ICS Testbed as a Visualized Protocol/HMI Honeypot

Contents

1 Group Members

1. Shiva Jyothi Angala
2. William Johnson
3. Pavan Madduri

2 Proposal

Proposed is the usage of a physical or simulated SCADA testbed as a honeypot in order to observe the physical effects of attacks both on the Modbus protocol over TCP/IP as well as on a HMI GUI that provides monitoring as well as component control.

Components involved are the physical or software-simulated testbed (including physical or software emulated PLCs running a Modbus interface over TCP/IP); a network security monitor such as Bro in order to detect attacks both created by the authors as well as attacks originating from a wide-area internet-exposed interface; and HMI software that reasonably and convincingly simulates HMI access to a water treatment plant, a power generation plant, and a pipeline.

The testbed, when convincingly exposed to the wider Internet with Modbus access as well as HMI, should provide forensic value much further than attack detection. It could be used to categorize attackers in terms of behavior (such as through attack scale, attack timings, and other fingerprinting categories). A physical testbed as honeypot also provides for a visual replay of various attacks if designed to detect and record/replay potentially discrete attacks.

The testbed would either be created through MathWorks Simulink or through a physical model. Network security monitoring would be provided through Bro NSM. The HMI software used to monitor as well as control some options such as pump status would be programmed from scratch or generated by using a preexisting (unknown as of yet) framework.

The attacks generated by the authors would primarily consist of Modbus commands. These attacks will assume that the authors have previously gained complete access to TCP/IP connected terminals of the testbed by some other vulnerability (firewall misconfiguration, reverse shell, etc.). TCP/IP-specific attacks will also be considered secondarily.

The core of the work would lie upon four areas: the creation of the HMI, the creation of the testbed (if built in Simulink), the creation of rules for Bro, and the creation of Modbus attacks by the authors. The HMI creation–as well as the creation of Bro rules–however, requires a heavy understanding of the testbed itself, so this work requires close interaction between group members. Also, Modbus attacks should be created with close collaboration amongst group members.

3 Portions of Work

1. HMI creation
2. Testbed creation
3. Bro rules
4. Modbus and TCP/IP attack creation