On Design and Enhancement of Smart Grid Honeypot System for Practical Collection of Threat Intelligence

- Long preliminary work paper -

Daisuke Mashima, Derek Kok, Wei Lin

*Advanced Digital Sciences Center, Illinois at Singapore*

Muhammad Hazwan, Alvin Cheng

*Custodio Technologies Pte Ltd*

This material is based on research/work supported in part by the Singapore National Research Foundation and the Cybersecurity R&D Consortium Grant Office under Seed Grant Award No. CRDCG2018-501. This research is partly supported by the National Research Foundation, Singapore, Singapore University of Technology and Design under its National Satellite of Excellence in Design Science and Technology for Secure Critical Infrastructure Grant (NSoE_DeST-SCI2019-005).
Background and Motivation

- **Honeypot** is an effective tool to collect intelligence about attackers in the real world.
  - The collected intelligence helps us fine-tune cybersecurity measures (e.g., Firewall, IDS)

- Honeypot for smart grid systems is still in early stage
  - No honeypot emulating the whole architecture or its cyber-physical behaviours
  - No established methodology for evaluating “goodness” of honeypot
Approach

• Develop **prototype** of honeypot (or honeynet) that emulates typical smart grid system

• Conduct **penetration testing** to evaluate the honeypot system from the attackers perspective

• **Improve** the honeypot implementation based on the findings
Initial Honeypot Design and Implementation

• Designed based on infrastructure compliant to IEC 60870 and IEC 61850

• Example of a setup that researchers would start with
Evaluation from Attackers’ perspective

- **Penetration testing** by cybersecurity experts
- Scenario developed based on ICS-CERT and ICS Cyber Kill Chain
- Use widely-used tools, such as Nmap and Metasploit
Insights obtained from the experiments

• Presence of virtual machines hinted by open ports
  
  Close related ports after virtual machines are started.

• Lack of user accounts on Windows machines, which does not look like active, lively used systems
  
  Prepared user accounts with popular ID and weak password

• OS/device fingerprinting results that are different from typical smart grid devices (IEDs, substation gateways)
  
  Discussed next
Countering OS Fingerprinting against Smart Grid Devices

• Passive device
  • Only acts as a server (E.g. IEDs)
  • Run the same network services (HTTP, IEC 61850 MMS)
  • MAC address belonging to the same device vendor (e.g. Siemens)
  • Honeyd to fake OS fingerprint

• Active device
  • Acts as a server and client (E.g., GW, PLC)
  • Run the same network services (HTTP, IEC 60870-5-104, SSH)
  • MAC address belonging to the same device vendor (e.g. Wago)
  • Use VM running a Linux OS close to the real devices
    • To counter passive fingerprinting tools (e.g., P0f), Honeyd is not effective.
    • Devices of this category often run Linux
Enhancement of Logging for Data Collection

- **Transparent proxy (TP)** for secure logging of networking
  - Implemented as **bump-in-the-wire device** for network traffic monitoring
- **Application-level logging** at virtual IED, PLC, and substation gateway

---

### Table 3: Logging Available on Improved Honeypot

<table>
<thead>
<tr>
<th>Information</th>
<th>Location</th>
<th>Secure?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timestamp of event</td>
<td>Honeyd and SoftGrid</td>
<td>Yes</td>
</tr>
<tr>
<td>Source IP</td>
<td>Honeyd</td>
<td>Yes</td>
</tr>
<tr>
<td>Destination IP</td>
<td>Honeyd</td>
<td>Yes</td>
</tr>
<tr>
<td>IEC 61850 MMS Command</td>
<td>SoftGrid (IED)</td>
<td>Yes</td>
</tr>
<tr>
<td>IEC 104 Command</td>
<td>SoftGrid (Gateway)</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

SoftGrid: an open-source software-based substation testbed
OS Fingerprints of Passive Devices

- Significant improvement compared to initial IED using Mininet
- Values of SP, ISR, and SS vary.
- Only constant difference is IPL.
  - Although the specific IED model we studied returns 240, smart grid devices return 164.
  - Without the knowledge of the specific IED model, it is not feasible to tell if it is a fake device.
OS Fingerprints of Active Devices

• Difference in P0f fingerprints is seen in “mss*”, which varies depending on the network link.
Conclusions & Future Work

• Designed and implemented a honeypot that emulate comprehensive smart grid infrastructure

• Presented the evaluation and enhancement of honeypot through penetration testing by security experts

• The outcome is publicly available.

• Conduct further evaluation with more participants, e.g., hacking/capture-the-flag competitions

• Deploy the improved honeypot for real-world data collection

• Explore use of honeypot for education/training purposes
Thank you very much!

• Questions and Inquiries:
  • Email: daisuke.m@adsc-create.edu.sg

• Materials, Images, and Project Overview:
  • Web: https://www.illinois.adsc.com.sg/spotify/index.html