Standards Based Measurable Security For Embedded Devices

Brice Copy

ICALEPCS 09

11 October 2009

Plan

- Project background
- Test bench objectives
- Implementation
- Investigation results
- Achievements
- Perspectives

Project background

- Based upon TOCSSiC, study the robustness of PLCs
- CERN Openlab backed project
- With SIEMENS funding
- CERN specific aspects
  - Strong demand for RBAC type security
  - Better built-in security mechanisms
  - Wide variety of risk assessments

Testbench objectives

- Investigate cyber security standards relevant to PLC equipment operation.
- Establish a working environment tailored for ICS to enable the discovery of new security vulnerabilities.
- Assess the robustness of SIEMENS Programmable Logic Controller (PLC) products.
- Perform automated security assessments of industrial control equipment.
- Determining which are the key aspects of cyber security in the CERN environment.

Cyber Security Standards

- ISO 27000, NERC CIP, ISA-99, IEC62xxx
- Slowly evolving towards ICS relevant standards
- ISA-99 relevant but still draft
- Vendors : Mexican standoff situation
- Everybody agrees it is better than legislation

Finding new vulnerabilities...

Directly related to quality processes

- First, define a method to test
- Second, define a method to reproduce results
- Third, define a method to fix and verify

Meanwhile, keep abreast of emerging threats and vulnerabilities

...In the comfort of your own lab

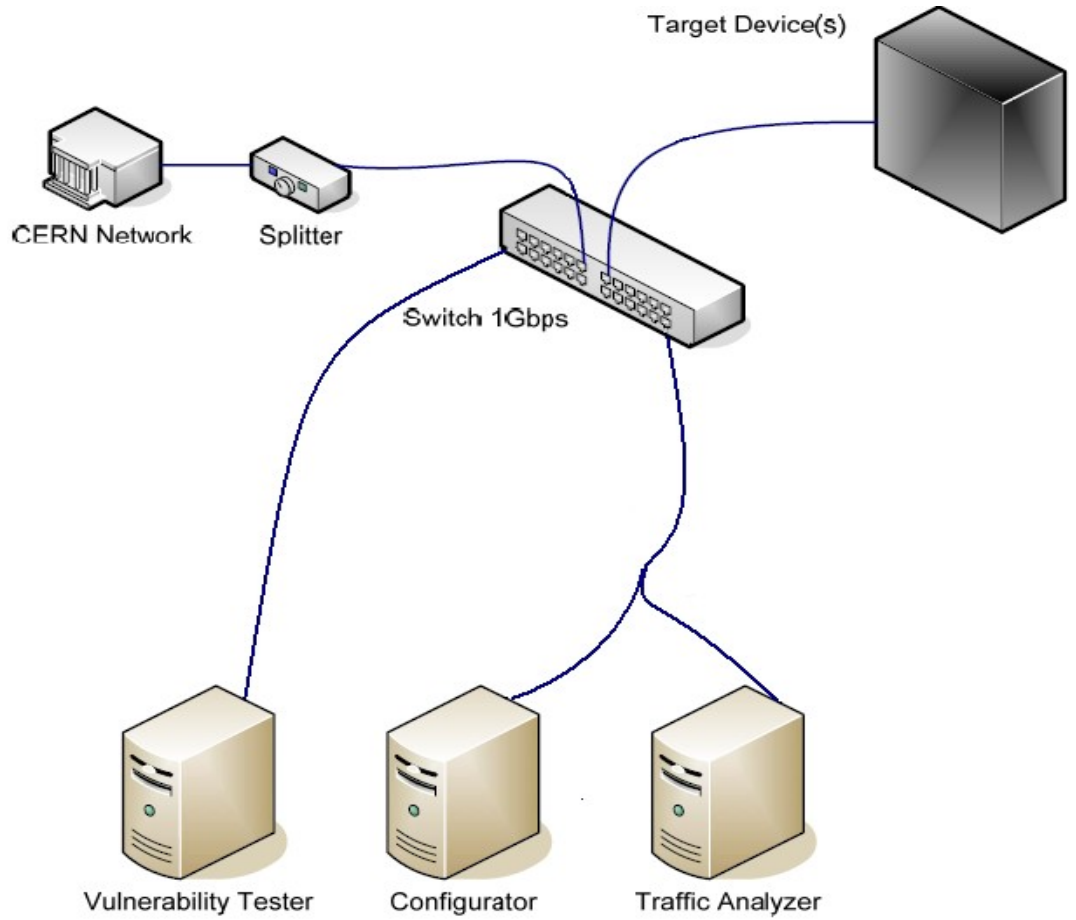
An environment that can play many roles...

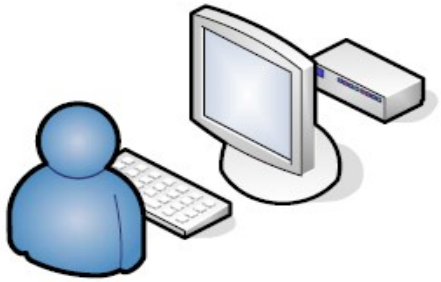
- ...Acts as a first class citizen in information exchanges

An environment that communicates...

- ... by accepting inputs from other tools
- ...and producing outputs for other consumers

Testbench in theory





And in practice ?

- A plug-in based environment OpenVas for general purpose testing
- A better set of PLC monitoring tools
- A protocol fuzzer to
  - convert grammars into vulnerability scanners
  - convert network trafic captures into vulnerability descriptions
- A way to feed vulnerabilities to our favourite PLC vendor (and sponsor)

Testbench in practice

Testbench in practice

Achievements and findings

- Newer PLC generations are better in many aspects...
- ...and surprisingly exposed in others
- Protocol fuzzing presents an unforeseen potential
- Communicating results to a third-party and making them reproduceable is still too much work

Perspectives

- Improve techniques to share results and analyse them
- Start integrating our tools more closely
- Adopt a cut down standard until full blown ones become ready