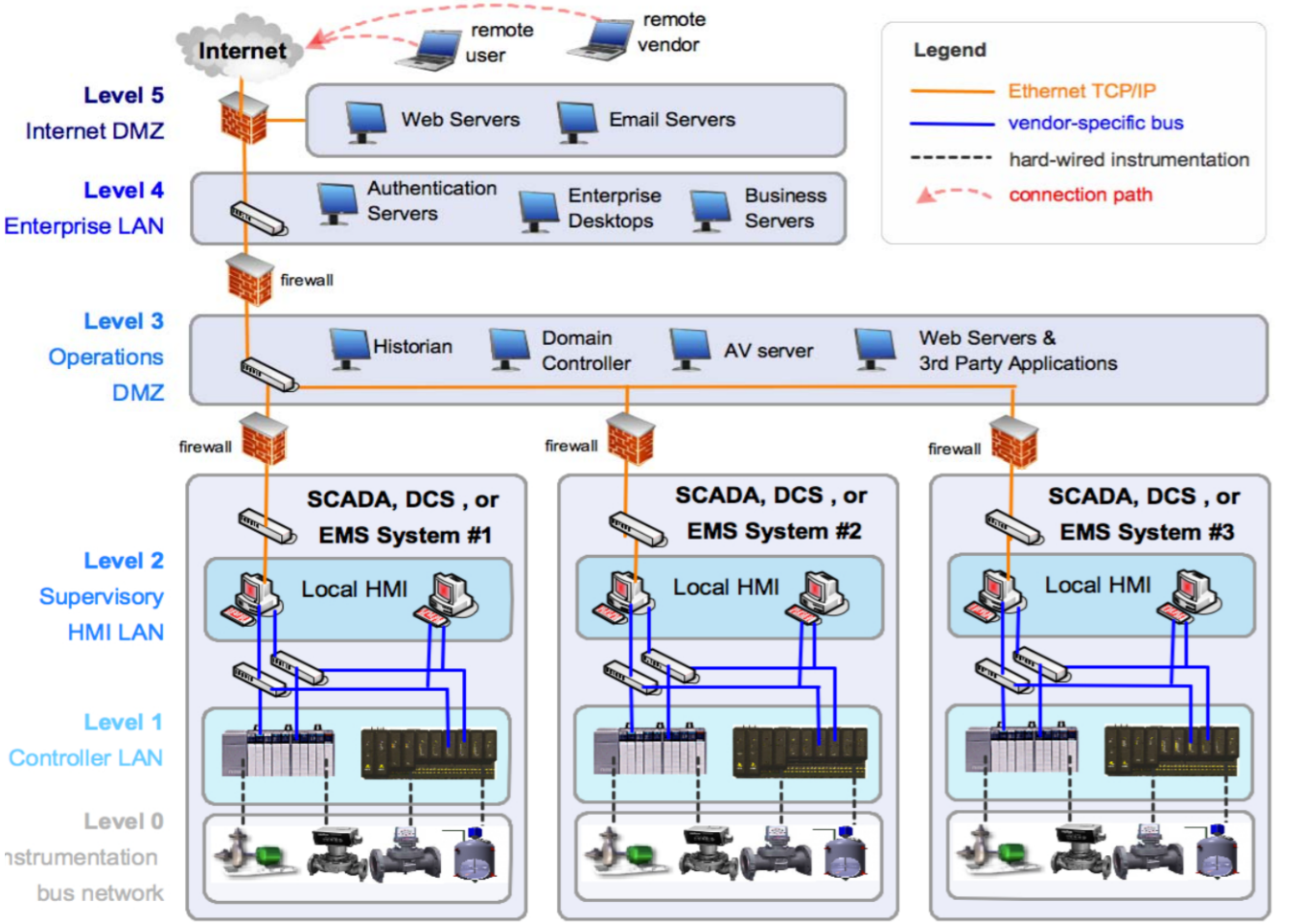
Explore OMRON FINS

The protocol the Crimson v3.0 desktop software uses when communicating with the Red Lion Controls G306a human machine interface (HMI).

Explore Crimson v3

SCADA / Industrial Control Systems

Supervisory Control and Data Acquisition

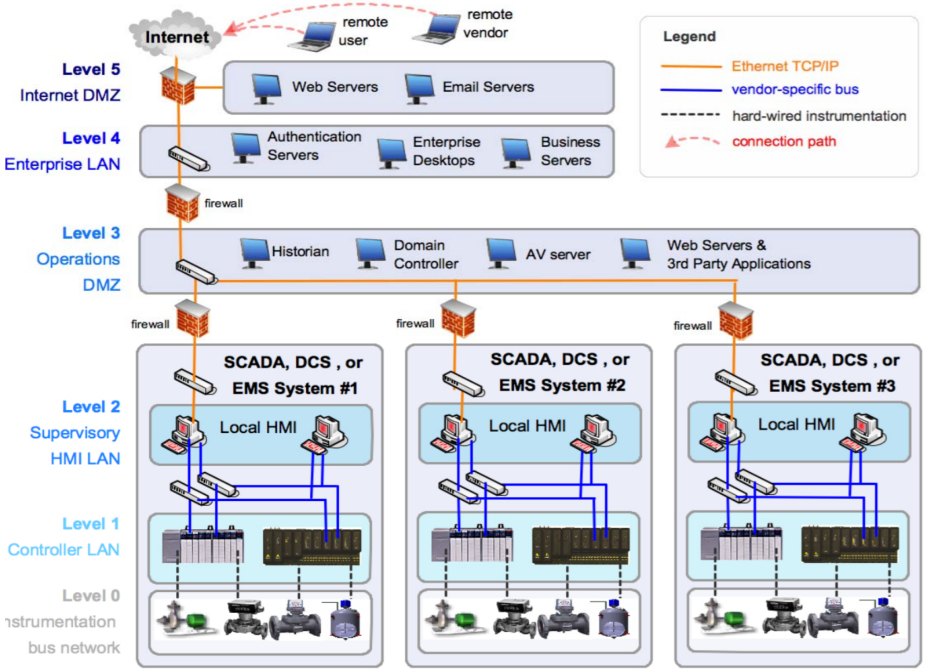


SCADA over public networks

One seemingly simple security objective

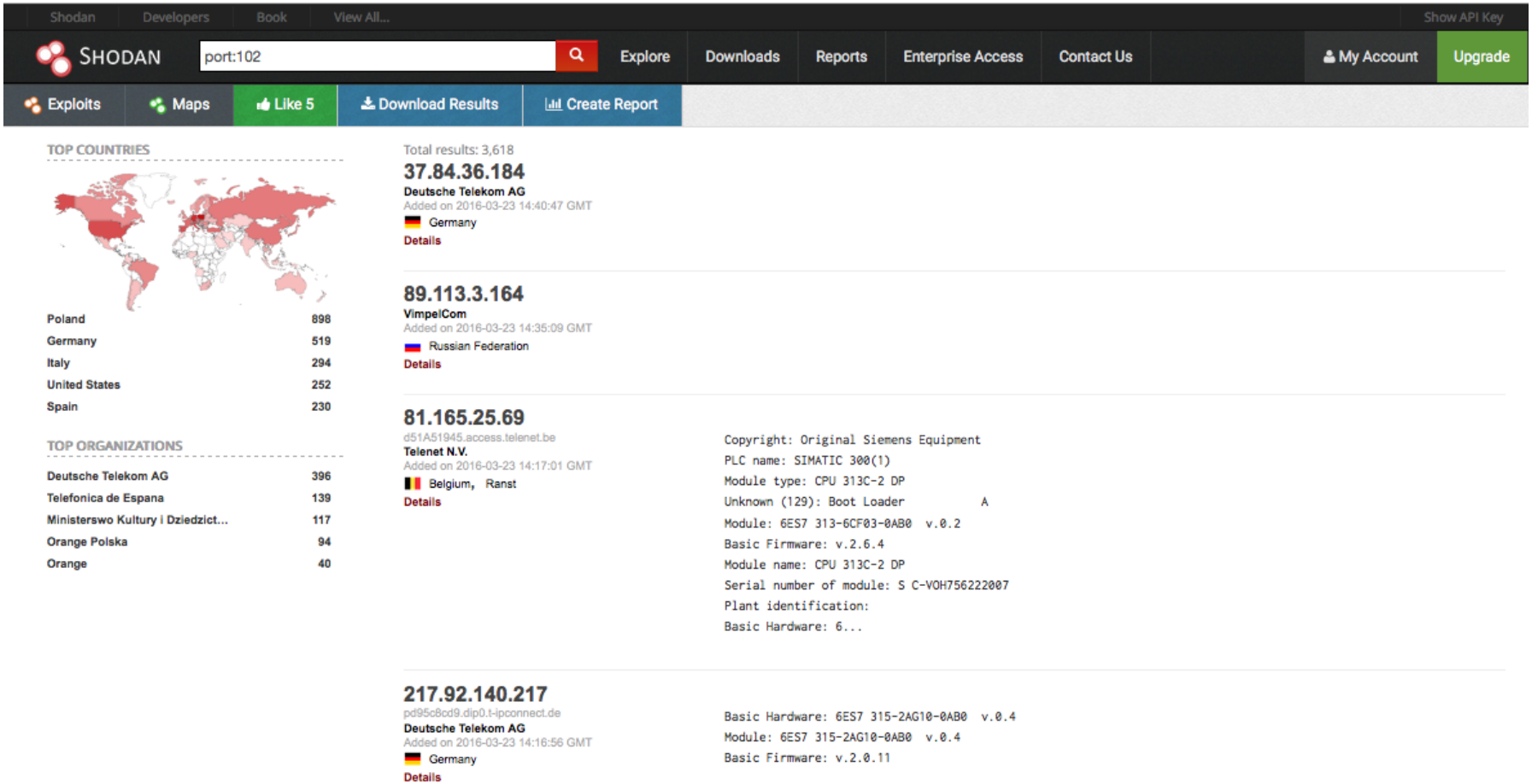
"[...] SCADA communications should be encrypted and routed through a VPN tunnel through corporate IT or other non-critical networks. [...]"

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



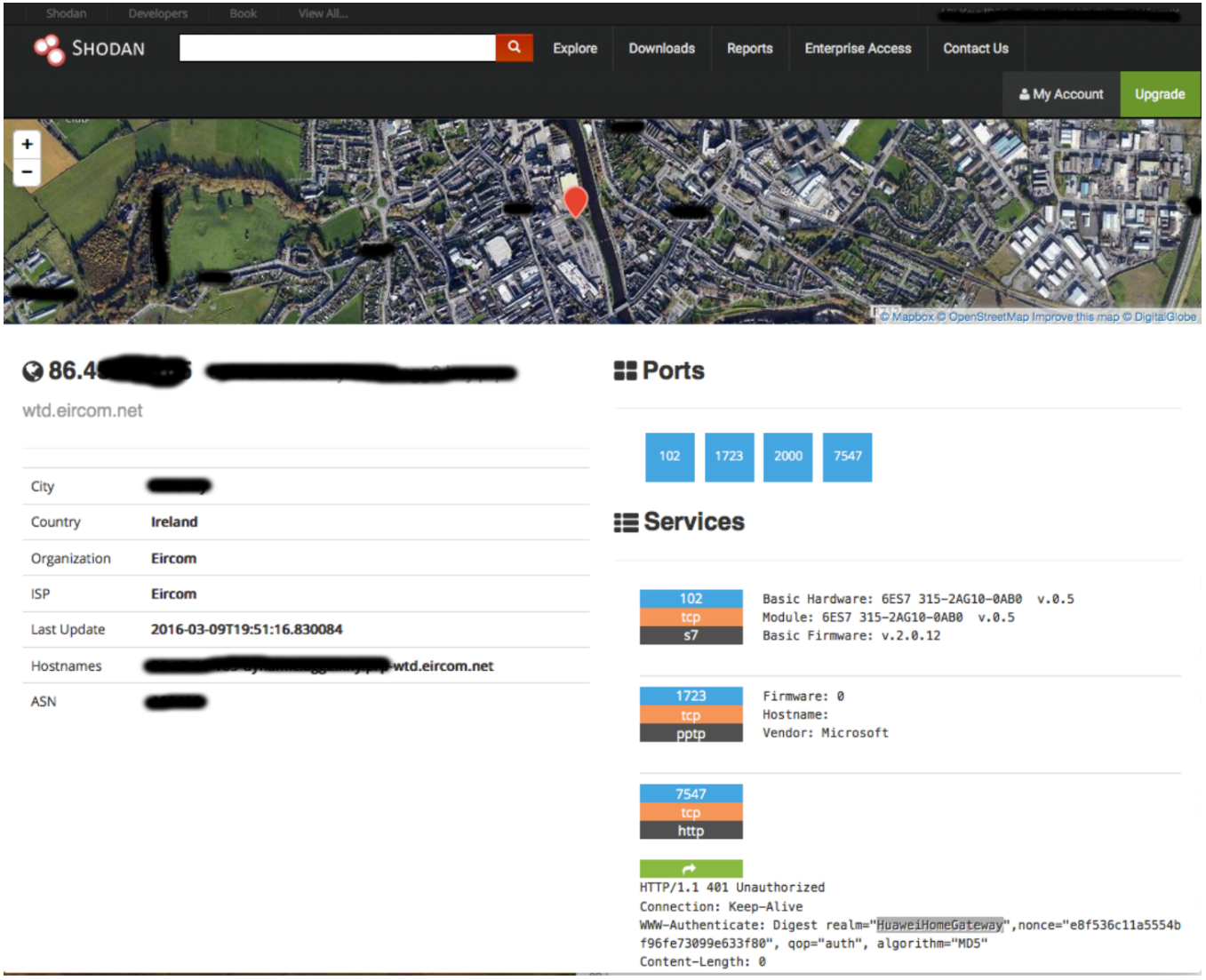
Use shodan to search for a use case

Siemens S7comm protocol over TCP/TSAP on Port 102

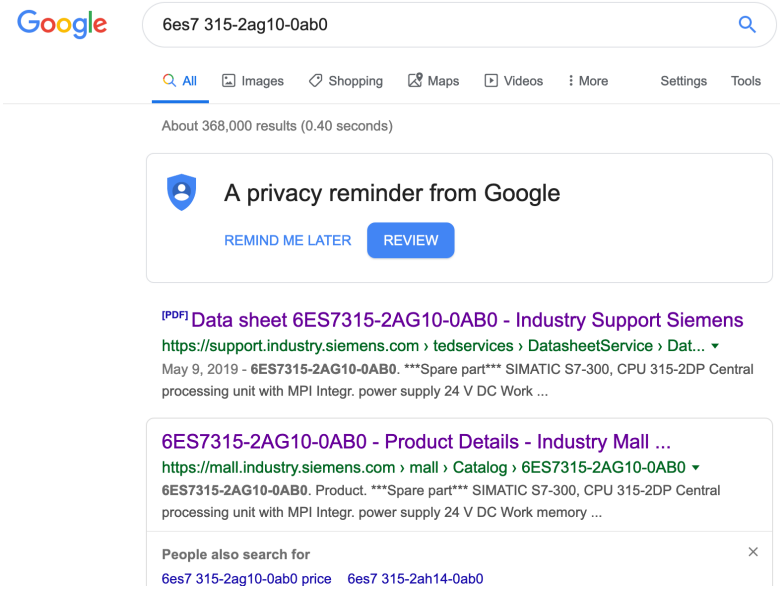


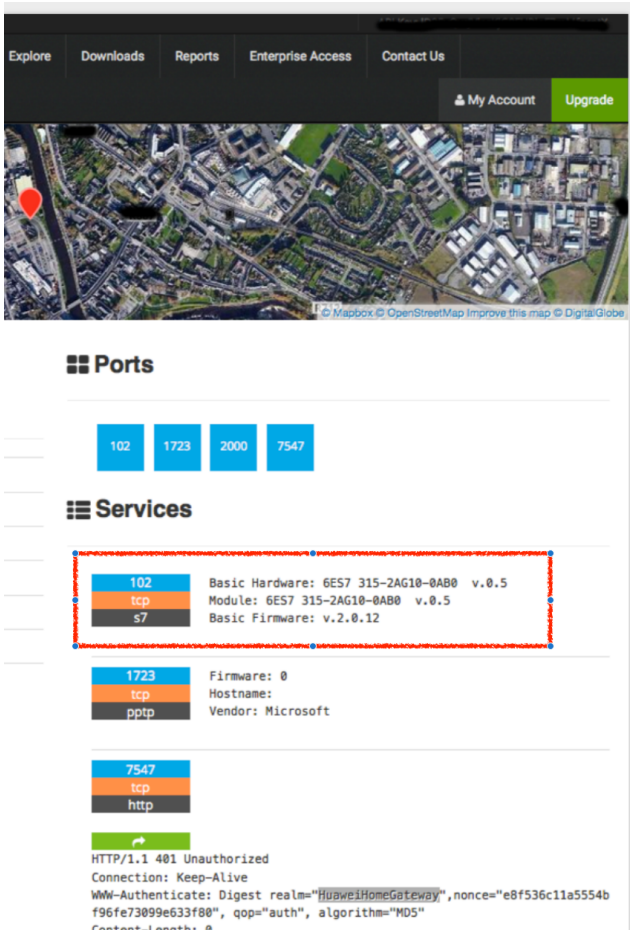
The ICS use case

Siemens S7comm protocol over TCP/TSAP on Port 102

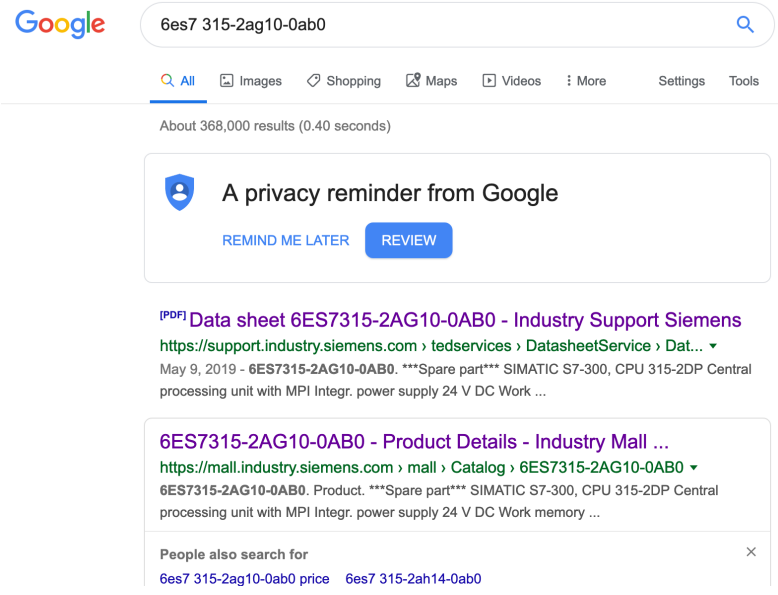


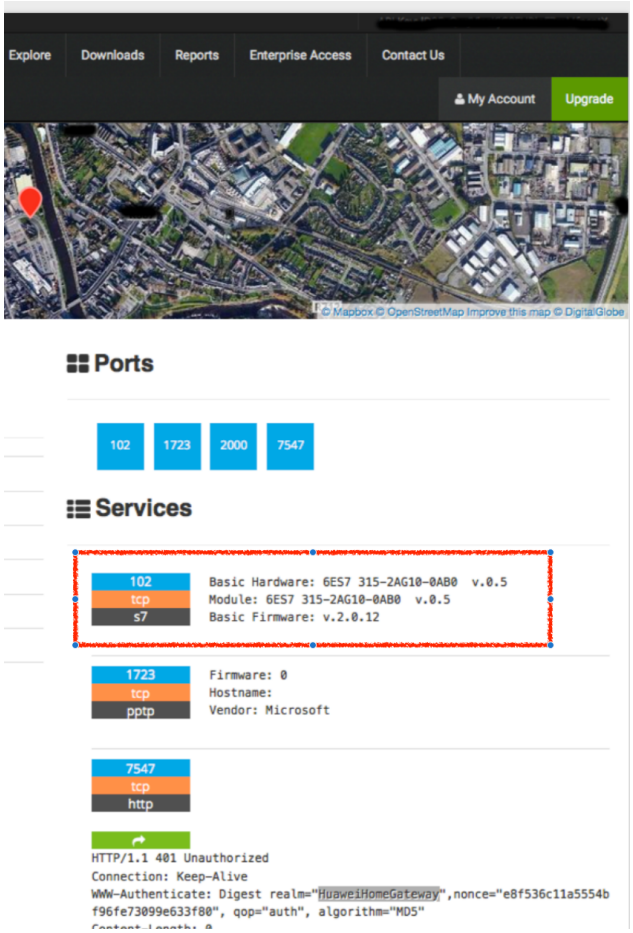
What have we found?





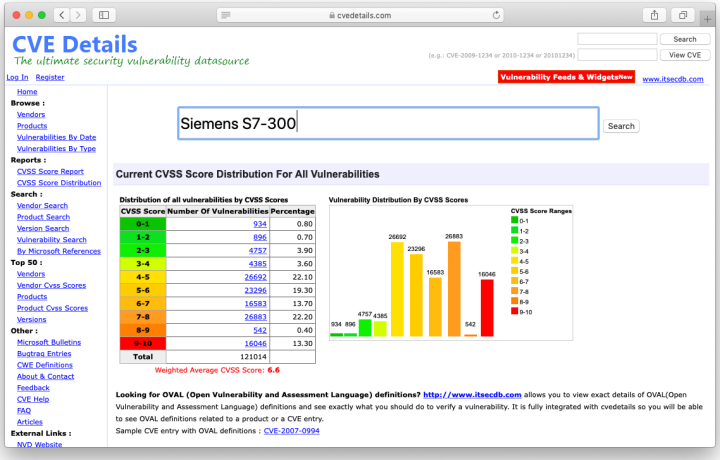
What have we found?





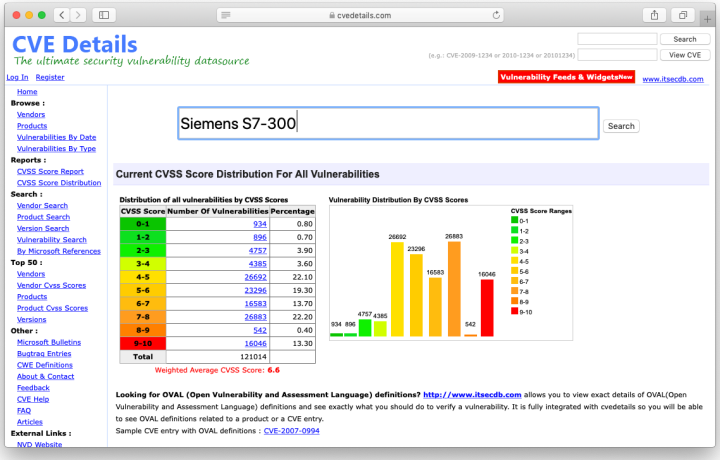
Are there any published vulnerabilities?

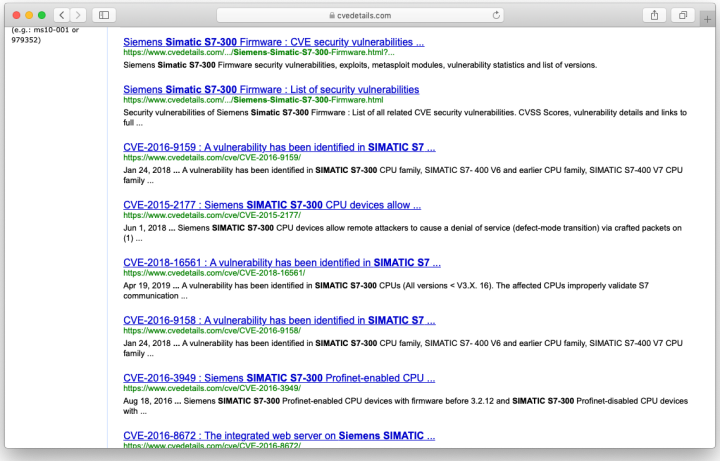
Search the CVE vulnerability database via CVE details



Are there any published vulnerabilities?

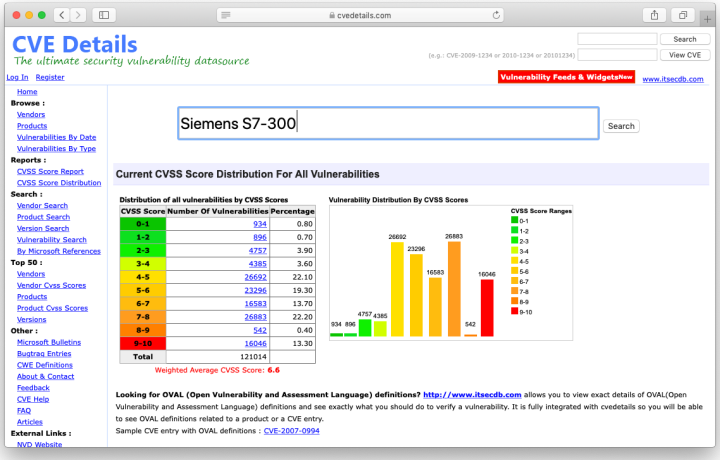
Search the CVE vulnerability database via CVE details

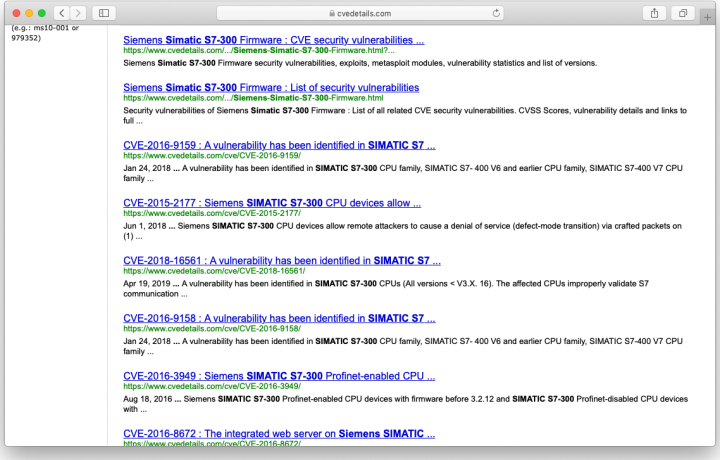




Are there any published vulnerabilities?

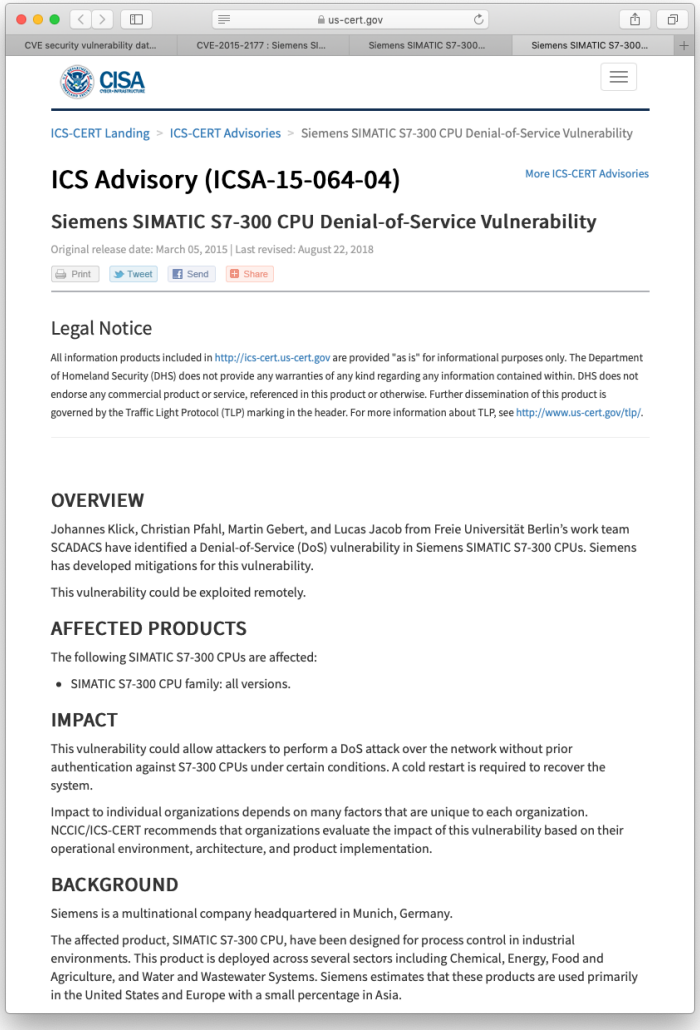
Search the CVE vulnerability database via CVE details





A denial of service vulnerability

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



us-cert.gov

CVE security vulnerability dat... | CVE-2015-2177 : Siemens SI... | Siemens SIMATIC S7-300... | Siemens SIMATIC S7-300...

CISA

ICS-CERT Landing > ICS-CERT Advisories > Siemens SIMATIC S7-300 CPU Denial-of-Service Vulnerability

ICS Advisory (ICSA-15-064-04)

More ICS-CERT Advisories

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

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

Print Tweet Send Share

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 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 Pfahl, 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

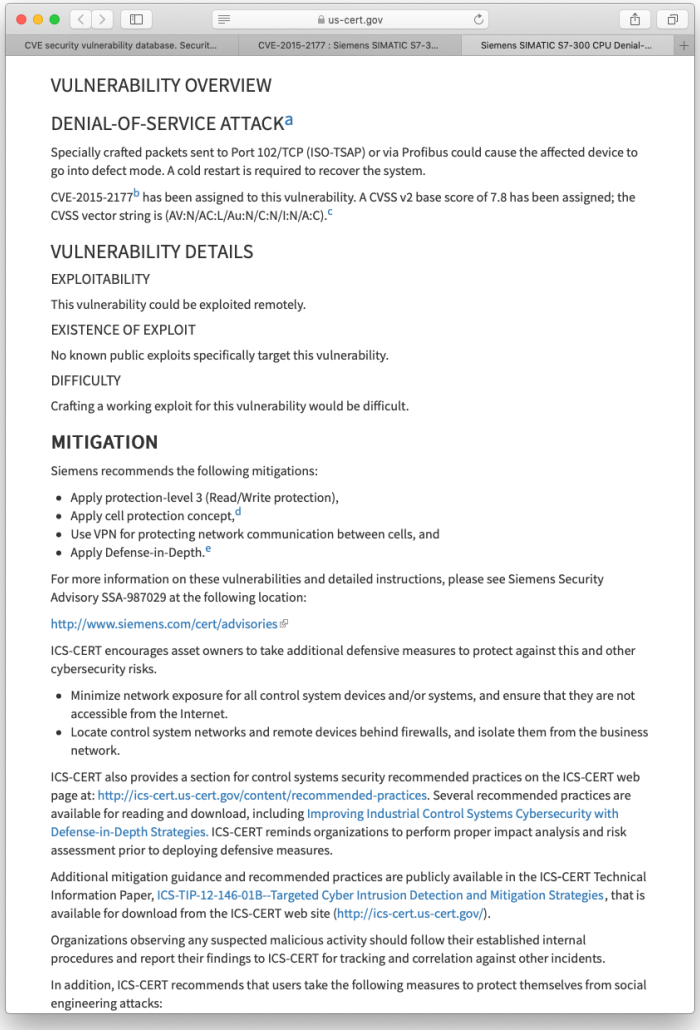
This vulnerability could allow attackers to perform a DoS attack over the network without prior authentication against S7-300 CPUs under certain conditions. A cold restart is required to recover the system.

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.



us-cert.gov

CVE security vulnerability database. Securit... | CVE-2015-2177 : Siemens SIMATIC S7-3... | Siemens SIMATIC S7-300 CPU Denial-...

VULNERABILITY OVERVIEW

DENIAL-OF-SERVICE ATTACK[a]

Specially 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 (AV:N/AC:L/Au:N/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 for 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-987029 at the following location:

http://www.siemens.com/cert/advisories

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-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies, 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.

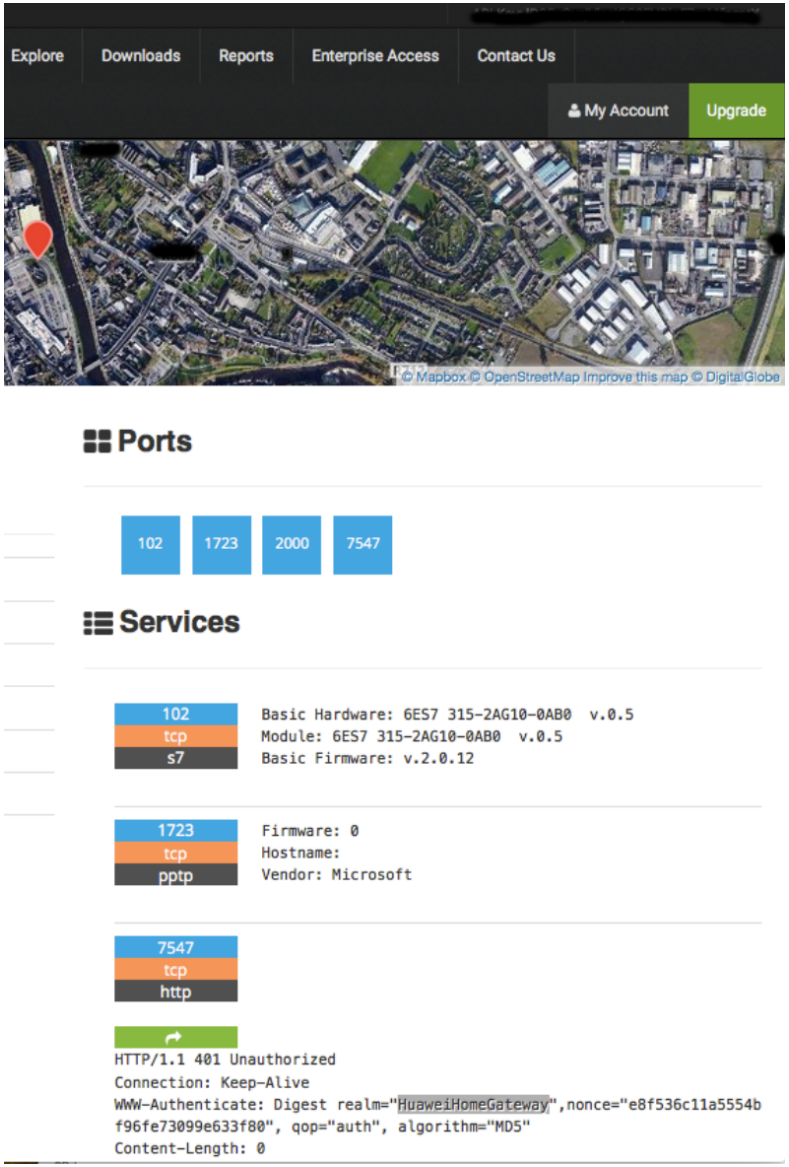
In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

Vulnerabilities

S7comm on Port 102

CVE-2015-2177 Denial of service;

Preset userid/password `Basisk`;



Vulnerabilities

S7comm on Port 102

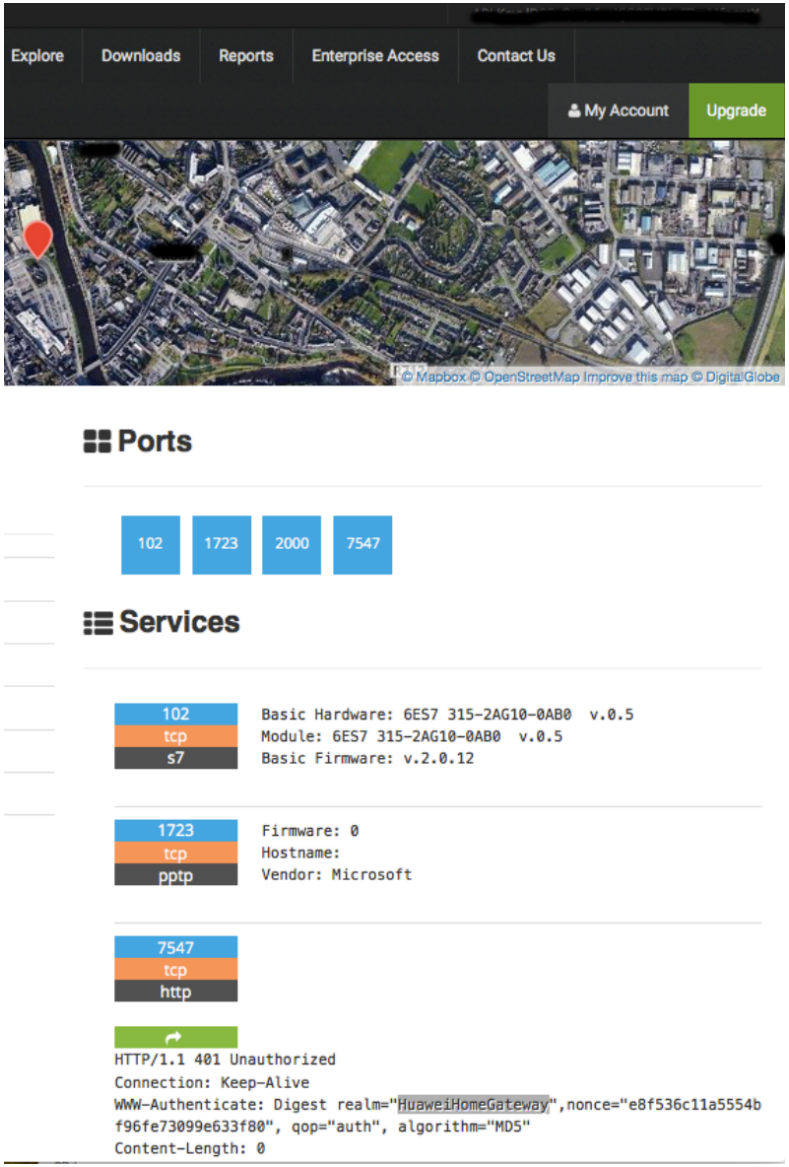
CVE-2015-2177 Denial of service;

Preset userid/password `Basisk`;

PPTP on Port 1723

MS Security Advisory 2743314:

MS-CHAPv2 weakness;...



Vulnerabilities

S7comm on Port 102

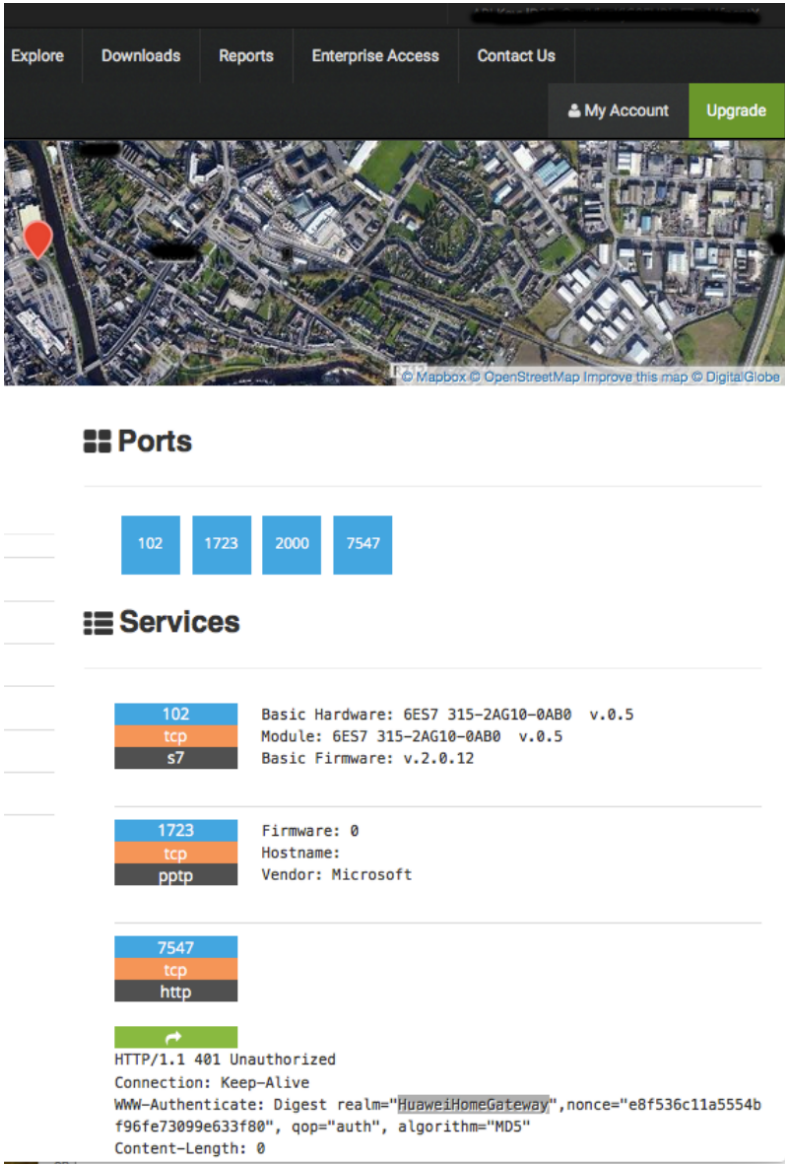
CVE-2015-2177 Denial of service;
Preset userid/password `Basisk`;

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

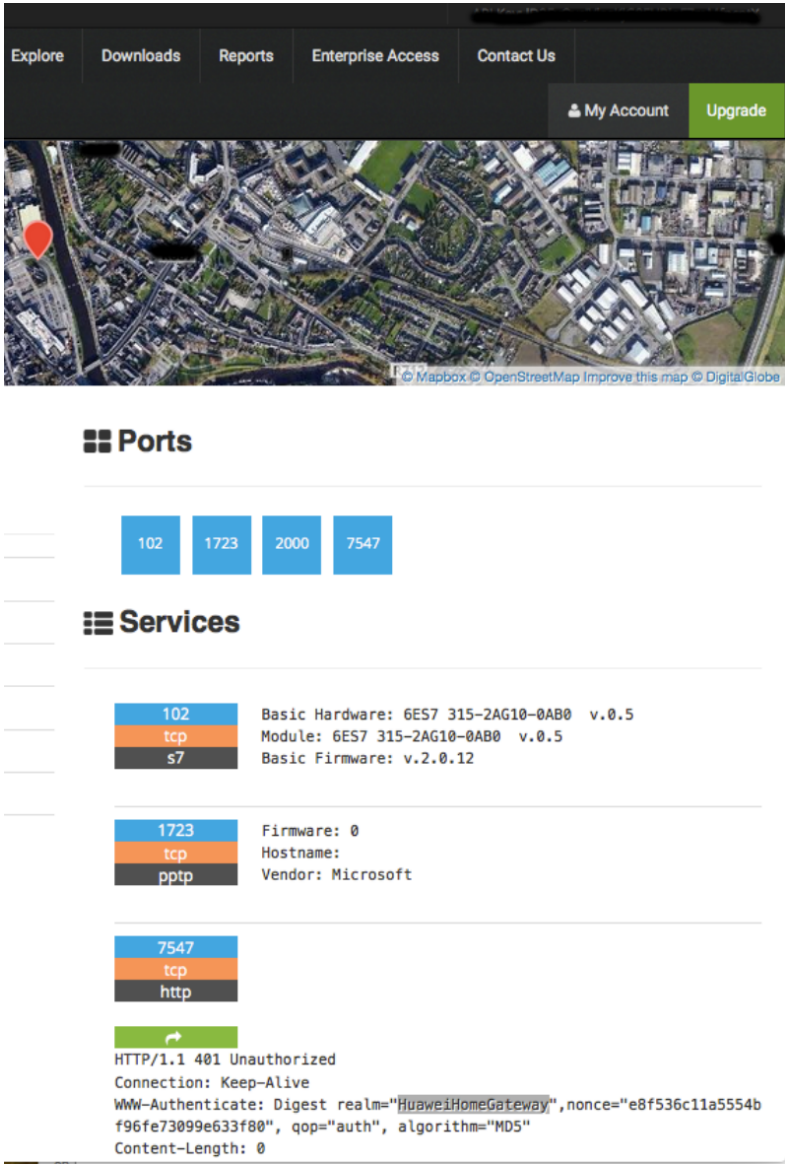
MS Security Advisory 2743314:
MS-CHAPv2 weakness;. . .

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;. . .

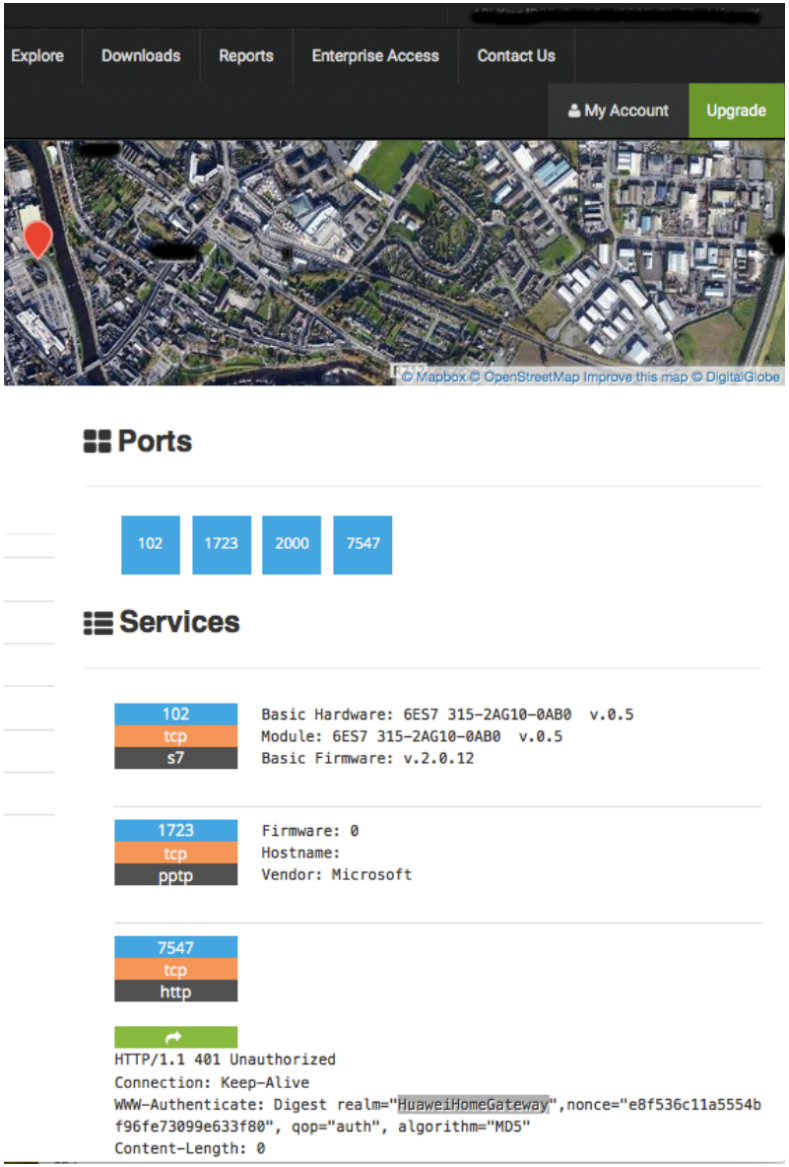
CWMP over HTTP

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, ..

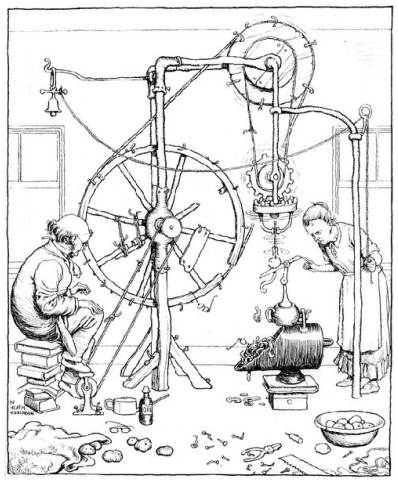
What exactly are the objectives?

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.

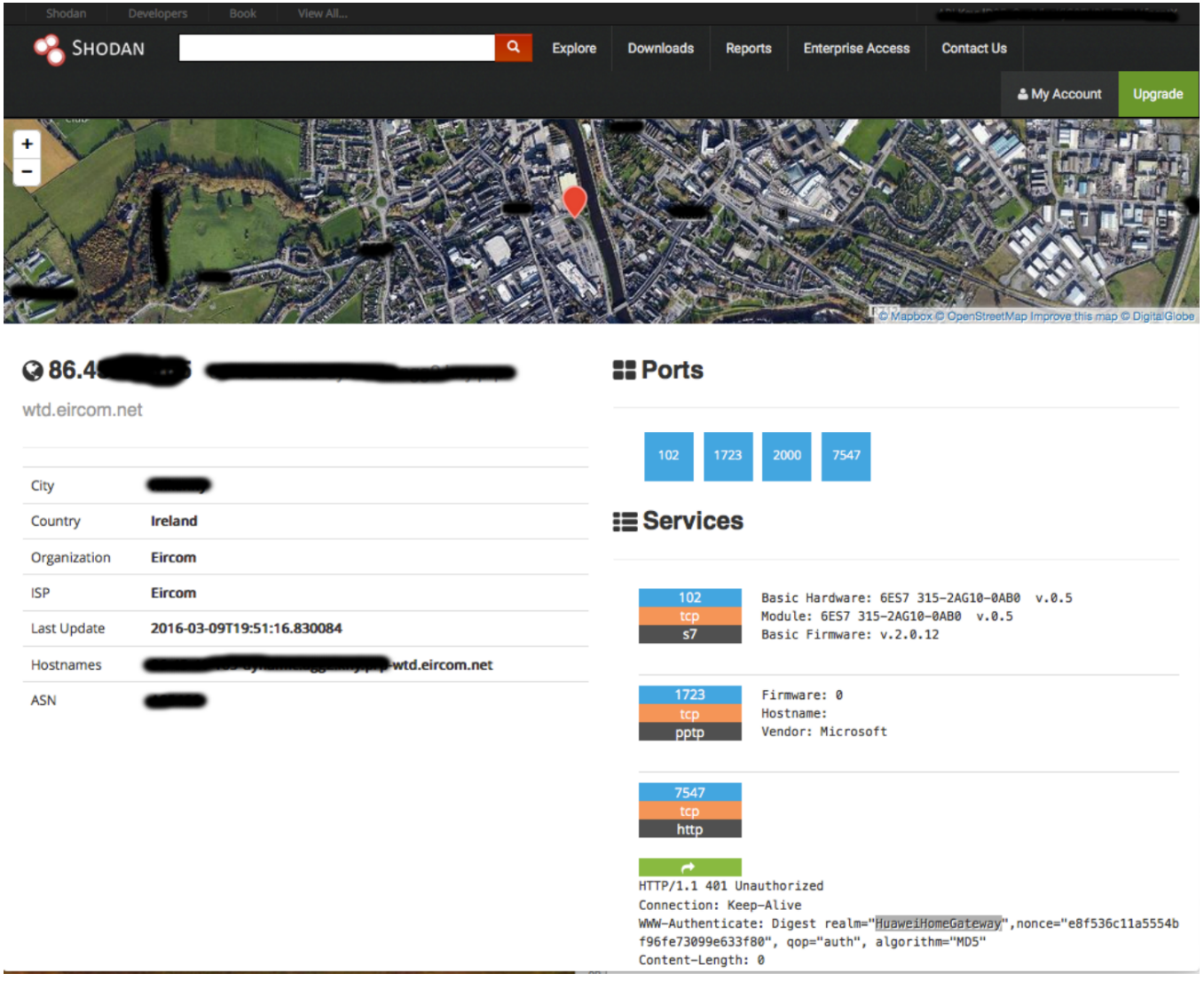


The Professor's invention for peeling potatoes.

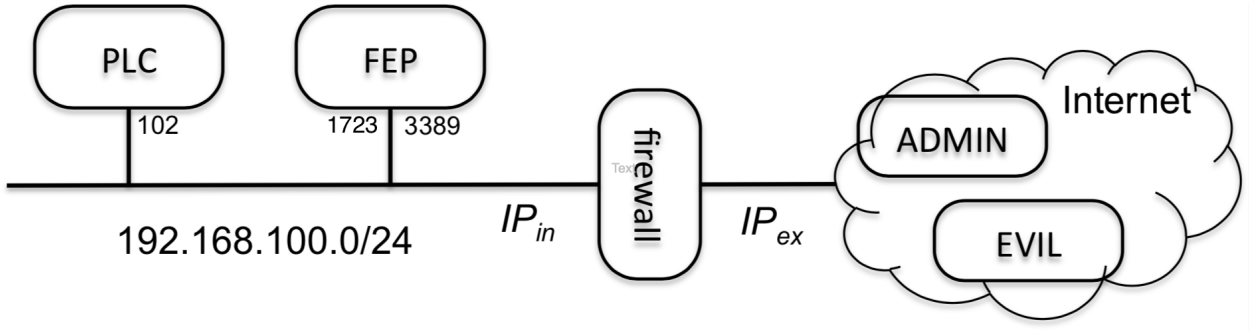
Outline of Talk

The ICS use case

Siemens S7comm protocol over TCP/TSAP on Port 102



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	...	*.*.*.*	$\geq$ 1024	PLC	102	ALLOW
2	...	*.*.*.*	$\geq$ 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. Siemen's 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.

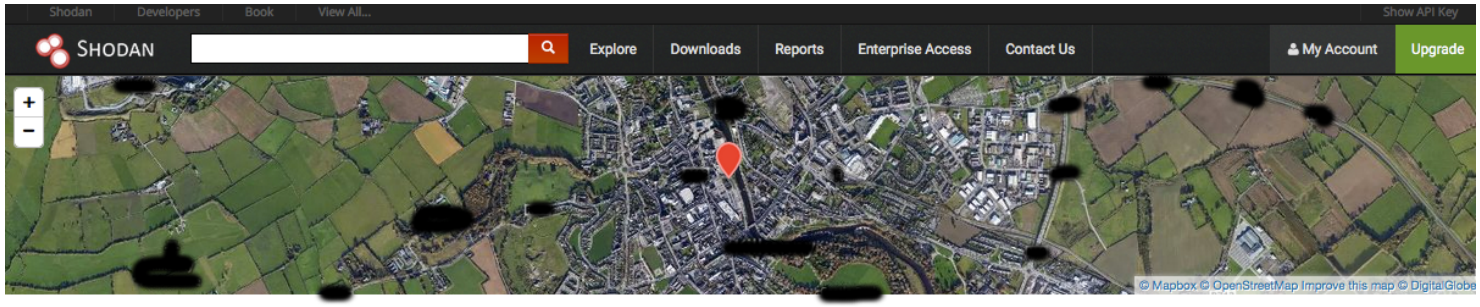
Best practices, for example [4], recommend that the controller and PLCs should be deployed on an internal control network and a VPN tunnel used when accessing the controller over the Internet/public network. VPN access to the local Control Network does appear to be provided via PPTP on Port 1723 on the 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



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 / tcp / s7

```
Basic Hardware: 6ES7 315-2AG10-0AB0  v.0.5
Module: 6ES7 315-2AG10-0AB0  v.0.5
Basic Firmware: v.2.0.12
```

1723 / tcp / pptp

```
Firmware: 0
Hostname:
Vendor: Microsoft
```

3389 / tcp / rdp

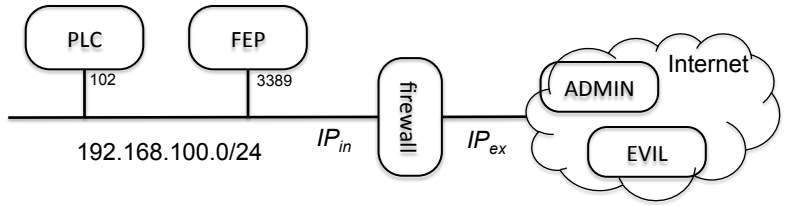
```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00
```

7547 / tcp / http

```
HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="e8f536c11a5554bf96fe73099e6
33f80", qop="auth", algorithm="MD5"
Content-Length: 0
```

Firewall policy objectives

(Keep things simple: VPN via Port 3389)

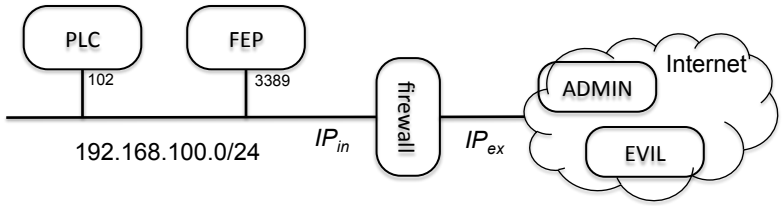


Initial policy *UPol*

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

Firewall policy objectives

(Keep things simple: VPN via Port 3389)



Initial policy *UPol*

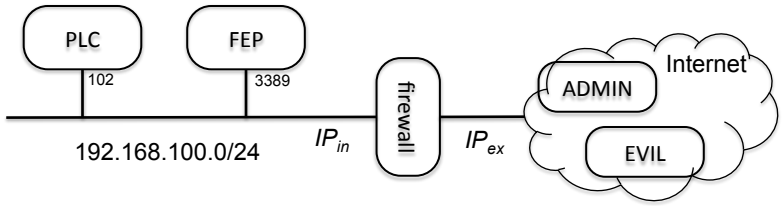
Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	*.*.*.*	$\geq$ 1024	PLC	102	ALLOW
2	...	*.*.*.*	$\geq$ 1024	FEP	3389	ALLOW

CPNI Recommendations: *CPNI*

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

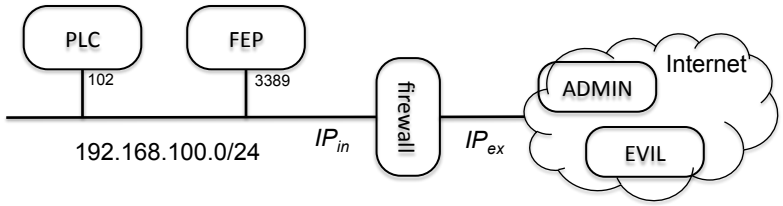
CPNI Recommendations: *CPNI*

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

Remote Desktop Policy: *RPol*

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

Composition of policy objectives

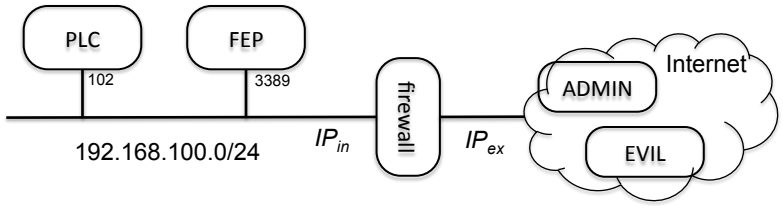


UPol;*CPNI*;*RPol*

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

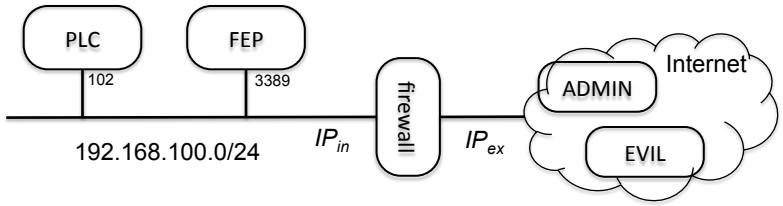


UPol;*CPNI*;*RPol*

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



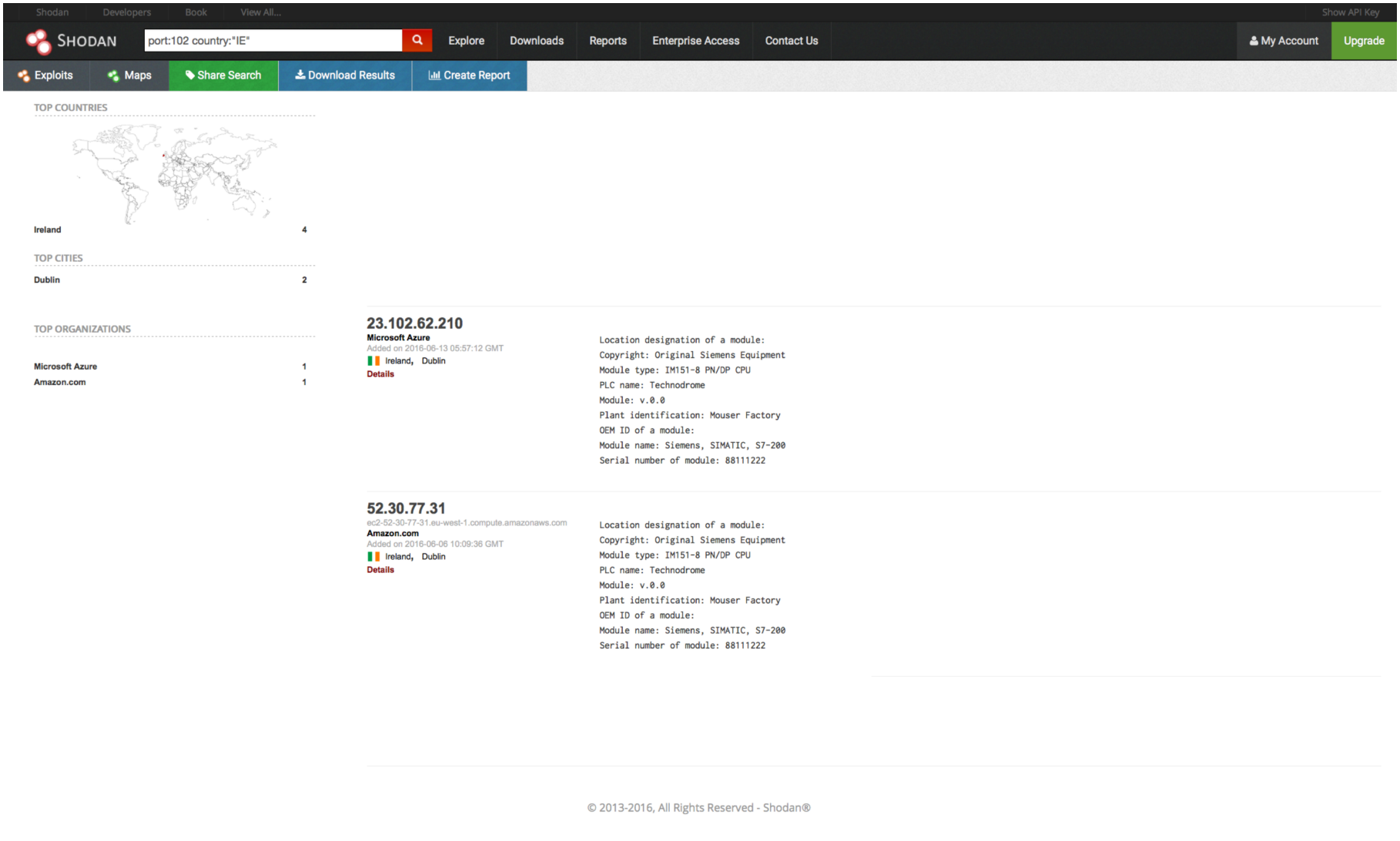
$$UPol ; CPNI ; RPol$$

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

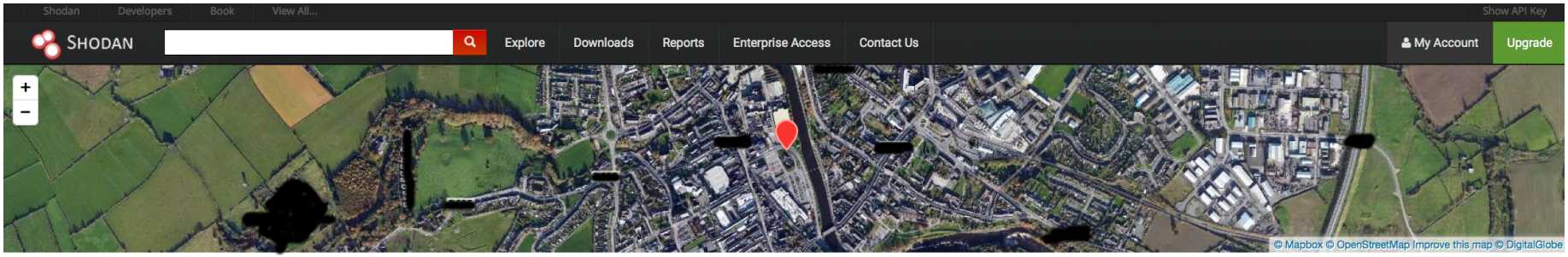
A *redundancy* conflict occurs when two firewall rules can filter the same packets and those rules have the same target actions over those packets and that the removal of the redundant rule does not affect the semantics of the firewall configuration.

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



Postscript - June 2016



86[redacted] [redacted]

City	[redacted]
Country	**Ireland**
Organization	**Eircom**
ISP	**Eircom**
Last Update	**2016-06-14T22:00:46.815189**
Hostnames	[redacted]
ASN	[redacted]

Ports

102 3389 7547

Services

102 tcp s7

```
Copyright: Original Siemens Equipment
PLC name:
Module type: CPU 315-2 DP
Unknown (129): Boot Loader           A
Module: 6ES7 315-2AG10-0AB0  v.0.5
Basic Firmware: v.2.6.11
Module name: CPU 315-2 DP
Serial number of module:
Plant identification:
Basic Hardware: 6ES7 315-2AG10-0AB0  v.0.5
```

3389 tcp rdp

```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00
```

7547 tcp http

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

Postscript - October 2016

[redacted]

City	[redacted]
Country	**Ireland**
Organization	**Eircom**
ISP	**Eircom**
Last Update	**2016-10-25T16:44:41.375207**
Hostnames	[redacted]
ASN	**AS5466**

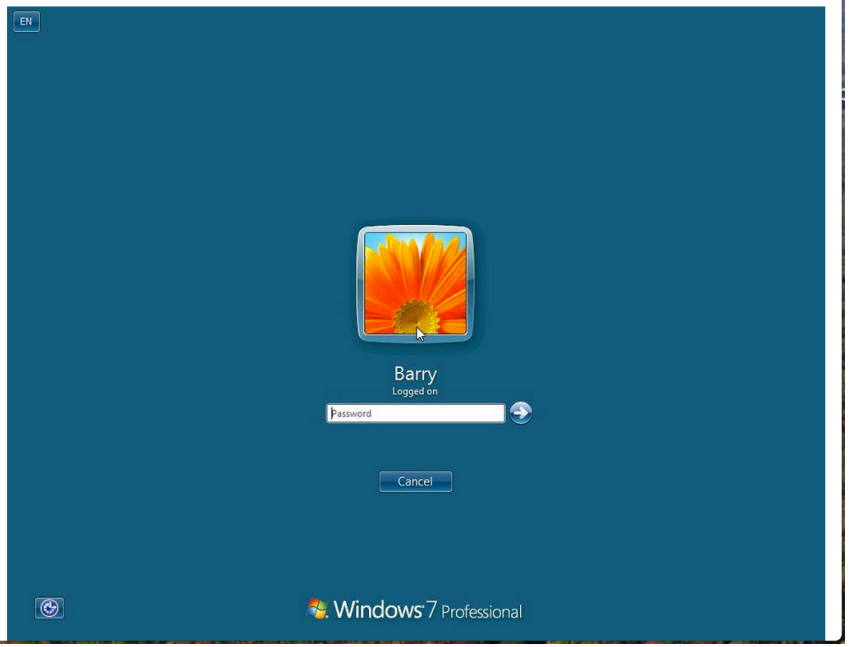
Ports

3389

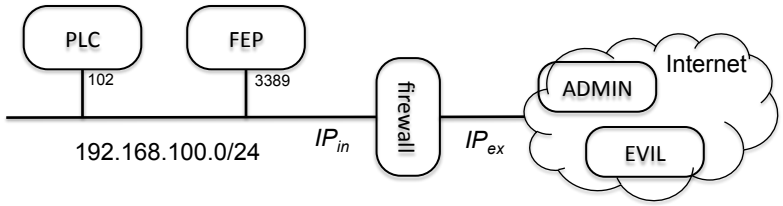
Services

3389
tcp
rdp

Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00



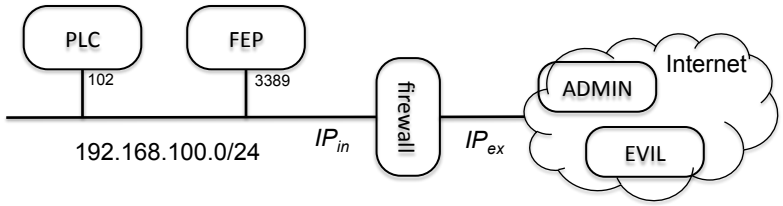
Composition of policy objectives



$CPNI ; RPol ; UPol$

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

Composition of policy objectives



CPNI;*RPol*;*UPol*

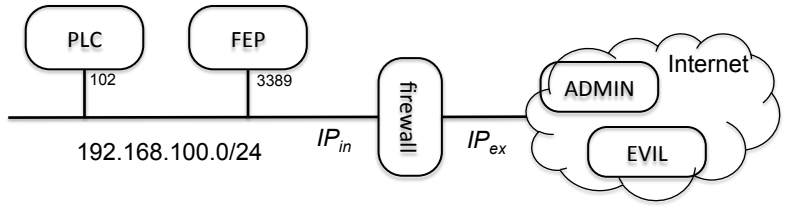
Index	[...]	Src IP	Src Port	Dst IP	Dst Port	Action
1	...	192.168.100.0/24	$\geq$ 1024	PLC	102	ALLOW
2	...	external IPs	*	PLC	102	DROP
3	...	external IPs	$\geq$ 1024	FEP	3389	ALLOW
4	...	ADMIN	$\geq$ 1024	FEP	3389	ALLOW
5	...	*.*.*.*	*	FEP	3389	DROP
6	...	*.*.*.*	$\geq$ 1024	PLC	102	ALLOW
7	...	*.*.*.*	$\geq$ 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 much be searched for and updated.]

Postscript - December 2016

City	
Country	**Ireland**
Organization	**Eircom**
ISP	**Eircom**
Last Update	**2016-10-25T16:44:41.375207**
Hostnames	
ASN	**AS5466**

Composition of policy objectives



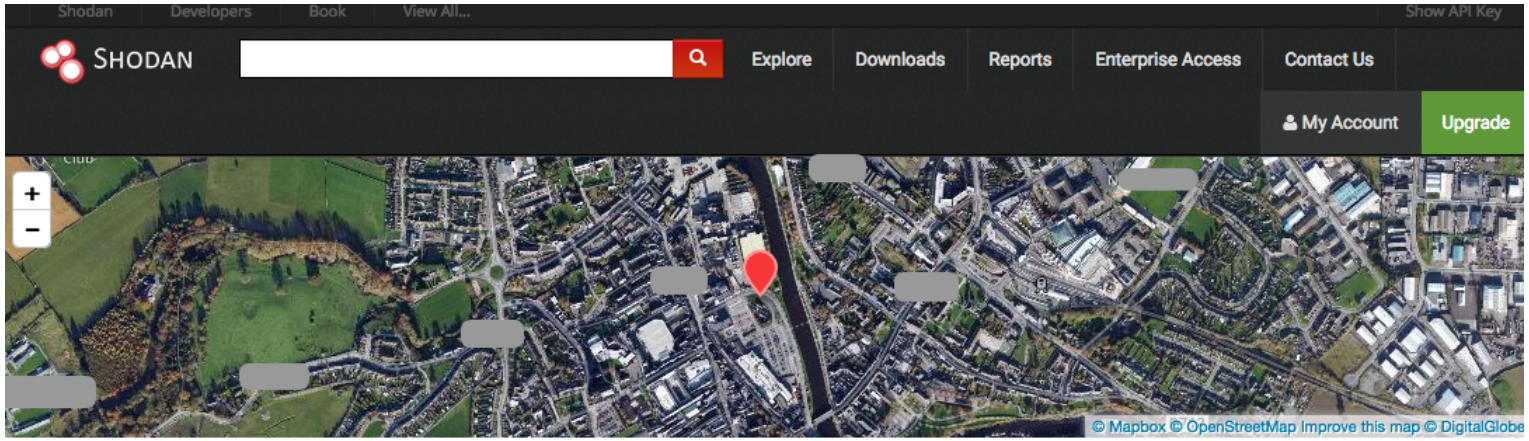
RPol;*CPNI*;*UPol*

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



86.4 [redacted]

[redacted]

City	[redacted]
Country	**Ireland**
Organization	**Eircom**
ISP	**Eircom**
Last Update	**2017-03-01T11:43:16.867182**
Hostnames	[redacted]
ASN	**AS5466**

Ports

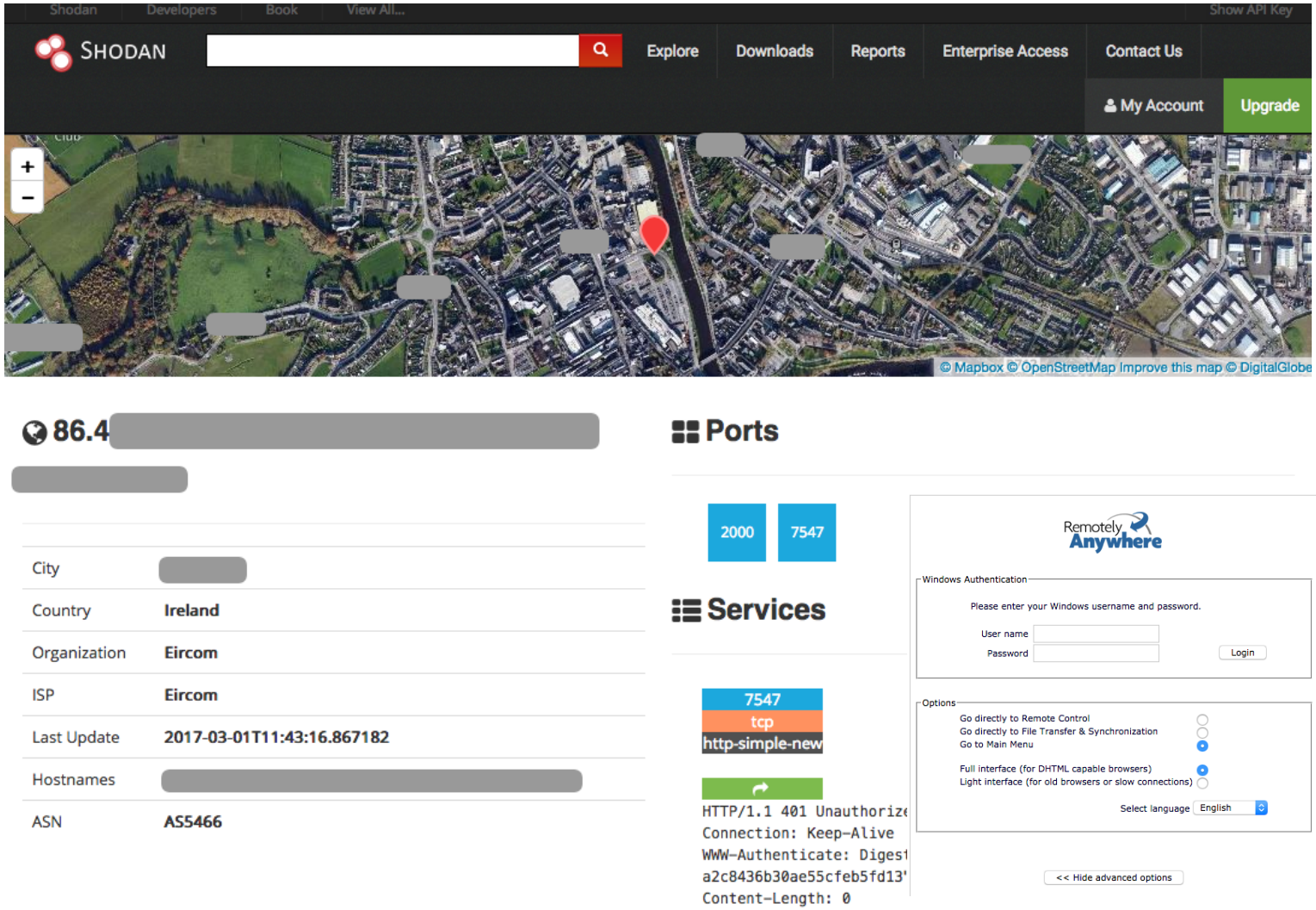
2000 7547

Services

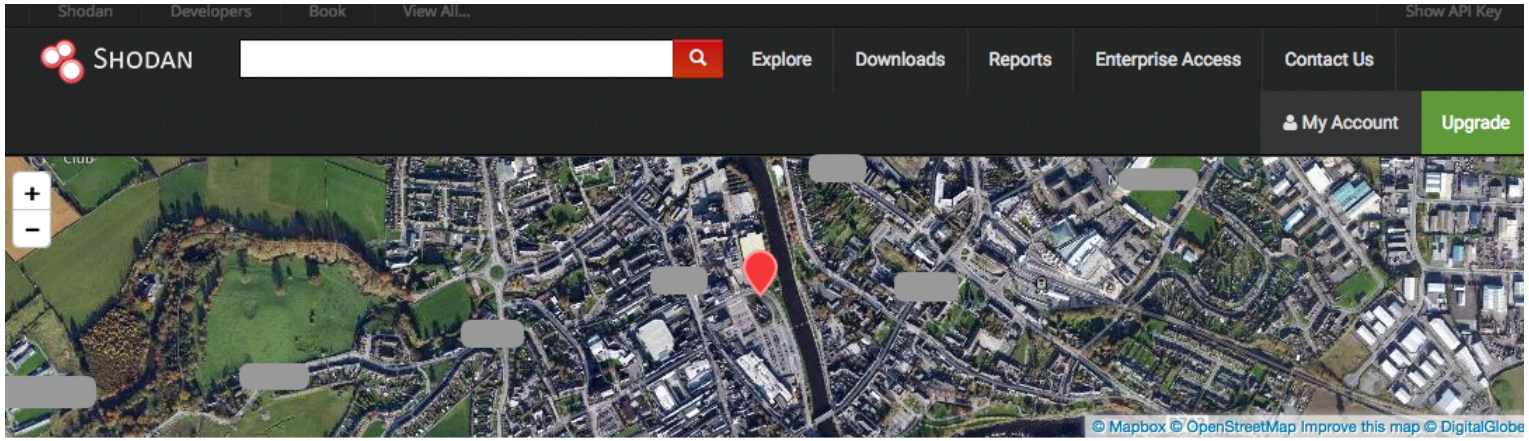
7547
tcp
http-simple-new

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

Postscript - 03 March 2017



Postscript - 03 March 2017



86.4[redacted]

[redacted]

City	[redacted]
Country	**Ireland**
Organization	**Eircom**
ISP	**Eircom**
Last Update	**2017-03-01T11:43:16.867182**
Hostnames	[redacted]
ASN	**AS5466**

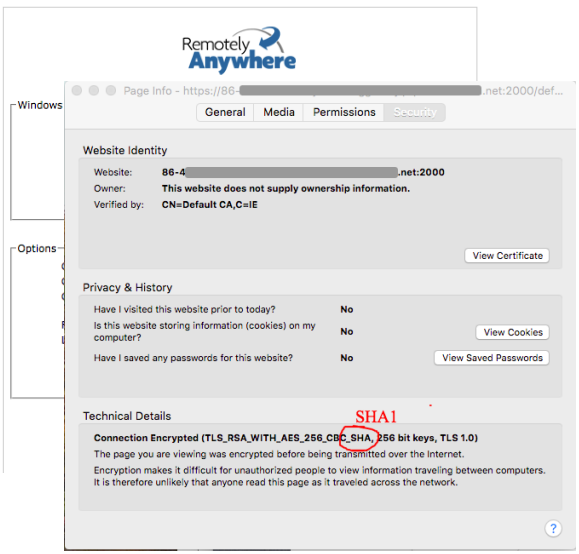
Ports

2000 7547

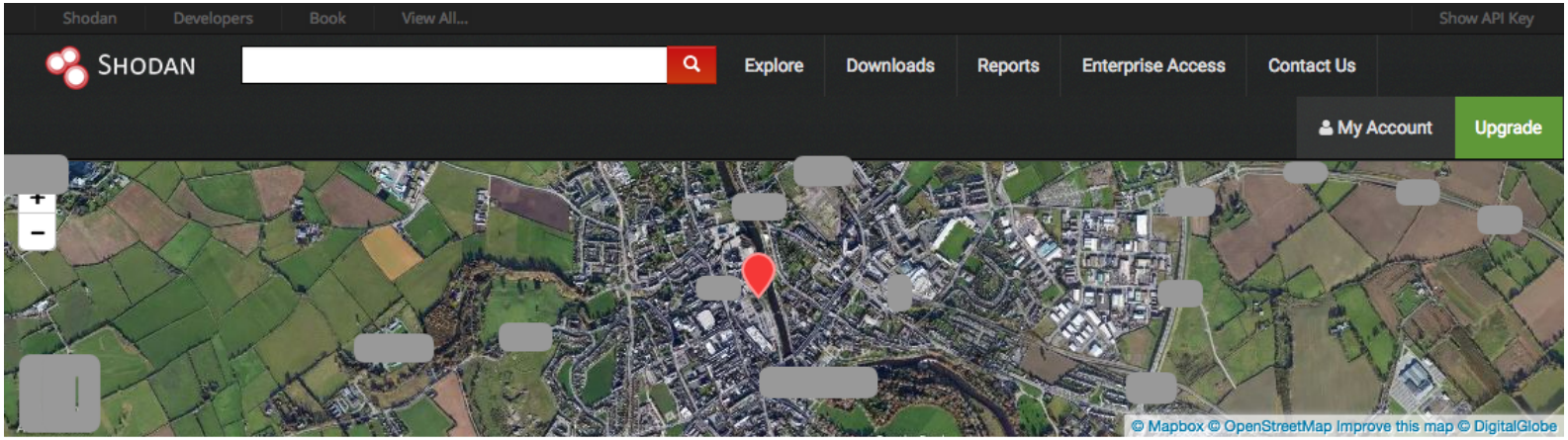
Services

7547
tcp
http-simple-new

```
HTTP/1.1 401 Unauthorize
Connection: Keep-Alive
WWW-Authenticate: Digest
a2c8436b30ae55cfeb5fd13'
Content-Length: 0
```



Postscript - 13 March 2017



86.4 [redacted]

[redacted]

City	[redacted]
Country	**Ireland**
Organization	**Eircom**
ISP	**Eircom**
Last Update	**2017-03-12T05:42:47.873487**
Hostnames	**86-4**[redacted]
ASN	**AS5466**

Ports

2000 3389 7547

Services

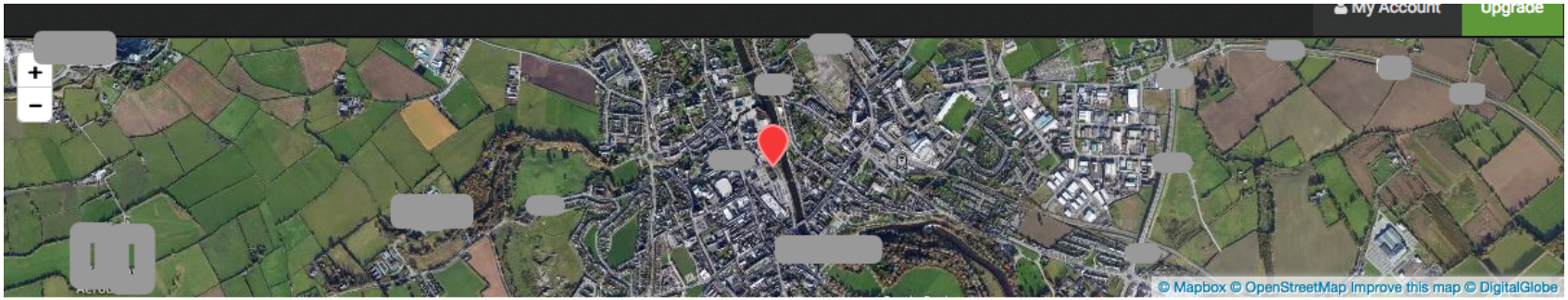
3389
tcp
rdp

```
Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\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. [redacted]

wtd.eircom.net

City	[redacted]
Country	**Ireland**
Organization	**Eircom**
ISP	**Eircom**
Last Update	**2017-03-01T11:43:16.867182**
Hostnames	[redacted]
ASN	**AS5466**

Ports

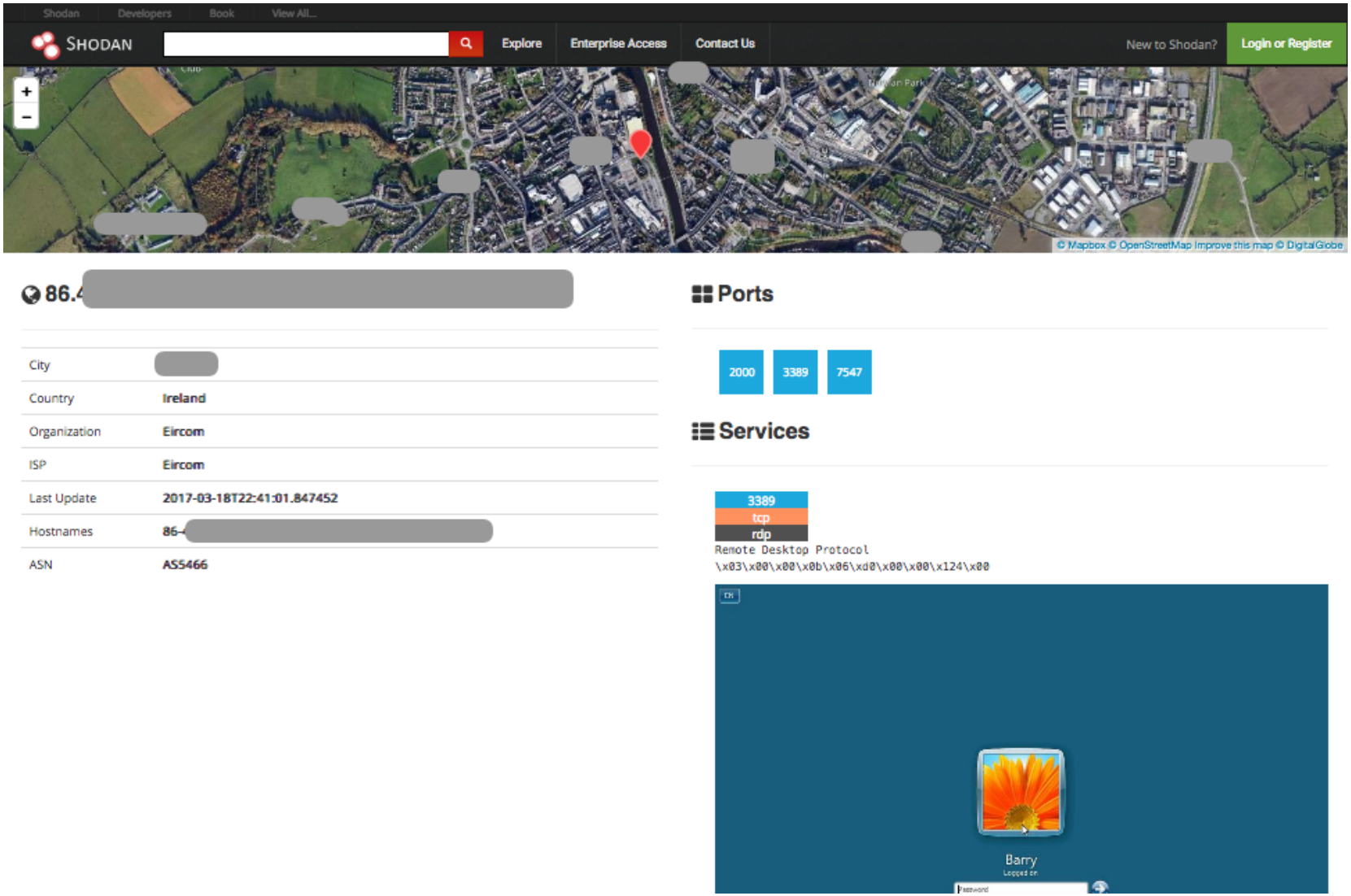
2000 7547

Services

7547
tcp
http-simple-new

```
HTTP/1.1 401 Unauthorized
Connection: Keep-Alive
WWW-Authenticate: Digest realm="HuaweiHomeGateway",nonce="1bb431991a2c8436b
30ae55cfeb5fd13", qop="auth", algorithm="MD5"
Content-Length: 0
```

Postscript - 20 March 2017



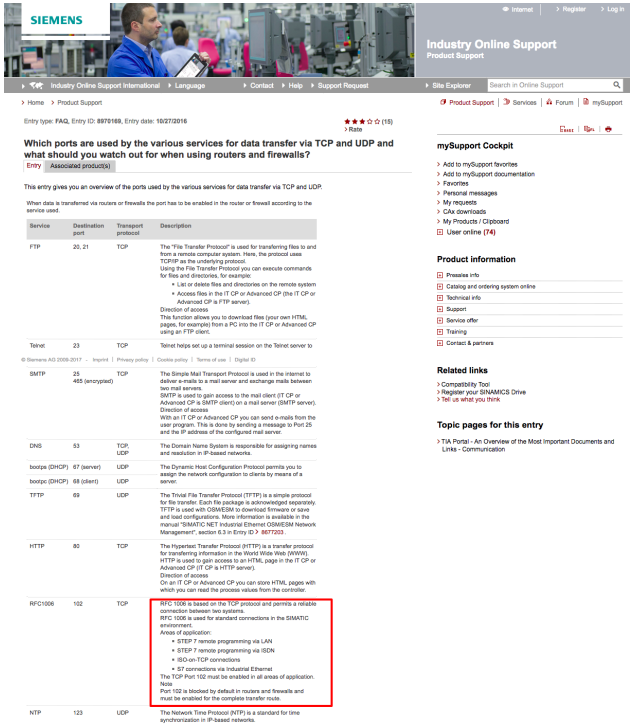
Outline of Talk

Conflicting control recommendations

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

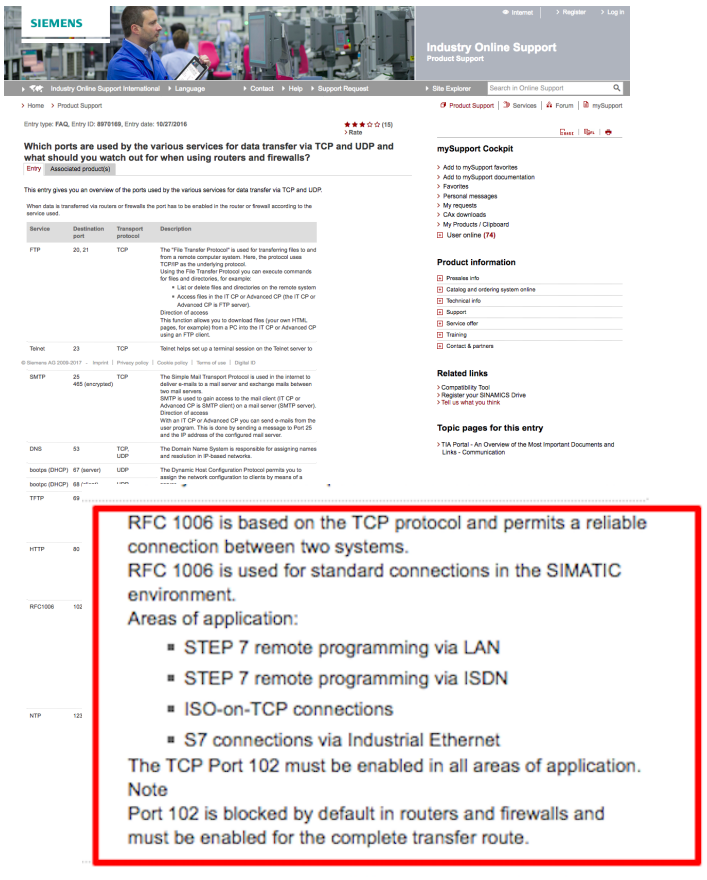
Conflicting control recommendations

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



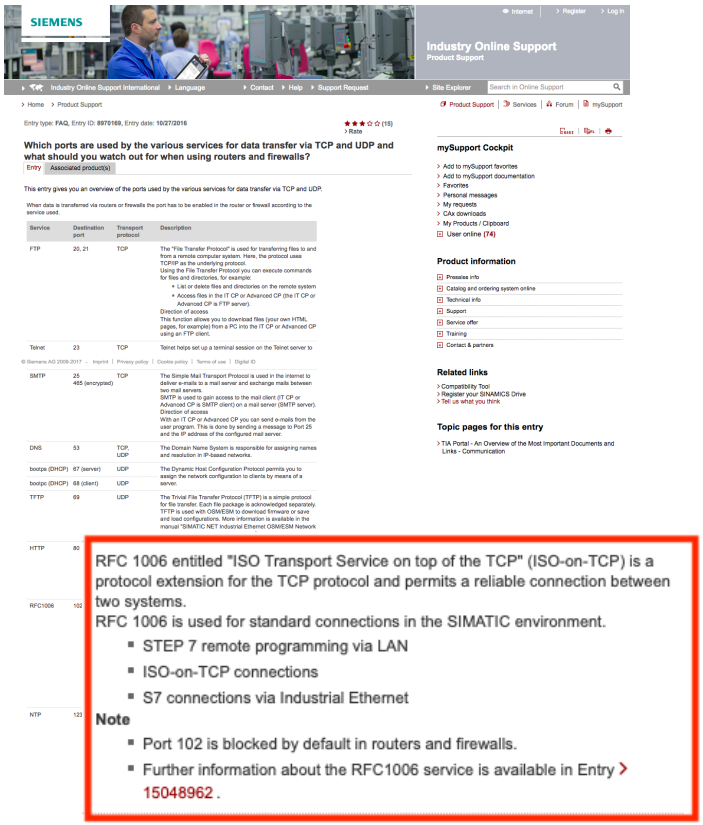
Conflicting control recommendations

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



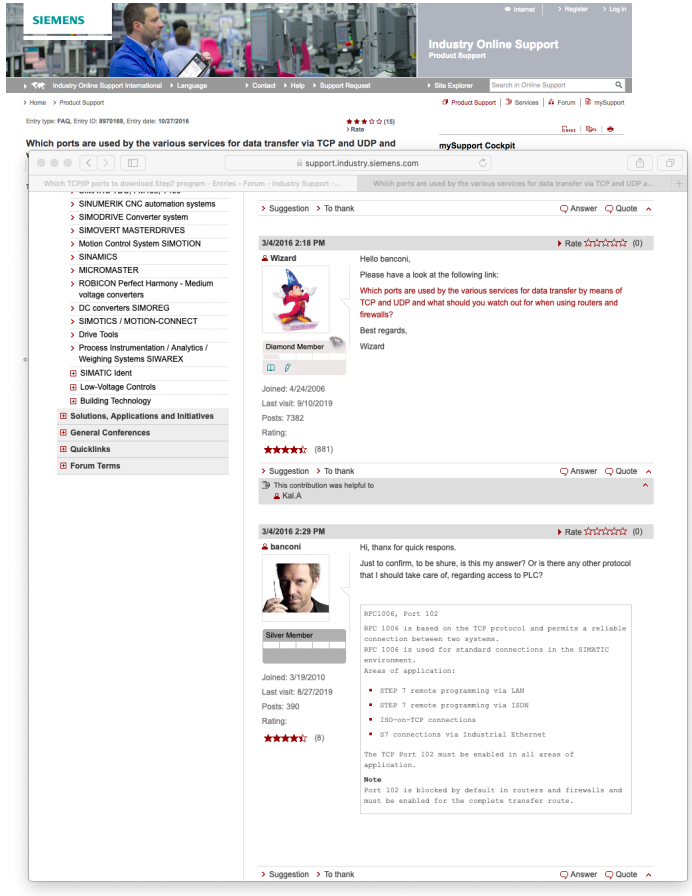
Conflicting control recommendations

- 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



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.

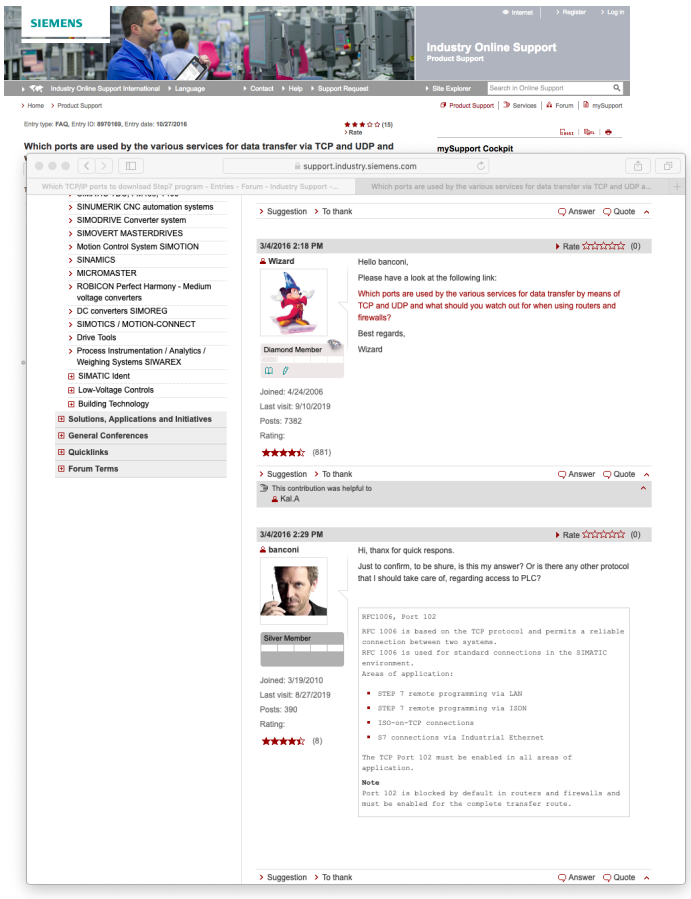


Conflicting control recommendations

- 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.



Security threat management for the ICS use case

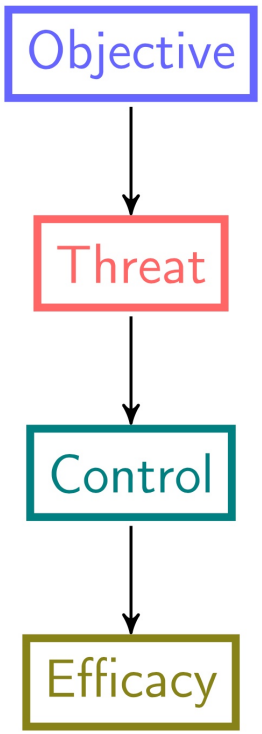
Objective: provide remote supervisory control to ICS

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

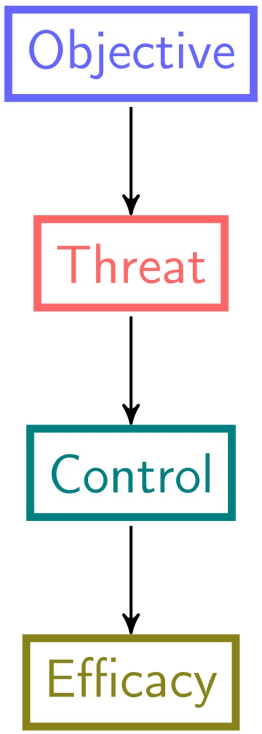
- CPNI: tunnel S7 traffic over VPN.
- Only admin IP may access via VPN.
- Software update mechanism.

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

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

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.

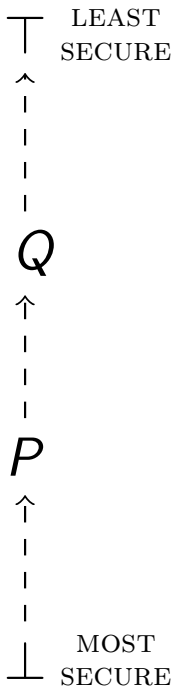
Shodan investigation only; did not visit/probe the sites

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.

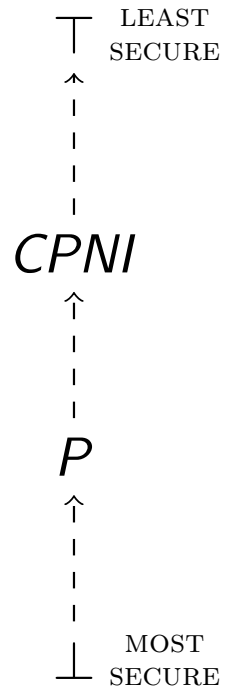


Security as comparison

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

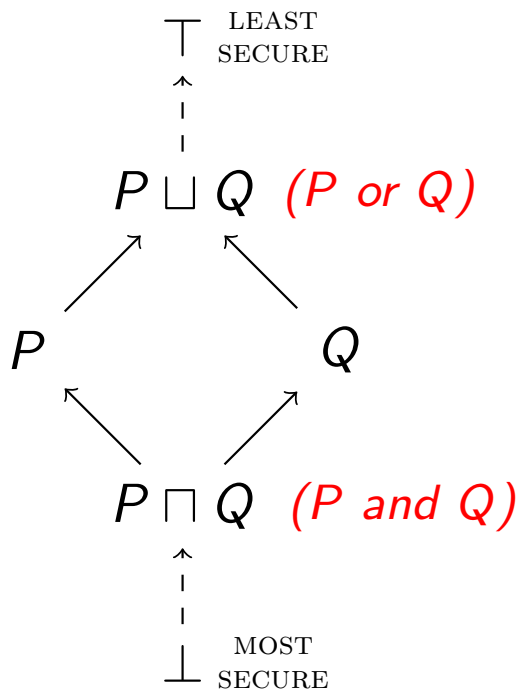
Formalizing what we mean by composition of policy objectives

Secure Replacement $P \sqsubseteq Q$

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

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 $P \sqcap (\mathit{CPNI} \sqcup \mathit{RFC5735})$



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 $P, Q : \mathit{Policy}$:

$$\begin{aligned} P \sqsubseteq Q &\equiv (\mathit{accepts}(P) \subseteq \mathit{accepts}(Q)) \wedge (\mathit{denies}(P) \supseteq \mathit{denies}(Q)) \\ P \sqcup Q &\Leftrightarrow (\mathit{accepts}(P) \cup \mathit{accepts}(Q)) \wedge (\mathit{denies}(P) \cap \mathit{denies}(Q)) \\ P \sqcap Q &\Leftrightarrow (\mathit{accepts}(P) \cap \mathit{accepts}(Q)) \wedge (\mathit{denies}(P) \cup \mathit{denies}(Q)) \end{aligned}$$

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

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

Policy compositions

$$\begin{aligned} \mathit{Pol} &= \mathit{UPol} \sqcap (\mathit{CPNI} \sqcup \mathit{RPol}) \\ &= (\mathit{RPol} \fatsemi \mathit{CPNI} \fatsemi \mathit{UPol}); \\ \mathit{Pol}' &= \mathit{Pol} \sqcap \mathit{RFC5735} \end{aligned}$$

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.