Pedagogical Resources for Industrial Control Systems Security: Design, Implementation, Conveyance, and Evaluation

Guillermo A. Francia III
Jacksonville State University, gfrancia@jsu.edu

Greg Randall
Snead State Community College, greg.randall@snead.edu

Abstract
Industrial Control Systems (ICS), which are pervasive in our nation's critical infrastructures, are becoming increasingly at risk and vulnerable to internal and external threats. It is imperative that the future workforce be educated and trained on the security of such systems. However, it is equally important that careful and deliberate considerations must be exercised in designing and implementing the educational and training activities that pertain to ICS. To that end, we designed and implemented pedagogical materials and tools to facilitate the teaching and learning processes in the area of ICS security. In this paper, we describe those resources, the professional development workshop to disseminate the curriculum materials, and the evaluation results pertaining to those artifacts and activities.

Disciplines
Information Security | Management Information Systems | Technology and Innovation

SUMMARY

Industrial Control Systems (ICS), which are pervasive in our nation's critical infrastructures, are becoming increasingly at risk and vulnerable to internal and external threats. It is imperative that the future workforce be educated and trained on the security of such systems. However, it is equally important that careful and deliberate considerations must be exercised in designing and implementing the educational and training activities that pertain to ICS. To that end, we designed and implemented pedagogical materials and tools to facilitate the teaching and learning processes in the area of ICS security. In this paper, we describe those resources, the professional development workshop to disseminate the curriculum materials, and the evaluation results pertaining to those artifacts and activities.

We start by providing a literature review of prior and similar works on enhancing control systems security. Next, we layout the four control systems curriculum modules that we designed and implemented for training college instructors in an information security area that has not been well developed. These modules include various discussions and laboratory exercises on control system networks and protocols, Programmable Logic Control (PLC) programming, Human Machine Interface (HMI) design and development, PLC and HMI security, defensive techniques and incident response, control system vulnerability assessment and penetration testing, control system reconnaissance, deep packet inspection and analysis, and intrusion detection systems. We also describe the 2-day professional development workshop for college teachers and present the evaluation results that were gathered to measure the effectiveness of the pedagogical materials, the presentation, and the control system toolkit. Overall, the pre- and post-workshop evaluation surveys indicate that the topics for the workshop were well-chosen and well delivered, and the toolkit was rated as excellent. The results highlight that Industrial Control System Security is a topic that is not well-covered in computer science curricula and the workshop, as intended, highlighted the importance of that and other aspects of cybersecurity. Further, the toolkit and the laboratory activities that were provided to enable the integration of control system security into the participants' information security courses were very much appreciated. Finally, we provide concluding remarks and discuss possible avenues for extending the project beyond campus boundaries.