KYPO4INDUSTRY: A Testbed for Teaching Cybersecurity of Industrial Control Systems

Pavel Čeleda, Jan Vykopal, Valdemar Švábenský, Karel Slavíček
celeda@ics.muni.cz

Institute of Computer Science, Masaryk University

March 14, 2020 @ SIGCSE’20, Portland, Oregon, USA
**Industrial Control Systems (ICS)**

- **Provide** vital services – electricity, water treatment, transportation, …
- **Used to be isolated but became connected** with IT systems and even to the Internet.
- **This connection has reduced costs and enabled new services.**
- **However, ICS assets became vulnerable to new cyber threats.**
University Cybersecurity Courses

- **Fall short** in covering ICS security.
- Traditionally focus on exploiting and defending IT assets.
- If they feature a hands-on part, they use virtual labs or testbeds composed from standard IT components (desktops, servers, switches, and routers).
Goal of This Paper

- Share experience with the **design and acquisition of KYPO4INDUSTRY testbed** (K4I).
- Describe a **course syllabus** to deliver cybersecurity training in a simulated industrial environment to computer science students.
# KYPO4INDUSTRY Testbed – K4I

## Table 1

<table>
<thead>
<tr>
<th>Group of Students</th>
<th>ICS Hardware</th>
<th>Cloud Infrastructure</th>
</tr>
</thead>
</table>

## Table 6

<table>
<thead>
<tr>
<th>Group of Students</th>
<th>ICS Hardware</th>
</tr>
</thead>
</table>
Hardware Components

Actuator - Linear Motor

I/O Module  Master PLC

Display - Touchscreen

I/O Module  PLC

Communication Gateway

I/O Module  PLC

IT Network

Pavel Čeleda et al.  •  KYPO4INDUSTRY: A Testbed for Teaching Cybersecurity of Industrial Control Systems
Software Components

• Central testbed **controller** (virtual appliance).
• **Docker repository** for containers run at programmable logic controllers (PLC).
• **PLCs** running fully-fledged operating system (Raspbian).
• **Open-source** building blocks (PLC → Raspberry Pi).
ICS Cybersecurity Course at K4I Testbed

• Goal of the course: provide undergraduate students with an awareness of threats within the ICS domain via hands-on experience.

• Primary JTF curriculum Knowledge Area covered: System Security, with Knowledge Units:
  • Common System Architectures,
  • System Thinking, and
  • System Control.

• Also exercises communication, presentation skills, and time management.

---

1 https://cybered.hosting.acm.org/wp/
Course Format

- Spans the whole semester (13 weeks).
- Taught as flipped classroom format.
- 2-hour long weekly lab sessions.
- Homework assignments.
- Hands-on semester project – creating an ICS cybersecurity training game.
## Course Schedule and Structure

<table>
<thead>
<tr>
<th>Week</th>
<th>Class content</th>
<th>Student homework task (% of the grade)</th>
<th>Instructor tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Motivation, real attacks, legal issues</td>
<td>Prepare a presentation about an ICS attack (5%)</td>
<td>—</td>
</tr>
<tr>
<td>2</td>
<td>Student presentations of chosen attacks</td>
<td>Read this paper and some of the references</td>
<td>Grade the presentations</td>
</tr>
<tr>
<td>3</td>
<td>Hands-on labs on ICS testbed familiarization</td>
<td>Write an ICS security threat landscape report (5%)</td>
<td>—</td>
</tr>
<tr>
<td>4</td>
<td>Threat discussion, demo on ICS testbed</td>
<td>Write a short survey of CTF games in ICS (5%)</td>
<td>Grade the reports</td>
</tr>
<tr>
<td>5</td>
<td>Merge surveys, introduce game concepts</td>
<td>Select threats for your game</td>
<td>Grade the surveys</td>
</tr>
<tr>
<td>6</td>
<td>Threat modeling, storyline, consultation</td>
<td>Write a game draft</td>
<td>Check the game drafts</td>
</tr>
<tr>
<td>7</td>
<td>Preparing ICS part, educational objectives</td>
<td>Add learning outcomes and prerequisites</td>
<td>Check the game drafts</td>
</tr>
<tr>
<td>8</td>
<td>Preparing ICS and IT part</td>
<td>Prepare an alpha version of the game</td>
<td>Deploy the games</td>
</tr>
<tr>
<td>9</td>
<td>Dry run of the games with peers</td>
<td>Improve the game, submit bug reports (5%)</td>
<td>Review bug reports</td>
</tr>
<tr>
<td>10</td>
<td>Bug presentations, game improvement</td>
<td>Improve the game</td>
<td>—</td>
</tr>
<tr>
<td>11</td>
<td>Documentation, automation, deployment</td>
<td>Submit the game for presentation (50%)</td>
<td>Deploy the games</td>
</tr>
<tr>
<td>12</td>
<td>Public run of the games</td>
<td>Write a reflection from the public run (5%)</td>
<td>Oversee the event</td>
</tr>
<tr>
<td>13</td>
<td>Final reflections</td>
<td>Fix any issues that emerged in the public run (15%)</td>
<td>Grade the games</td>
</tr>
</tbody>
</table>
Experience and Lessons Learned

- Testbed components (PLCs, sensors, actuators) are available off the shelf.
- However, building a hardware setup that will replicate ICS in a laboratory environment is challenging.
- Students need a lot of guidance on how to create games with the ICS component.
- Otherwise, they will create games with the traditional IT component and do not fully exploit the capabilities of the ICS testbed.
Conclusions

- KYPO4INDUSTRY is a testbed for teaching ICS cybersecurity in a hands-on way.
- A novel course employs the testbed:
  - students learn about ICS threats,
  - develop an educational cyber game, and
  - exercise their soft skills during multiple public presentations.