GreHack

IOActive™

# GREHACK
# VULNERABILITY INHERITANCE IN PROGRAMMABLE LOGIC CONTROLLERS

**NOVEMBER 2013**

## Using Our Past to Secure Your Future

2013-11-15

# Agenda (it's traditional)

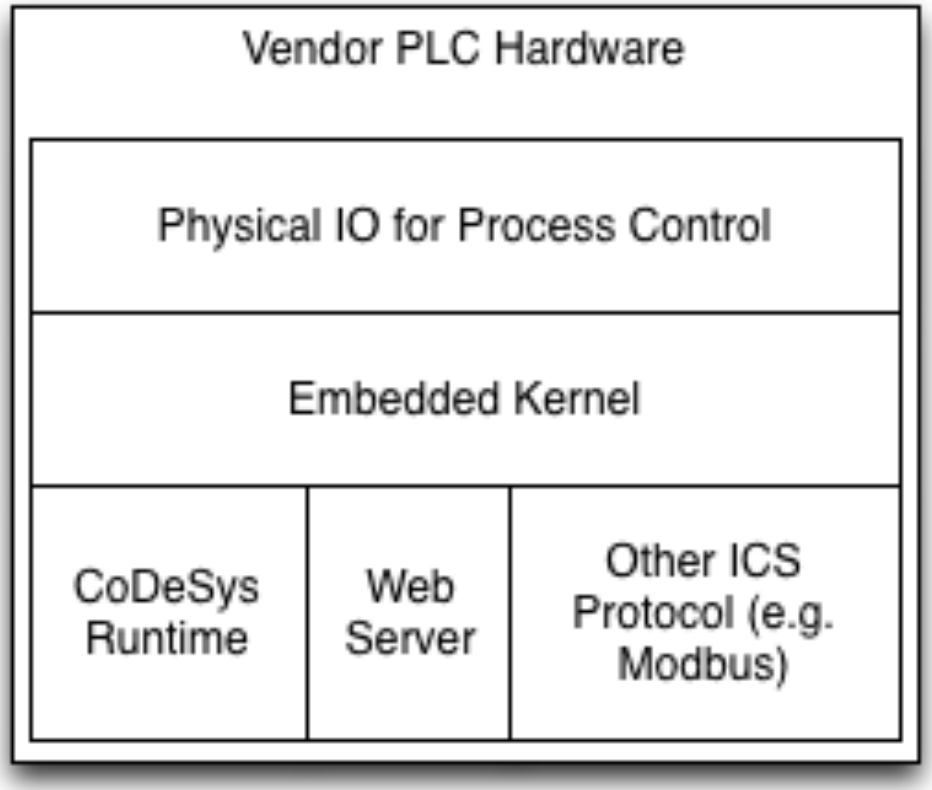
GreHack

- Introductions
- Very Light intro to PLCs
- Codesys runtime in context
- Codesys services on the PLC
- Vulnerability….gets inherited all the way down the supply chain
- Vendor "Response"
- Scan Methodology
- Open Port Results
- Actually Vulnerable Services
- Random Image of Darth Vader On a Unicorn
- Analysis
- Metrics (not just for ICS?)
- Conclusions

# Hello Automation World

- Programmable Logic Controllers (PLCs) are computers too!
- Developed nearly 40 years ago, where is next gen PLC?
- They're cheap computers we use in the field where it's dull, dirty, or dangerous.
- IEC 61131-3 is the 3rd part of an 8 part standard
- Commonly called "ladder logic"
- Basically allows Electrical Engineers to program
- The rest of the standard is other methods of programming
- This is how PLCs automate things
- So an engineer writes a ladder logic program
- Connects to a PLC from an Engineering Workstation (EWS)
- Uploads ladder logic
- PLC monitors inputs (sensor data) and alters outputs (control signal)
- We'll talk about Codesys runtime for the rest of this presentation
- It is middle ware for PLCs and EWSs

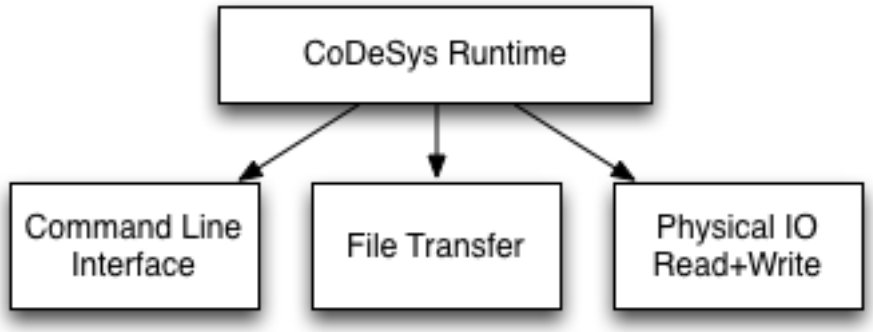
# Codesys in context




- Runs as root || admin
- PLCs are single user environments
- EWS might not have to be admin, but developers always are
- $otherconference referee suggested this run on PLCs with lower level of privilege -> non-issue

OK, what does this runtime do?

# Codesys services on the PLC




**Officially supports:**

- Embedded Windows CE
- vxWorks
- Linux

**Wide variety of hardware supported:**

- Embedded Intel x86
- Power PC
- m68k CPUs
- & many more including a “soft plc” to run on desktops
- Even one entire line of microcontrollers specifically for this runtime!

Given this diversity of hardware & OS, how can we understand the scope of this?

The hardest part of exploiting SCADA devices is getting your hands on them.

# Vulnerability Inheritance right through the supply chain

GreHack

- Suppose you have designed and hardened a PLC
- But you deem it cheaper to use a Third Party Runtime system
- Which then adds an authenticated shell
- Oops, the shell has an auth-bypass (Hat-tip Reid Wightman)
- Shouldn't your QA catch that if theirs hasn't?
- Or at least your customers?
- Or perhaps you'd do other tests before deploying on the internet

For scope analysis this raised problems for us.

Traditionally, Reid and I have gained a sense of the scale of vulnerability exposure to the internet by doing banner analysis.

Realizing we had no way of discovering 200+ banners, Reid decided to fingerprint the service itself. The NMAP script for vulnerable service is in the paper.

**…But first, how did the vendor respond to the vulnerability?**

# Best Vendor Response Ever!



You are here: CODESYS - industrial IEC 61131-3 PLC programming » News & Events » Press Releases

## Security Vulnerability in CODESYS V2.3 Runtime System

30. October 2012

Kempten, October 2012: Password protection bypass for CODESYS controllers

A security vulnerability which affects the CODESYS V2.3 Runtime System is currently being discussed on several different internet platforms: The password protection of a publicly accessible CODESYS controller can be bypassed with the help of an external tool. A password protected controller can then be accessed just like any unprotected PLC and it is possible to execute commands with the controller shell or load applications.

Of course, we take this issue very seriously. A fix version which resolves the reported vulnerability is now available for download for our direct OEM customers.

In general, we do not offer any standard tools in CODESYS which are to protect the controller from a serious cyber attack. Should the offered password functionality suggest such a protection, this was definitely not our intention. The implementation of standard security mechanisms (firewall, VPN access) is an absolute must when operating a PLC runtime system on a controller accessible through the internet.

# Scanning 0.0.0.0/0 Methodology

GreHack

1. Scan /8s with unicornscan at about 750 PPS
    1. Do this for both ports 1200 and 2455
    2. Two machines from $VPShosting
    3. Host web page on scanning machines with explanation and contact
    4. If people send cease and desist, remove them from target list
2. Scan anything with open ports using NMAP Vuln script
    1. Analyse results to strip out actually vulnerable machines
    2. Do post analysis to determine ASN, DNS, rDNS, Registrar, ETC
    3. Send offer of data on vulnerable systems to 30 countries
    4. # collaborated with us, to contact system owners

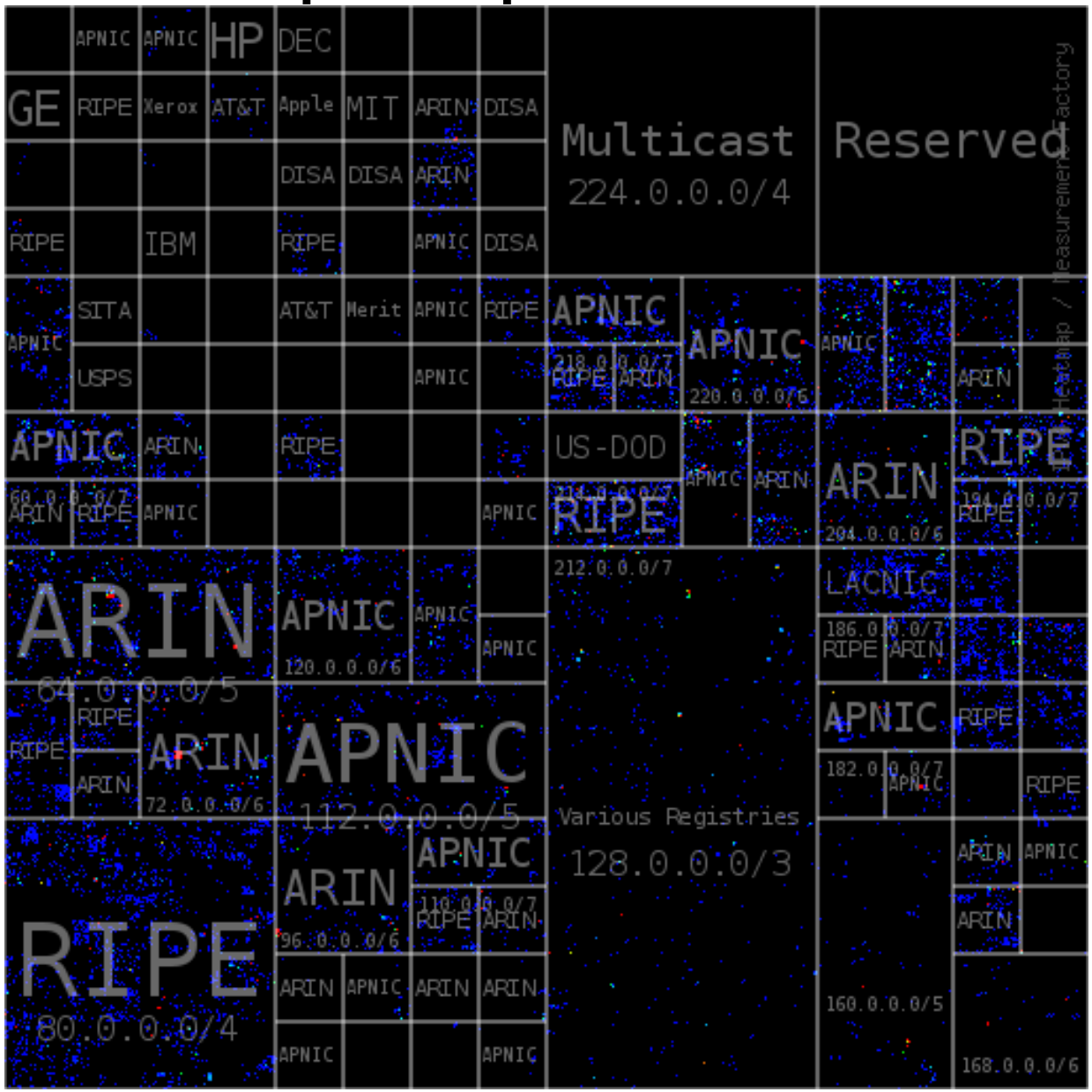
You might be tempted to ask why we do this.

Primarily, because we live in small towns and there isn't much to do in the evenings. However, it's also to get a sense of scale for ICS security problems, to make friends in IR, to avoid being biased towards one country, and finally to motivate customers to push back on security with ICS companies.

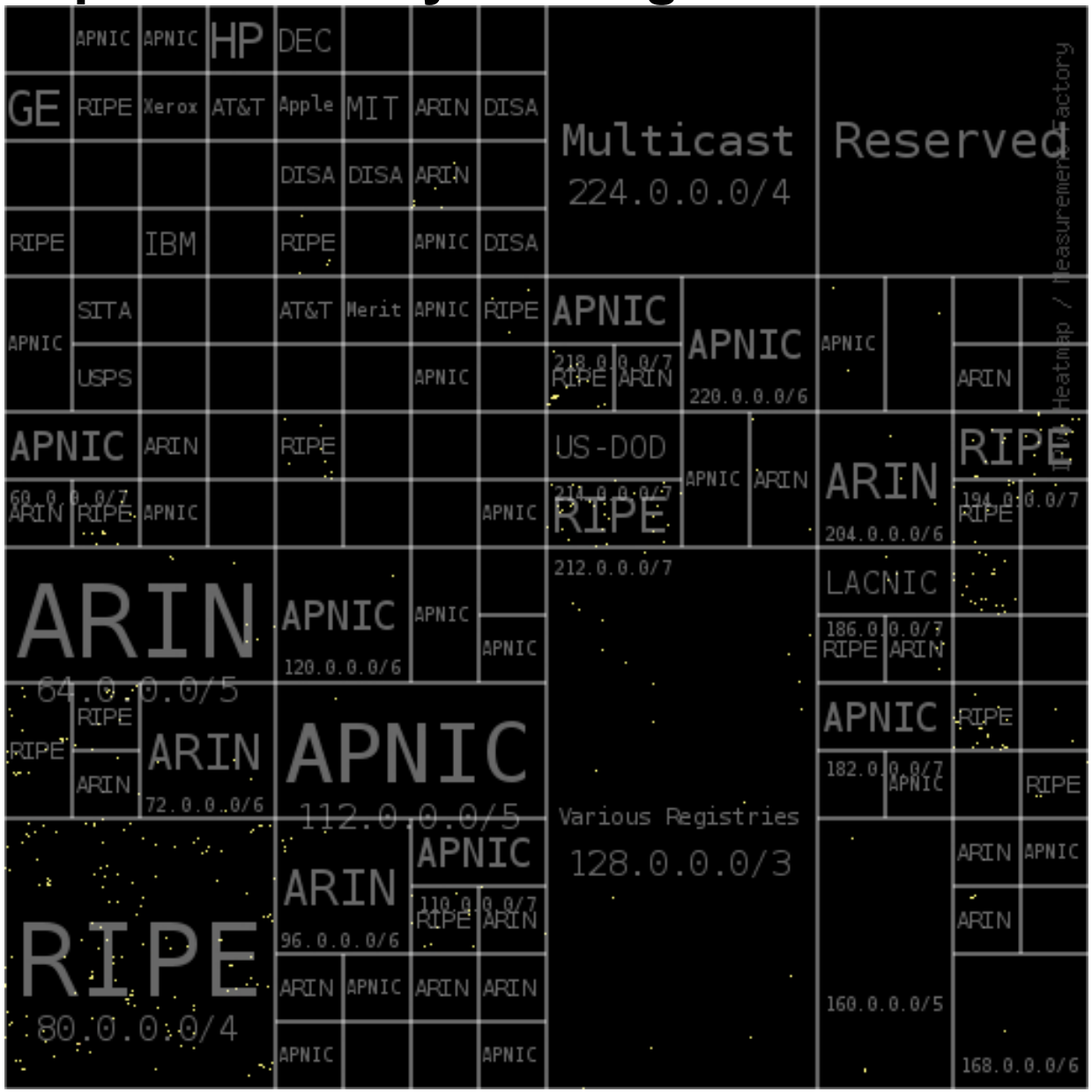
By scanning and informing, we skip the vendor "PR" problem.

We are an independent voice.

# Initial Results: Open on ports 2455 or 1200



# Second pass: Actually running vulnerable codesys



# That's how we rode a Unicorn and saved some SCADAz!

GreHack

But what did we learn in a wider sense?

# SCADA-SEC is first world problems

GreHack

**Table 1.** Ten Autonomous Systems containing the largest number of vulnerable PLCs

| PLCs Found | ASN | CC | Registrar | AS Name |
|---|---|---|---|---|
| 9 | 6327 | CA | arin | Shaw Communications Inc. |
| 9 | 6830 | AT | ripencc | Liberty Global Operations B.V. |
| 12 | 5610 | CZ | ripencc | Telefonica Czech Republic, a.s. |
| 21 | 28929 | IT | ripencc | ASDASD-AS ASDASD srl |
| 25 | 12605 | AT | ripencc | LIWEST Kabelmedien GmbH |
| 28 | 3269 | IT | ripencc | Telecom Italia S.p.a. |
| 28 | 3303 | CH | ripencc | Swisscom (Switzerland) Ltd |
| 43 | 1136 | EU | ripencc | KPN Internet Solutions[2] |
| 43 | 286 | EU | ripencc | KPN Internet Backbone |
| 44 | 3320 | DE | ripencc | Deutsche Telekom AG |

**Table 2.** Ten Countries containing the largest number of vulnerable PLCs

| PLCs Found | Country Code |
|---|---|
| 21 | CA |
| 21 | ES |
| 29 | CZ |
| 33 | AT |
| 33 | US |
| 38 | CH |
| 60 | PL |
| 64 | NL |
| 80 | DE |
| 81 | IT |

**Table 3.** Number of Vunerable Devices per RIR

| PLCs Found | Registry |
|---|---|
| 0 | afrnic |
| 4 | apnic |
| 6 | lacnic |
| 54 | arin |
| 526 | ripencc |

# Translation metrics: technical -> economic & policy

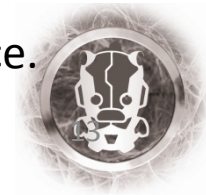
GreHack

2011 using Shodan: similar results were $1.56 per vulnerable system/device.
Using Unicorn and NMAP, we found vulnerable Codesys for $0.86 per device.

1. This metric is methodology and technology independent.
2. As costs for parallelisation fall this is incorporated into the metric.
3. As newer, faster scanners (such as ZMAP) are developed this is also included in the metric.
4. The density of vulnerability across a network space is factored into the metric.
5. Partial scans can still be used for metrics.
6. We understand the cost to attackers of finding opportunistic targets.
7. We understand the low cost to this methodology of defending.
8. We understand the change over time in the lifecycle of exposure and vulnerability.
9. It naturally translates a technical problem into an economic one ready for debate and policy discussion.

Testing these assumptions then:

Using ZMAP we could have done the same work for $0.11 per vulnerable device.



# Conclusions:
# For 11 cents a day you can sponsor a vulnerable SCADA device!


- This vulnerability was missed by the QA of Codesys runtime
- The company freely admits it is not in the security game
- It was missed by integrators of Codesys runtime
- It was missed when deploying systems openly on the internet

We provided an NMAP script to help others determine vulnerable products
We scanned over the winter of 02012/02013 to get a sense of scale

**~600** (Lower than we thought!)

Finally, we propose a simple measure of vulnerability exposure
Which helps understand exposure over time

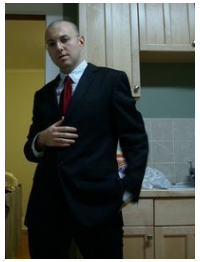
In short:

What we've done isn't big, and it isn't clever.

It is effective, though.

# Thank you for listening and inviting us to France!

GreHack




## Reid Wightman

Senior Security Consultant, ICS & Smart Grid

Reid[dot]Wightman[at]IOActive.co.uk

@ReverseICS



## Éireann Leverett

Senior Security Researcher, ICS & Smart Grid

Eireann[dot]Leverett[at]IOActive.co.uk

@blackswanburst