Title: Moving-Target Defense for Modbus networks

Industrial Control Systems (ICS) are widely used in critical infrastructures such as nuclear power plants, power grids, water purification systems and more. ICS Modbus® network communication protocol for ICS was developed in 1979 with no authentication or encryption. Addresses of Modbus® devices are static, which opens an attack vector for an adversary, who aims to send malicious commands to Modbus® devices. As many ICS networks use static addressing schemes and the number of available addresses is significantly lower, a malicious outsider can infest and attack the ICS network. In addition, many ICSs were designed and deployed without a secure authentication and encryption for low-level sensor devices. In order to provide protection for Modbus® communication networks, we propose a Moving Target Defense (MTD) for Modbus® networks. The addresses of Modbus® devices are changed either on a pre-determined schedule or after a suspicious network activity has been detected by monitoring the traffic analysis. MTD intends to complicate things for the attackers by changing the addresses so that they miss their targets. To ensure synchronicity and protection from malicious outsiders, communicating network nodes must be able to change the address based on the time stamp. Our method for MTD implementation ensures the synchronicity of the address change in the ICS.