INDUSTRIAL CONTROL SYSTEMS

Pentesting PLCs 101

WHO AM I?

ARNAUD SOULLIÉ

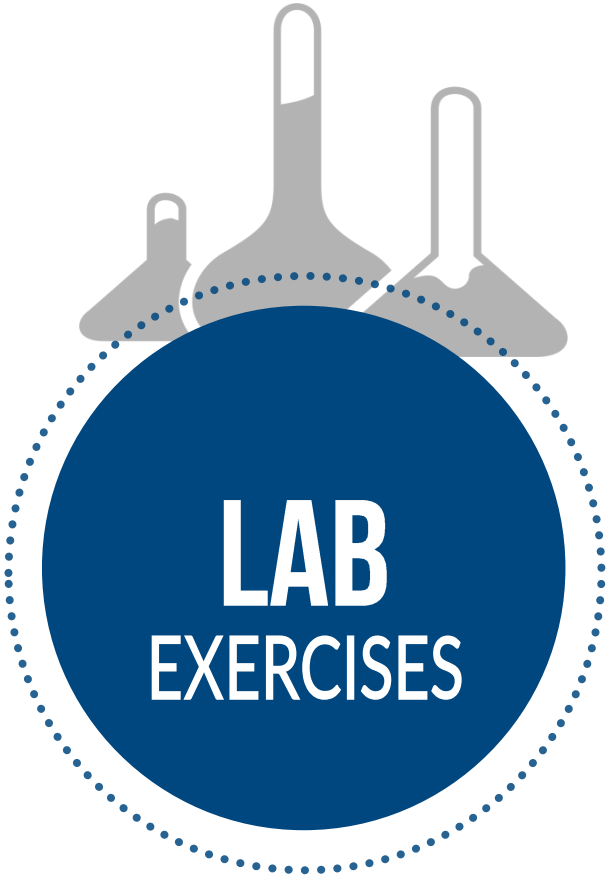
Senior security auditor

@arnaudsoullie

INTERESTS

- Windows Active Directory
  Can a Windows AD be secured ? JSSI 2013
  (French, sorry)
- SCADA stuff
- Wine tasting
  (we're not going to talk about it today)

solucom
management & IT consulting



LAB PREREQUISITE
WHAT'S IN THE LAB VM?

KALI LINUX

ADDITIONAL TOOLS

- MODBUSPAL
- MBTGET
- PLCSCAN
- SNAP7
- ...

SCRIPTS AND FILE EXAMPLES

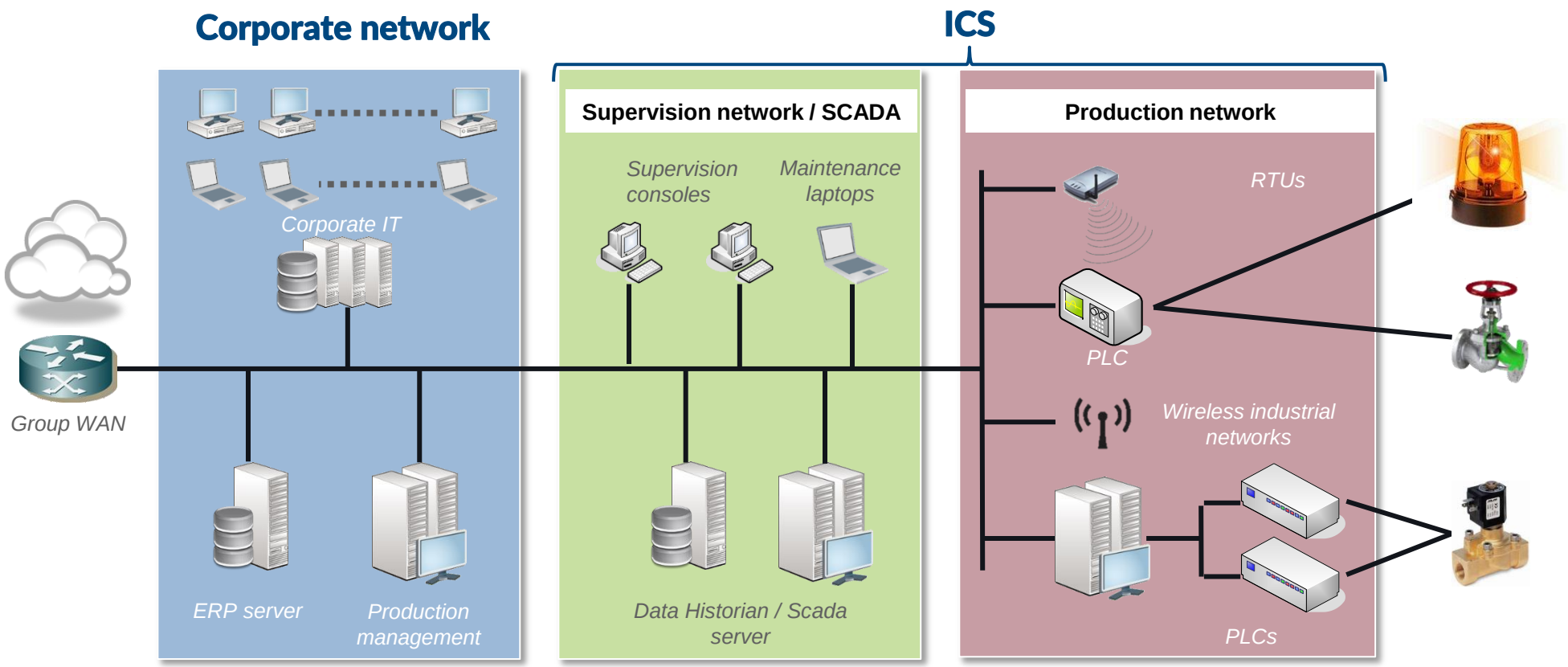
- PCAP SAMPLES
- SCRIPTS SKELETONS
- ...

AGENDA

1. ICS INTRODUCTION
2. MODBUS PROTOCOL
3. ATTACKING PLCS

ICS INTRODUCTION

WHAT IS AN INDUSTRIAL CONTROL SYSTEM (ICS)?



Corporate IS handle data

≠

ICS handle interfaces data with physical world

A BIT OF VOCABULARY

ICS (*Industrial Control System)*

=

IACS (*Industrial Automation and Control Systems)*

~=

SCADA (*Supervisory Control And Data Acquisition*)

~=

DCS (Distributed Control System)

Nowadays, people tend to say "SCADA" for anything related to ICS

ICS COMPONENTS

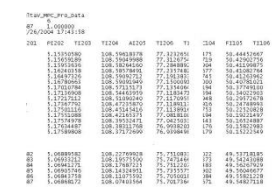
- **Sensors and actuators**: allow interaction with the physical world (pressure sensor, valves, motors, ...)

- **Local HMI**: Human-Machine Interface, permits the supervision and control of a subprocess

- **PLC**: Programmable Logic Controller : manages the sensors and actuators

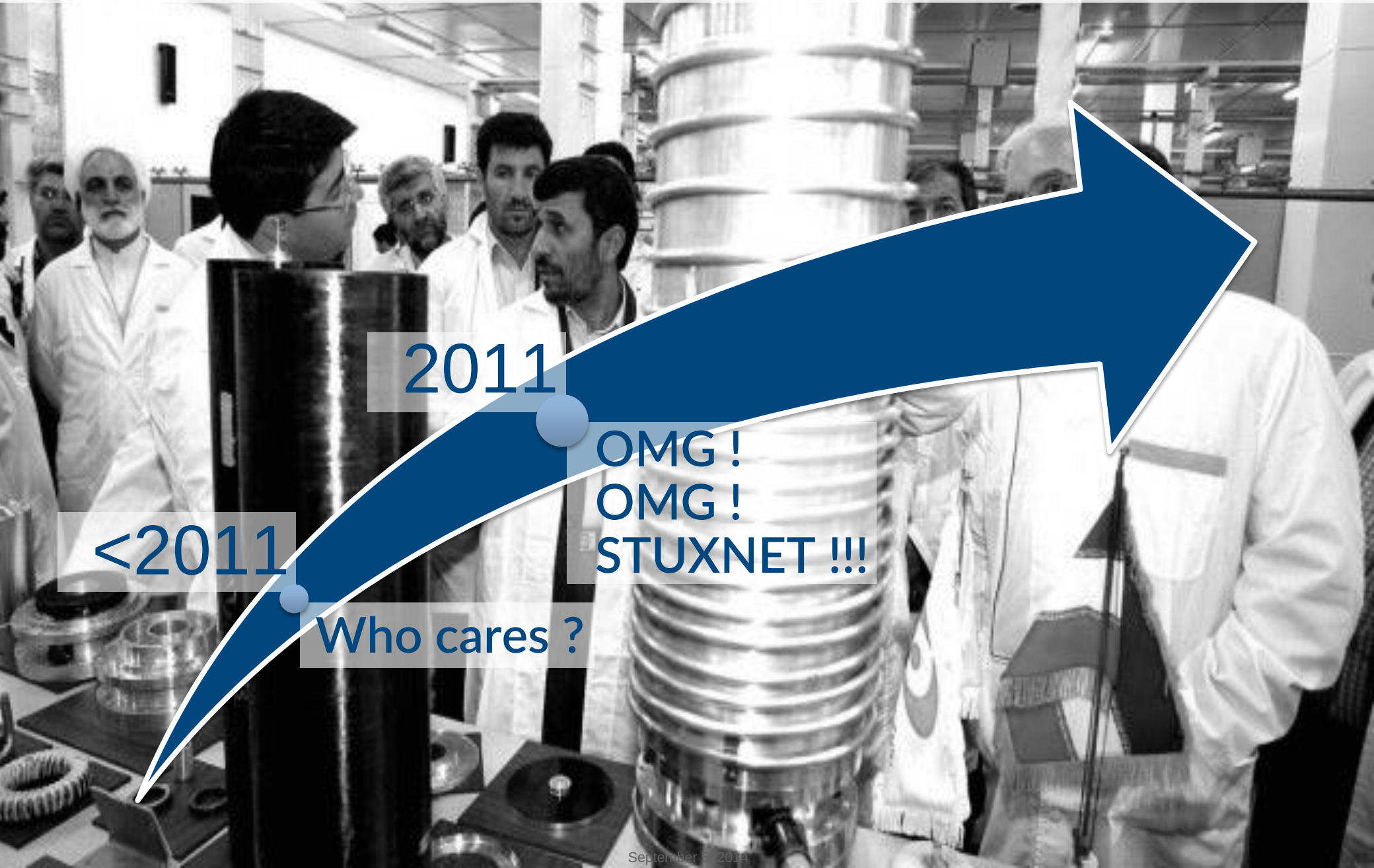
- **Supervision screen**: remote supervision of the industrial process

- **Data historian**: Records all the data from the production and Scada networks and allows exporting to the corporate IS (to the ERP for instance)

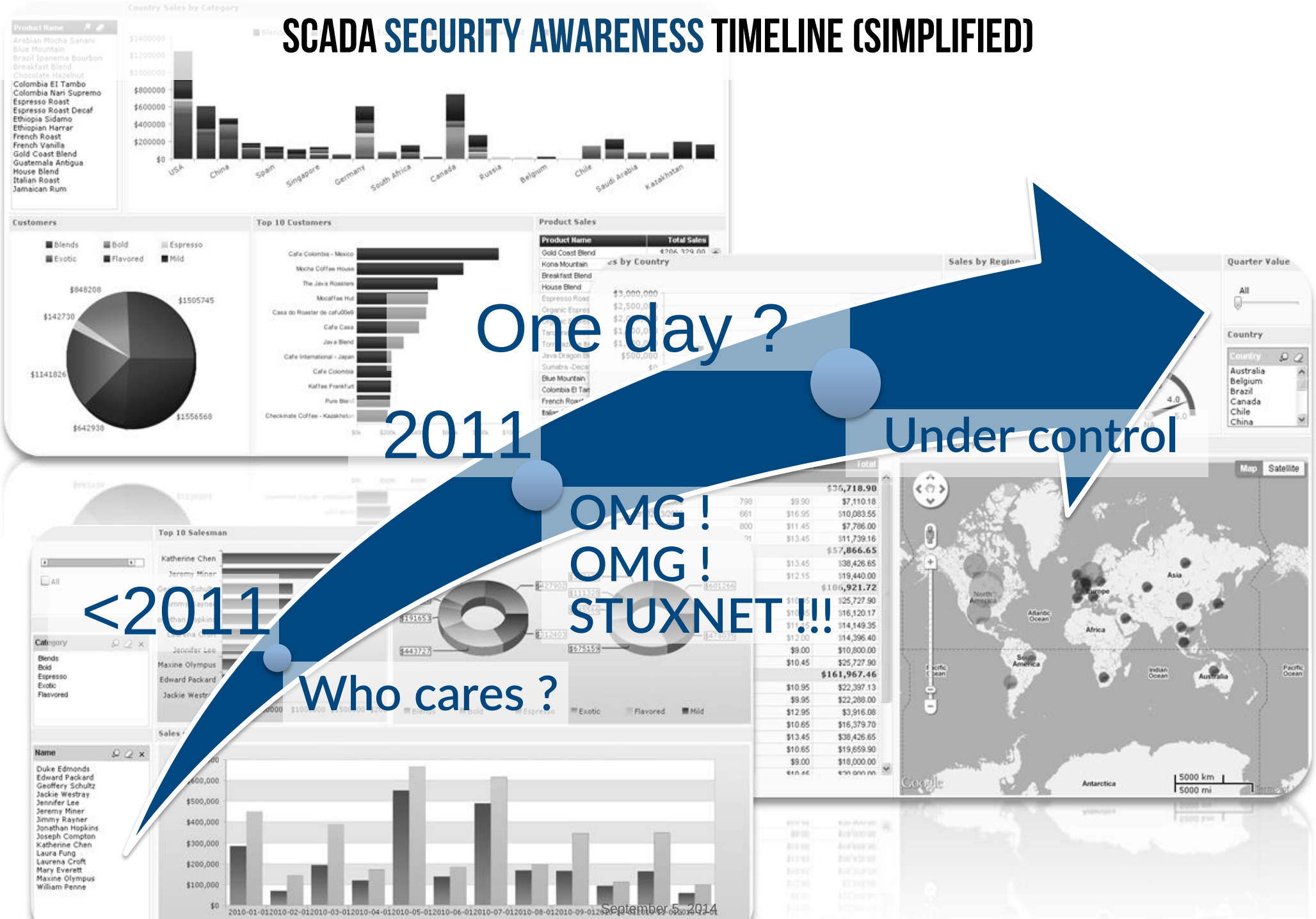


SCADA SECURITY AWARENESS TIMELINE (SIMPLIFIED)

SCADA SECURITY AWARENESS TIMELINE (SIMPLIFIED)



SCADA SECURITY AWARENESS TIMELINE (SIMPLIFIED)



WHAT IS WRONG WITH CURRENT ICS SECURITY?

- ORGANIZATION & AWARENESS
- NETWORK SEGMENTATION
- VULNERABILITY MANAGEMENT
- SECURITY IN PROTOCOLS
- THIRD PARTY MANAGEMENT
- SECURITY SUPERVISION

ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

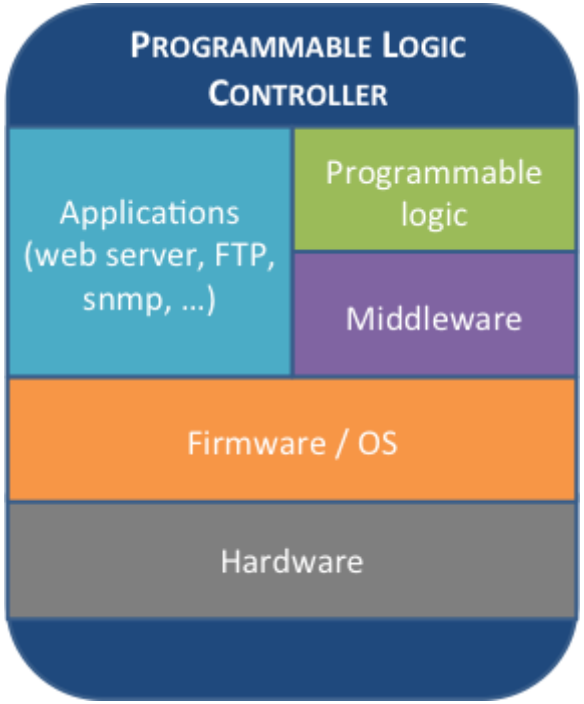
ICS-CERT listed over **250 attacks** on ICS in 2013

- **59%** of attacks targeted the energy sector
- **79** attacks successfully compromised the target
- **57** attacks did not succeed in compromising the target
- **120** attacks were not identified/investigated

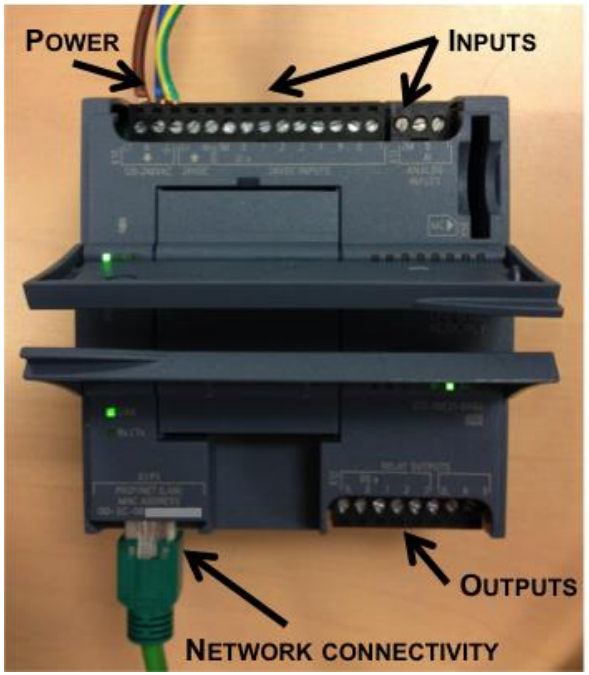
WHAT IS A PLC?

- Real-time digital computer used for automation
- Replaces electrical relays
- Lots of analogue or digital inputs & outputs
- Rugged devices (immune to vibration, electrical noise, temperature, dust, ...)

WHAT'S INSIDE ?



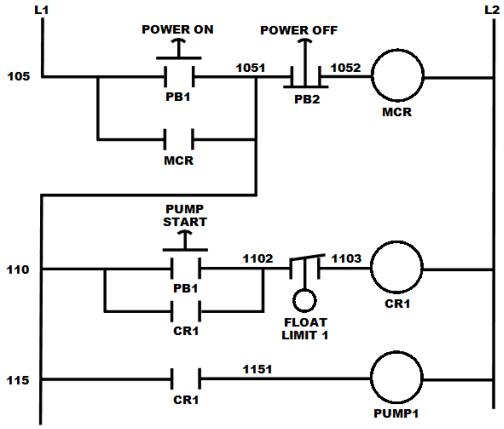
SIEMENS S7-1200



PLC
PROGRAMMING

- "*Ladder Logic*" was the first programming language for PLC, as it mimics the real-life circuits
- IEC 61131-3 defines 5 programming languages for PLCs
  - LD: Ladder Diagram
  - FBD: Function Block Diagram
  - ST: Structured Text
  - IL: Instruction List
  - SFC: Sequential Function Chart

LADDER DIAGRAM EXAMPLE



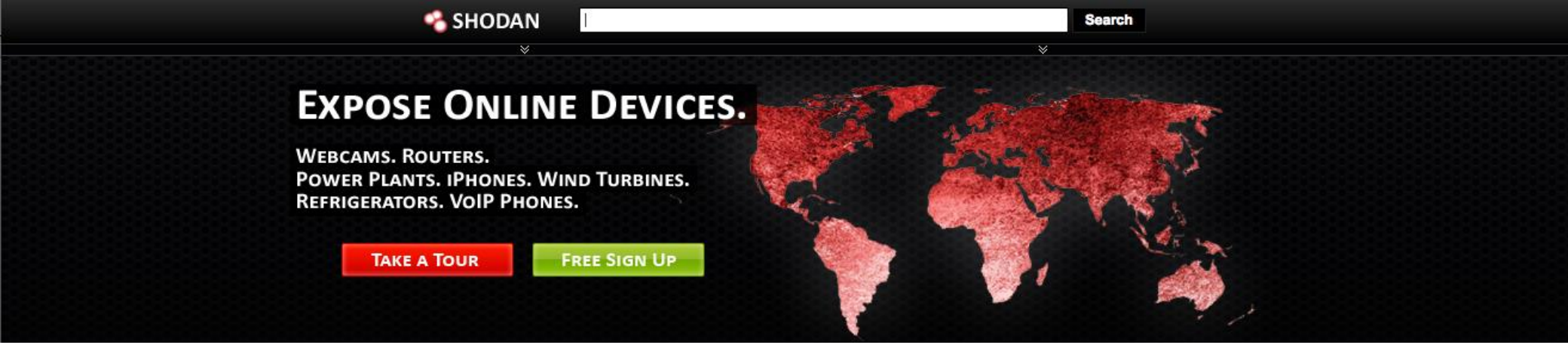
STRUCTURED TEXT EXAMPLE

```
(* simple state machine *)
TxtState := STATES[StateMachine];

CASE StateMachine OF
   1: ClosingValve();
ELSE
    ;; BadCase();
END_CASE;
```

INSTRUCTION LIST EXAMPLE

```
LD      Speed
          GT      1000
          JMPCN   VOLTS_OK
          LD      Volts
VOLTS_OK  LD      1
          ST      %Q75
```



- Shodan is a search engine dedicated to find devices exposed to the Internet
- It regularly scans the whole Internet IPV4 range (~4,3 billions IPs)
- Results are partially free (you have to pay to export the results)

WHAT CAN YOU FIND?

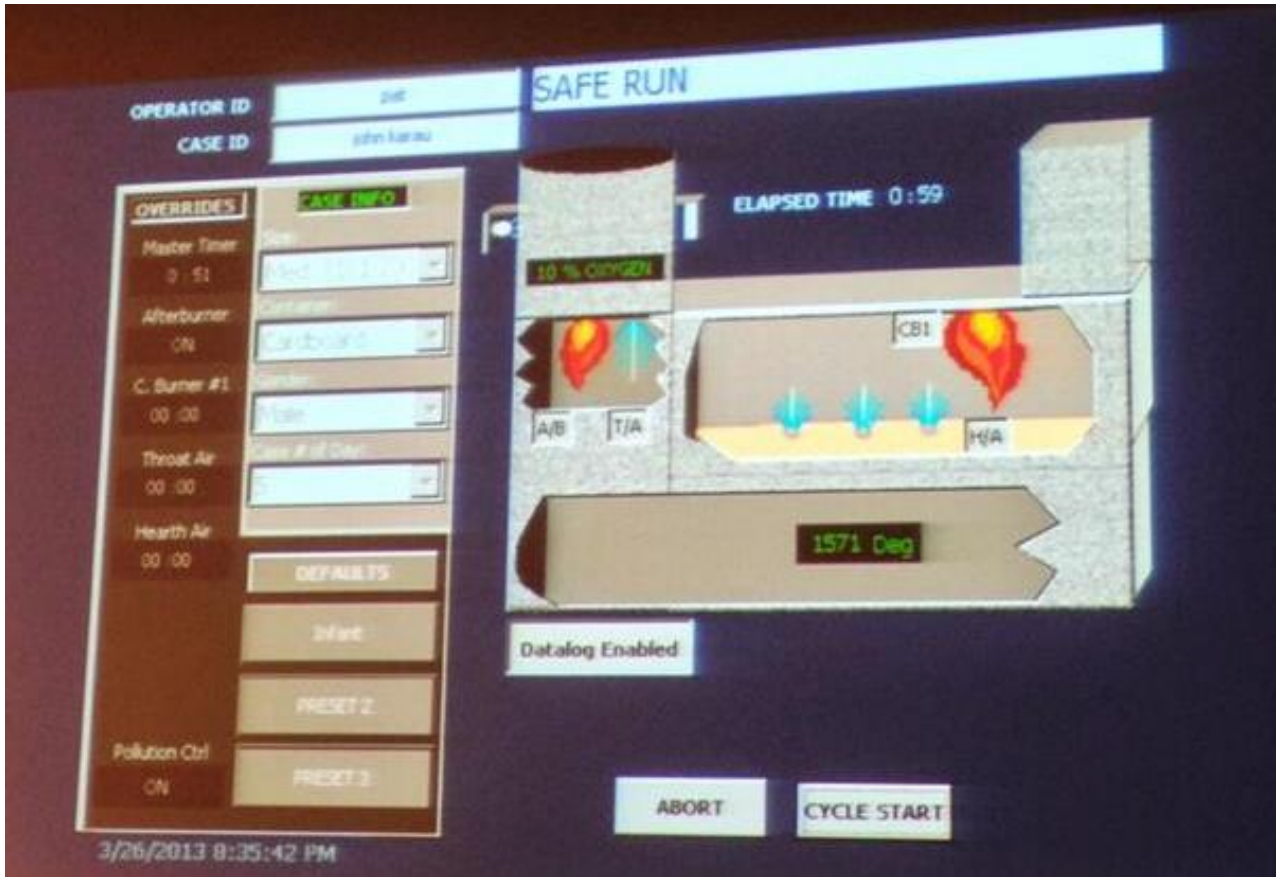
- All kinds of connected devices
  - PLCs
  - Webcams
  - Smart-things (fridge, TV, ...)
- Things you can't even imagine...
- Example ICS report : https://www.shodan.io/report/l7VjfVKc

ALTERNATIVES?

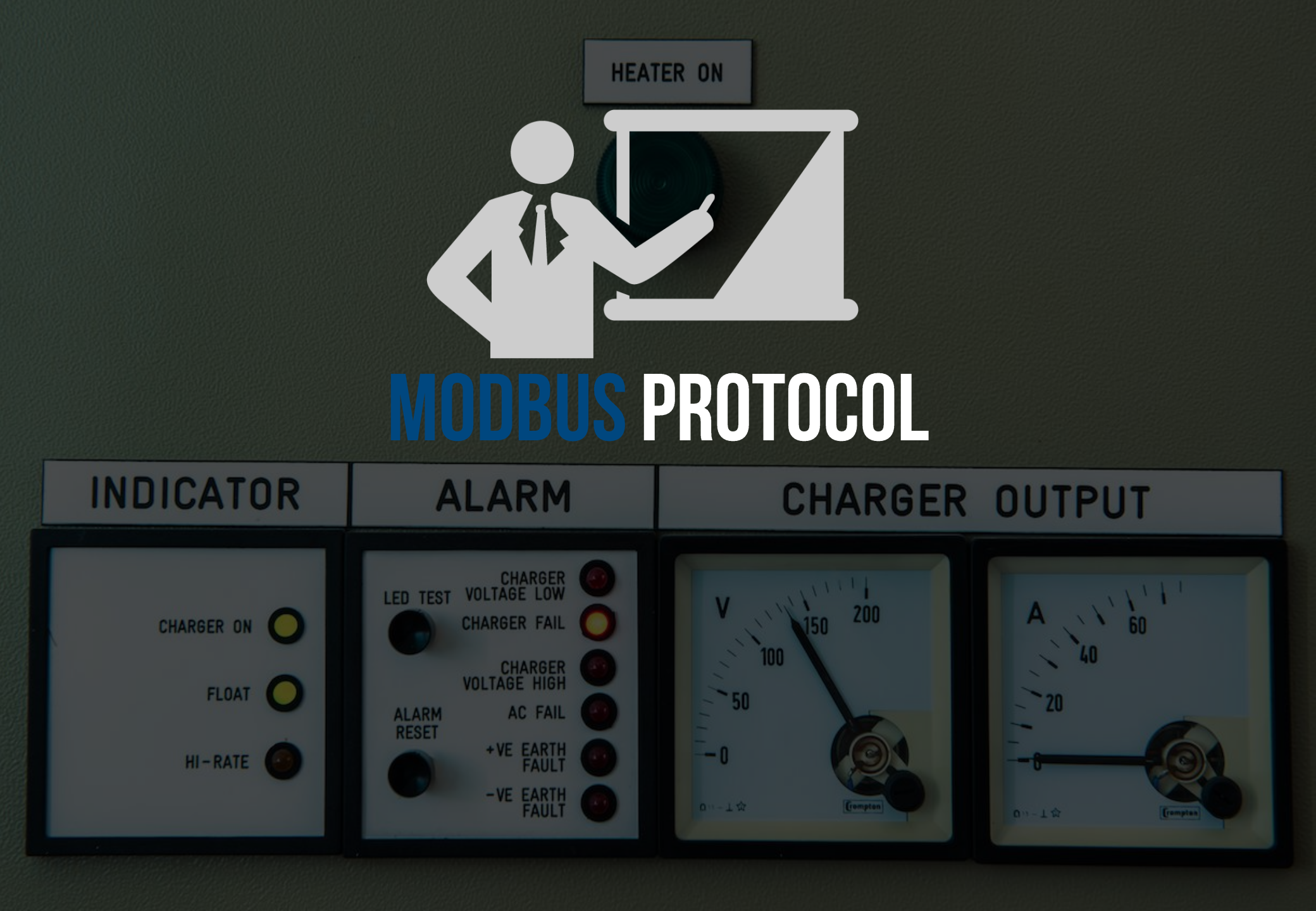
- Scan the Internet yourself (Zmap, Massscan)
- Other online services/surveys

FUNNY THINGS YOU CAN FIND ON TEH INTERWEBS

It's not just webcams.



THIS IS A CREMATORIUM.
ON THE INTERNET.


HEATER ON
MODBUS PROTOCOL
INDICATOR
ALARM
CHARGER OUTPUT
CHARGER ON
FLOAT
HI-RATE
LED TEST
CHARGER VOLTAGE LOW
CHARGER FAIL
CHARGER VOLTAGE HIGH
ALARM RESET
AC FAIL
+VE EARTH FAULT
-VE EARTH FAULT
V
0
50
100
150
200
A
0
20
40
60

MODBUS PROTOCOL

- Serial communication protocol invented in 1979 by Schneider Electric
- Developed for industrial application
- Royalty-free
- Now one of the standards for industrial communications

HOW IT WORKS

- Master / Slave protocol
- Master must regularly poll the slaves to get information
- Modbus addresses are 8 bits long, so only 247 slaves per master
- There is no object description: a request returns a value, without any context or unit

SECURITY ANYONE?

- Clear-text
- No authentication

MODBUS PROTOCOL

- Modbus was originally made for serial communications
- However it is now often used over TCP

MODBUS/TCP FRAME FORMAT

Name	Length	Function
Transaction identifier	2	For synchronization between server & client
Protocol identifier	2	Zero for Modbus/TCP
Length field	2	Number of remaining bytes in this frame
Unit identifier	1	Slave address (255 if not used)
Function code	1	Function codes as in other variants
Data bytes or command	n	Data as response or commands

MODBUS PROTOCOL

- The most common Modbus functions allow to read and write data from/to a PLC
- Other functions, such as file read and diagnostics functions also exist
- Undocumented Modbus function codes can also be used to perform specific actions

COMMONLY USED MODBUS FUNCTION CODES

Function name	Function code
Read coils	1
Write single coil	5
Read holding registers	3
Write single register	6
Write multiple registers	16
Read/Write multiple registers	23

MODBUS PROTOCOL

ALL DOCUMENTED MODBUS FUNCTION CODES (FROM WIKIPEDIA)

http://en.wikipedia.org/wiki/Modbus

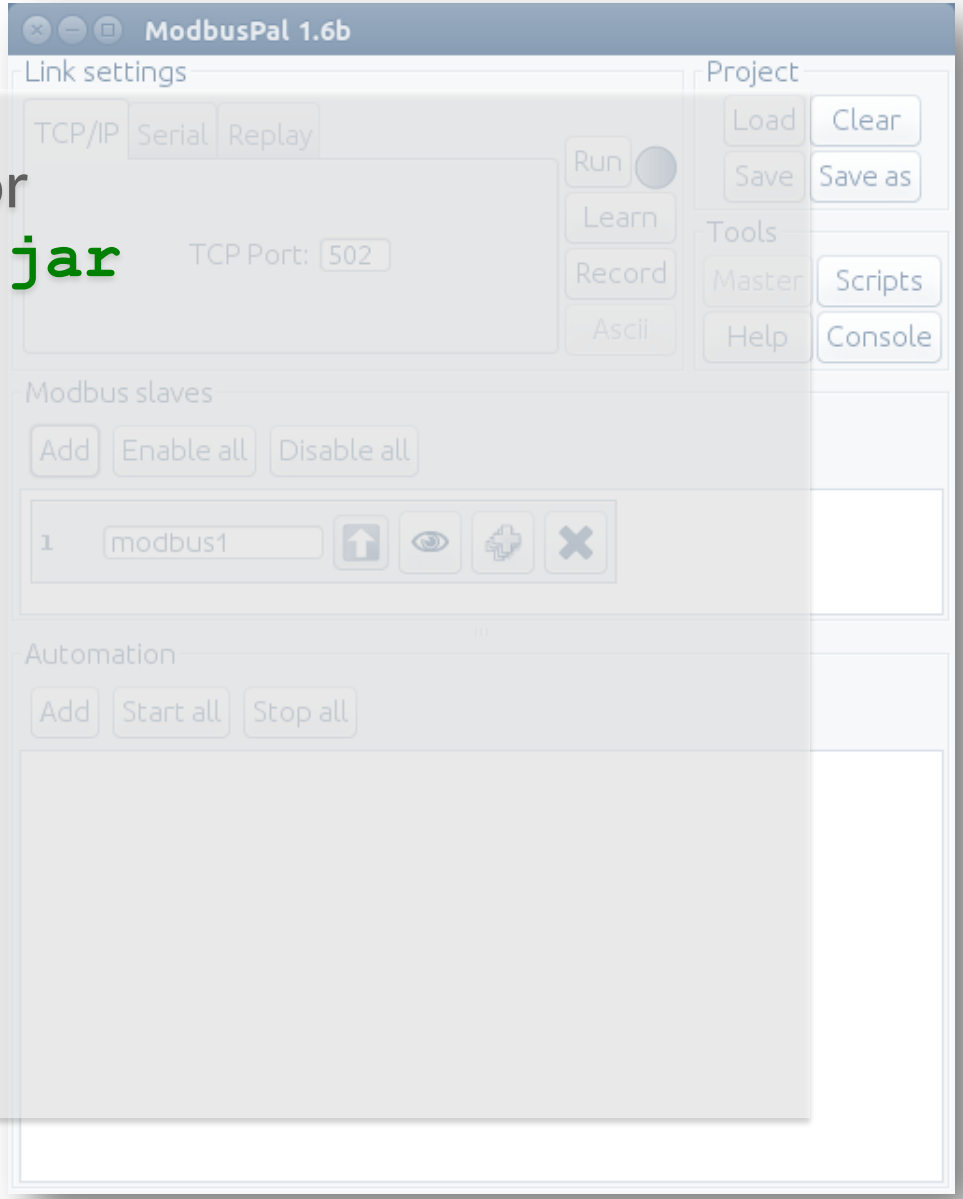
Function type			Function name	Function code
Data Access	Bit access	Physical Discrete Inputs	**Read Discrete Inputs**	2
		Internal Bits or Physical Coils	**Read Coils**	1
			Write Single Coil	5
			Write Multiple Coils	15
	16-bit access	Physical Input Registers	**Read Input Registers**	4
		Internal Registers or Physical Output Registers	**Read Holding Registers**	3
			Write Single Register	6
			Write Multiple Registers	16
			Read/Write Multiple Registers	23
			Mask Write Register	22
			Read FIFO Queue	24
	File Record Access		Read File Record	20
			Write File Record	21
Diagnostics			Read Exception Status	7
			Diagnostic	8
			Get Com Event Counter	11
			Get Com Event Log	12
			Report Slave ID	17
			Read Device Identification	43
Other			Encapsulated Interface Transport	43

LAB SESSION #1: ANALYZING A MODBUS COMMUNICATION WITH WIRESHARK

- Launch Wireshark
- Open "`modbus1.pcap`"
- Try to understand what's going on
- What's the value of register #123 at the end?

LAB SESSION #2: MODBUSPAL

- Modbuspal is a modbus simulator
  `$ > java -jar ModbusPal.jar`
- Add a modbus slave
- Set some register values
- Query it with:
  - MBTGET Perl script
  - Metasploit module
- Analyze traffic with Wireshark



LAB SESSION #2: MODBUSPAL + MBTGET

- Mbtget is a perl script to perform Modbus/tcp queries

```
$ > cd toolz
$ > ./mbtget -h
```

- Read requests
  - Coils (1 bit)

```
$ > ./mbtget -r1 -a 0 -n 8 127.0.0.1
```

  - Words (8 bits)

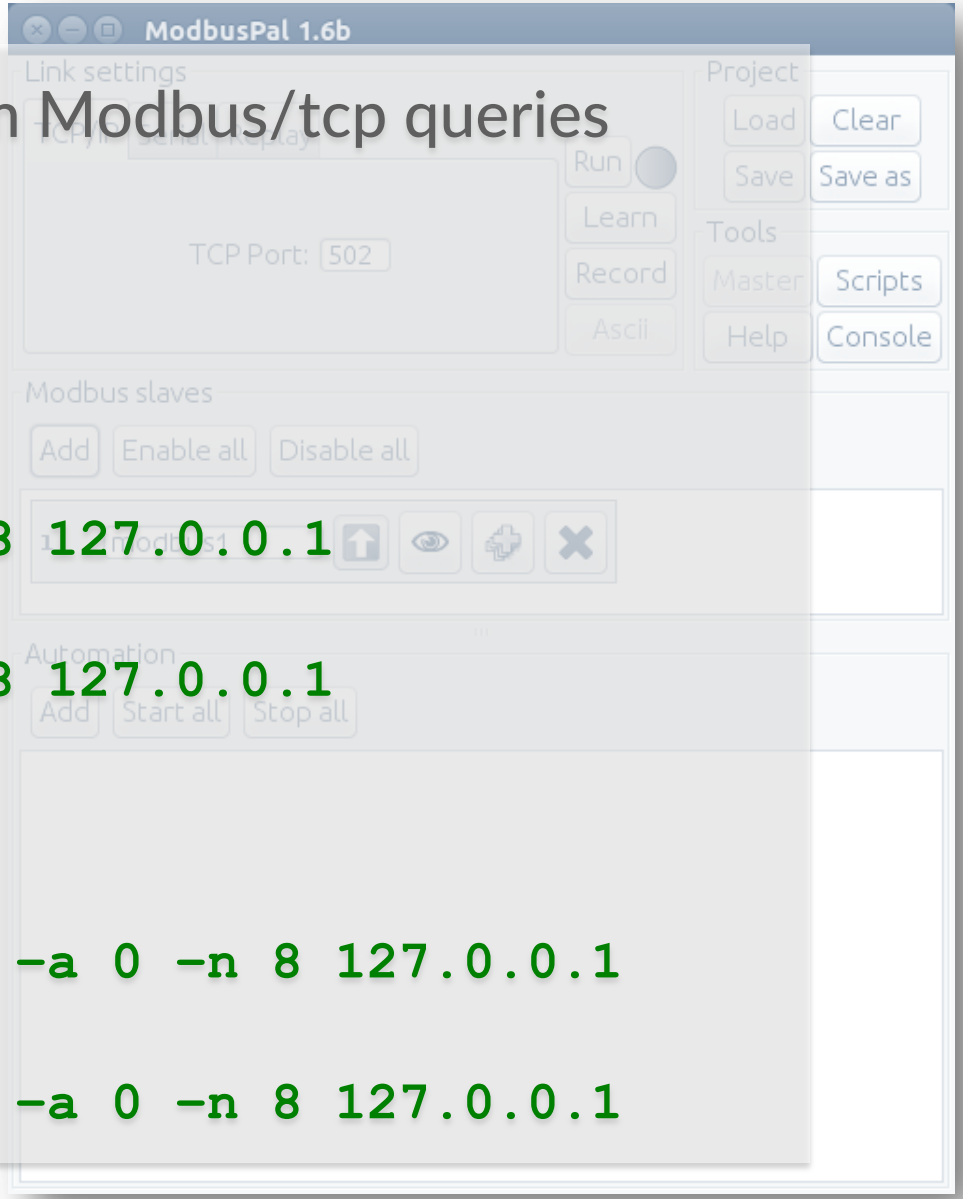
```
$ > ./mbtget -r3 -a 0 -n 8 127.0.0.1
```

- Write requests
  - Coils (1 bit)

```
$ > ./mbtget -w3 #{VALUE} -a 0 -n 8 127.0.0.1
```

  - Words (8 bits)

```
$ > ./mbtget -w6 #{VALUE} -a 0 -n 8 127.0.0.1
```



LAB SESSION #2: MODBUSPAL + METASPLOIT

- A simple modbus client that I developed
- Can perform read and write operations on coils and registers
- Included in msf's trunk so you already have it ☺

- Launch msf console

```
$ > msfconsole
msf > use auxiliary/scanner/scada/modbusclient
msf auxiliary(modbusclient) > info
```

- Play!

```
msf auxiliary(modbusclient) > set ACTION
```


WARNING
The following show features stunts
performed either by professionals or
under supervision of professionals.
performed on this show.
ATTACKING PLCS
NEVER DO THIS
ON LIVE PRODUCTION SYSTEMS

LAB SESSION #3 : RECONNAISSANCE

- Objective : Identify all exposed services on a device or a range of devices
- Often the first step in a pentest

- We will use two tools
  - Nmap: The world's finest port scanner
  - PLCSCAN: A reconnaissance tool dedicated to PLCs

- PLCs IP addresses
  - 192.168.0.50: Siemens S7-1200
  - 192.168.0.5: Schneider m340

LAB SESSION #3 : RECONNAISSANCE (NMAP)

- The de-facto tool for port scanning
- Can be really dangerous on ICS

- Two stories from NIST SP800-82
  - *A ping sweep broke for over 50 000$ in product at a semi-conductor factory*
  - *The blocking of gas distribution for several hours after a pentester went slightly off-perimeter during an assessment for a gas company*

- Nmap useful setup for ICS scanning
  - Reduce scanning speed! Use « `--scan-delay=1` » to scan one port at a time
  - Perform a TCP scan instead of a SYN scan
  - Do not perform UDP scan
  - Do not use fingerprinting functions, and manually select scripts (do not use "`-sC`")

LAB SESSION #3 : RECONNAISSANCE (PLCSCAN)

Siemens PLC

```
127.0.0.1:102 S7comm (src_tsap=0x100, dst_tsap=0x102)
  Module                    : 6ES7 151-8AB01-0AB0  v.0.2        (36455337203135312d38414230312d304142302000c000020001)
  Basic Hardware            : 6ES7 151-8AB01-0AB0  v.0.2        (36455337203135312d38414230312d304142302000c000020001)
  Basic Firmware            :                      v.3.2.6      (202020202020202020202020202020202020202000c056030206)
  Unknown (129)             : [illegible]                       (2020202020202020202020202020202020000041200909)
  Name of the PLC           : SIMATIC 300(xxxxxxxxx)            (53494d41544943203330302800000000000000000029000000000000000000)
  Name of the module        : IM151-8 PN/DP CPU                 (494d3135312d3820504e2f44502043505500000000000000000000000000)
  Plant identification      :                                   (202020202020202020202020202020202020202020202020202020202020)
  Copyright                 : Original Siemens Equipment        (4f726967696e616c205369656d656e73204571756970656e74000000000000)
  Serial number of module   : S C-BOUVxxxxxxxx                  (5320432d424f5556xxxxxxxxxx000000000000000000000000000000000000)
  Module type name          : IM151-8 PN/DP CPU                 (494d3135312d3820504e2f44502043505500000000000000000000000000)
```

Modbus device

```
127.0.0.1:502 Modbus/TCP
  Unit ID: 0
    Response error: ILLEGAL FUNCTION
    Device info error: ILLEGAL FUNCTION
  Unit ID: 255
    Response error: GATEWAY TARGET DEVICE FAILED TO RESPOND
    Device: Lantronix [illegible]
```

- https://code.google.com/p/plcscan/ by SCADAStrangeLove (http://scadastrangelove.org/)
- Scans for ports `102` (Siemens) and `502` (Modbus) and tries to pull information about the PLC (modules, firmware version,…)
- Not exhaustive since not all PLCs use Modbus or are Siemens

LAB SESSION #4 : ATTACKING STANDARD SERVICES

- Most PLCs have standard interfaces, such as HTTP and FTP
- Lets' say security was not the first thing in mind when introducing these features …

- Schneider M340
  - Connect to the webserver
  - Default password
  - Hardcoded password ?
  - Take a look at Java applets !

LAB SESSION #5 : ATTACKING ICS PROTOCOLS

- Modbus
  - Scan for registry values using `mbtget`
  - Python / Ruby / Perl / PHP, your call !

- Unauthenticated actions

  - STOP/RUN
    `msf > use auxiliary/admin/scada/modicon_command`

  - Logic download/upload
    `msf > use auxiliary/admin/scada/modicon_stux_transfer`

Reading program instruction

little endian counter

Modbus Function Code

WHAT CAN WE DO ABOUT IT ?

It's difficult, but not all hope is lost.

NETWORK SEGMENTATION

- Do not expose your ICS on the Internet
- Do not expose all of your ICS on your internal network
- Use DMZ / Data diodes to export data from ICS to corporate network

PATCH WHEN YOU CAN

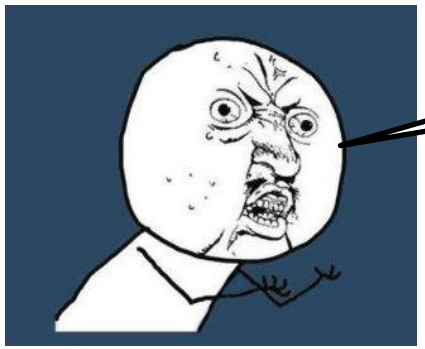
- Patching once a year during plant maintenance is better than doing nothing

APPLY CORPORATE BEST PRACTICES

- Change default passwords
- Disable unused services

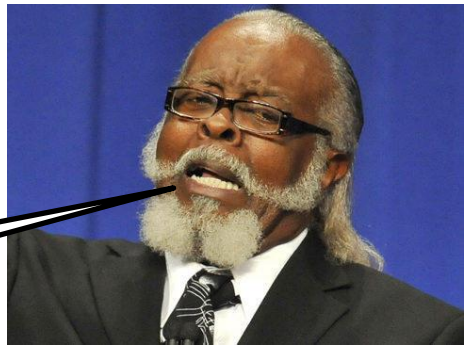
SECURITY SUPERVISION

- IPS have signatures for ICS
- Create your own signatures, it is not that difficult



Y U NO SECURE ICS ?

THE COST IS TOO DAMN HIGH !



The power of simplicity

«Ce qui est simple est fort»

www.solucom.fr

Contact

Arnaud SOULLIE

Senior consultant

arnaud.soullie[AT]solucom.fr