Implementing Attacks for Modbus/TCP Protocol in a Real-Time Cyber Physical System Test Bed

Bo Chen¹, Nishant Pattanaik², Dr. Ana Goulart³, Dr. Karen L. Butler-Purry⁴, Dr. Deepa Kundur⁵

¹: Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX, USA
²: Department of Computer Science and Engineering, Texas A&M University, College Station, TX, USA
³: Department of Engineering Technology and Industrial Distribution, Texas A&M University, College Station, TX, USA
⁴: Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON, Canada

Introduction

To understand security vulnerabilities of communication protocols used in power systems, a real-time cyber-physical test bed was developed. It integrates a real-time power system simulator and a communication system simulator to study the cyber and physical system vulnerabilities in smart power grids. The power system is simulated using the Real-Time Digital Simulator (RTDS), with LabVIEW and PXI modules that simulate the supervisory control and data acquisition (SCADA) system and intelligent electronic devices (IEDs). The communication system simulation is implemented using OPNET’s System-in-the-Loop (SITL) simulator and open source Linux tools and servers. Results of cyber-attacks on the Modbus/TCP protocol are presented.

Background and Motivation

Smart grids are vulnerable to cybersecurity events
- Innovative smart grid technologies involve bidirectional communication
- Numerous access points (e.g., WAMS, AMI, internet, public telecommunications network)
- Lack of cybersecurity awareness in most early SCADA system designs (e.g., off-the-shelf software, operating systems, protocols)

Need for a cyber-physical testbed
- Create a cyber-physical environment
- Understand the impact of cybersecurity events
- Allow researchers to perform studies on defending and mitigating cybersecurity events

Capabilities and Applications

Application
- Test and evaluation of cyber attacks
- Impact of cyber attacks on systems
- Vulnerability evaluation
- Mitigation evaluation
- Training and education

Power System Automation Lab
Department of Electrical and Computer Engineering
Texas A&M University
College Station, TX 77843-3128

Hardware and Software

RTDS
- Power system and control simulation
  - 50 microsecond time step
- Data acquisition and communication
  - GTAD0, GTDI0: Analogue and digital ports
  - GTNET (IEC 61850 Sampled Values, GSE, etc.)
- Hardware-In-The-Loop: Connect to controller, protective relays, amplifiers, etc.
- RSCAD
  - User-friendly interface to RTDS hardware
  - Modeling libraries: Power systems, control systems, protection and automation, power electronics, etc.
- PSSE and MATLAB/Simulink integration

NI LabVIEW and PXI
- Interface with RTDS through analogue and digital I/O
- Controller/Protection implementation
- Industrial Communications Protocols (DNP3, Modbus TCP, etc.)

OPNET
- Communication system simulation
- System-In-The-Loop (SITL)
  - Allow to connect to real world networks
  - Attack PC can connect to real and simulated node

Real World Devices
- Intelligent Electronic Devices (IEDs)
- Networking devices (switch, router, etc.)

Control Center Applications
- Customer-defined applications
  - Modeled in LabVIEW with MATLAB interface
- Real-Time applications modeled in ETAP

Attack PC
- Open source cyber attack software

Case Studies

Test System
- Transmission system
- 2 generators and 11 buses
- Controllers (governor, automatic voltage regulator (AVR, power system stabilizer (PSS))

Mitigation Data of Connections

<table>
<thead>
<tr>
<th>BRK</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gen1</td>
<td>100</td>
<td>110</td>
<td>120</td>
<td>130</td>
<td>140</td>
<td>150</td>
<td>160</td>
<td>170</td>
<td>180</td>
<td>190</td>
</tr>
<tr>
<td>Gen2</td>
<td>200</td>
<td>210</td>
<td>220</td>
<td>230</td>
<td>240</td>
<td>250</td>
<td>260</td>
<td>270</td>
<td>280</td>
<td>290</td>
</tr>
</tbody>
</table>

Networking Devices

<table>
<thead>
<tr>
<th>BRK1</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gen1</td>
<td>100</td>
<td>110</td>
<td>120</td>
<td>130</td>
<td>140</td>
<td>150</td>
<td>160</td>
<td>170</td>
<td>180</td>
<td>190</td>
</tr>
<tr>
<td>Gen2</td>
<td>200</td>
<td>210</td>
<td>220</td>
<td>230</td>
<td>240</td>
<td>250</td>
<td>260</td>
<td>270</td>
<td>280</td>
<td>290</td>
</tr>
</tbody>
</table>

TCP SYN Flood Attack
- TCP SYN flood attack can flood the Modbus Master using TCP three-way connection handshake mechanism
- TCP SYN flood attack floods the Modbus Master with TCP connection requests from potential Modbus clients with spoofed source IP addresses and random destination TCP ports
- Remotely control over BRK1 may be delayed by TCP SYN flood attack

Supported in part by NSF grants EECS-1028246 and EEC-1062603