An Open Framework for Deploying Experimental SCADA Testbed Networks

Peter Maynard, Kieran McLaughlin, and Sakir Sezer

August, 2018

Queen’s University Belfast « CSIT
Outline

▶ Background
▶ High-Level Overview of Framework
▶ Tooling
▶ Ongoing/Future Work
About Myself

▶ Research Assistant, at Queen’s University Belfast, CSIT
  ▶ PhD 4 years ICS Network-IDS
▶ Research Engineer, at Southampton University, UK
  ▶ 5G Networks
▶ Computer Science BSc, at Aberystwyth University, UK
Framework for creating virtualised SCADA networks
Developed for packet generation for NIDS
Open Source (GPLv3)
Related Work

- IDS networking datasets (e.g. KDD’99)
- Lack of reproducible ICS/SCADA testbeds
- Lack of IEC 60870-5-104 protocol support
Use Cases TestBed

- Packet Generation
- Attack Simulations
- Agent Benchmarking
- Extending Limited Hardware
Requirements of a TestBed

- Reproducible
- Scalability
- Domain Fidelity
- Process Simulation
- Network Emulation
- Physical Network
- Physical Devices
- Multi-Protocol
High-Level Overview of Framework

a) Compilation Stage
1) CreateBaseImage()
2) CompileSource()
3.1) ConfigureBaseImage()
3.2) LoadConfig()
3.3) InstallPackages()
Provision
Configuration Profile

b) Orchestration Stage
Deploy
4) BootUpVirtualMachine()
Provision
5.1) AssignIP()
5.2) LoadConfig()
5.3) StartServices()
Start
Configure
Operational Profile

VM
RTU/HMI/...

C) Operation Stage
Control VM
SSH/Console/Telnet
Manage
Shutdown Testbed

Monitor()
<table>
<thead>
<tr>
<th>Host</th>
<th>IP</th>
<th>IEC104</th>
<th>OPC-UA</th>
<th>Other</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>HMI</td>
<td>10.50.50.150</td>
<td>26,158</td>
<td>0</td>
<td>17,688</td>
<td>43,846</td>
</tr>
<tr>
<td>Historian</td>
<td>10.50.50.151</td>
<td>0</td>
<td>14,695</td>
<td>14,927</td>
<td>29,622</td>
</tr>
<tr>
<td>RTU-1</td>
<td>10.50.50.101</td>
<td>3,592</td>
<td>2,940</td>
<td>5,543</td>
<td>12,075</td>
</tr>
<tr>
<td>RTU-2</td>
<td>10.50.50.102</td>
<td>3,665</td>
<td>2,941</td>
<td>5,876</td>
<td>12,482</td>
</tr>
<tr>
<td>RTU-3</td>
<td>10.50.50.103</td>
<td>3,668</td>
<td>2,940</td>
<td>5,793</td>
<td>12,404</td>
</tr>
<tr>
<td>RTU-4</td>
<td>10.50.50.104</td>
<td>3,690</td>
<td>2,940</td>
<td>5,771</td>
<td>12,404</td>
</tr>
<tr>
<td>RTU-5</td>
<td>10.50.50.105</td>
<td>3,576</td>
<td>930</td>
<td>7,933</td>
<td>12,442</td>
</tr>
<tr>
<td>MITM</td>
<td>10.50.50.99</td>
<td>2,390</td>
<td>0</td>
<td>3,449</td>
<td>5,839</td>
</tr>
<tr>
<td>SCAN</td>
<td>10.50.50.3</td>
<td>15</td>
<td>0</td>
<td>28,351</td>
<td>28,366</td>
</tr>
</tbody>
</table>

- Network Reconnaissance
- IEC104 Command Injection
- 192K Packet Dataset
Ongoing Work

- Integration Process Simulators
- Implementing additional operation/configuration profiles
- Simplify deployment
- Expand documentation
Future Work

▶ Testbed Federation
▶ Auto configuration of networking equipment
▶ Amazon Web Services (AWS) and Google Compute Engine
▶ Experimentation with alternative network paradigms
www: petermaynard.co.uk

twitter: @pgmaynad

e-mail: p.maynard@qub.ac.uk

git: https://github.com/PMaynard/ICS-TestBed-Framework

dataset: https://dx.doi.org/10.6084/m9.figshare.6133457.v1