Wasfi Momen

SCADA and ICS Graduate Project Proposal

Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems (ICS) have been ignored in the connected world for a while, but the development of new technologies and demand for statistics create new risks for industrial control. Engineering these systems are now multifaceted with engineers working together with computer scientists. With the packaged software and hardware of SCADA and ICS, system designers must be aware of new threats. The goal of this project is to study the integration of new technologies into both existing and developing systems, summarize the analysis of papers discussing past attacks in specific cases and general models, and propose future design suggestions that protect exposed SCADA and ICS to the new connected world.

Understanding the history and context of past and future attacks on SCADA and ICS will be important to interpret future problems with currently developing systems and their potential attackers. Looking at past attacks and attackers gives a deeper look into if the current state of SCADA and ICS will be enough to protect against new threats that arise from the integration of new technology. Existing systems will be analyzed for their holes in security both from the control systems layers [5] and their corresponding threats [3]. We can then look at current and future system development such as the MARTA transit service [1] and power grids in developing countries [4] for additional threats caused by the adoption of new technology such as Internet of Things (IoT) for Remote Terminal Units (RTU).

As a part of additional qualitative data, papers discussing the analysis of current security standards and models will summarize the broad organizational vulnerabilities for SCADA and ICS. Exploring the different aspects that compromise the design and development of SCADA and ICS form the restrictions and demands that system designers face as well as their attempts to solve issues using new technology to give a customer-focused view. The advantages and disadvantages of security standards that the industry utilizes will be reviewed to understand the baseline for which further protections can be developed [2]. From the adoption and later abandonment of these standards, we can see the industry change in what roles SCADA and ICS can play with data-driven industrial processes.

The main quantitative part will rely on conducting research on the physical aspects of SCADA and ICS. Focus will be given to the software/hardware implement of concepts such as HMI (Human Machine Interface) and data historian/logging. Surveying how many organizations use new technologies such as smartphone apps, modern browsers, and business intelligence software visualizes the span of potential vulnerabilities in SCADA and ICS, even though the systems themselves are off the Internet.

From the results of the project, we can predict future threats and issue new protections for SCADA and ICS. These protections can correlate to past vulnerabilities and integrate themselves in the development and design of future systems. Even with a market and customer driven focus, the new SCADA and ICS of tomorrow can be both smarter and secure.

References

[1] D. Springstead, “MARTA Optimizing TAM Using a Systems Approach”, *U.S. Department of Transportation, Federal Transit Administration, 5th State of Good Repair Roundtable, June 3rd, 2015*

[2] K. Stouffer, V. Pilliterri, S. Lightman, M. Abrams, A. Hahn, “GUIDE TO INDUSTRIAL CONTROL SYSTEMS (ICS) SECURITY”, *NIST Special Publication, 800-82, Revision 2, USA*

[3] P. Singh, S. Garg, V. Kumar, Z. Saquib “A Testbed for SCADA Cyber Security and Intrusion Detection”*, 2015 International Conference on Cyber Security Of Smart cities, Industrial Control System and Communications (SSIC), 5-7 Aug. 2015*

[4] R. B. Roy, “Application of SCADA for Controlling Electrical Power System Network” in *University of Information Technology & Sciences, Volume 1 Issue 2, Dhaka, Bangladesh,* pp.85-97

[5] R. E. Johnson III, “Survey of SCADA Security Challenges and Potential Attack Vectors”, *2010 International Conference for Internet Technology and Secured Transactions (ICITST), 8-11 Nov. 2010*