Abstract: Securing SCADA Component Communication with the Utilization of Different Encryption Schemes

MinKyu Choi[1], Rosslin John Robles[2], Zita Vale[1], Carlos Ramos[1], Hoon Ko[1] and Goreti Marreiros[1]*
[1]*GECAD – Knowledge Engineering and Decision Support Group*
Institute of Engineering – Polytechnic of Porto, Portugal
{minky,zav,csr,hko,mgt}@isep.ipp.pt
[2]*Information Technology Department, College of Arts and Sciences*
University of San Agustin, Gen. Luna Street, Iloilo City 5000 Philippines
rosslin_john@yahoo.com

Abstract

SCADA Communication plays a vital role for Supervisory Control and Data Acquisition (SCADA) Monitoring Systems. The early SCADA communication took place over radio, modem, or dedicated serial lines. Today, it is much more common for SCADA communications to travel over LAN or WLAN. As the industry grows, SCADA systems become connected to other networks and the Internet. The open standards for SCADA Communications make it very easy for attackers to gain in-depth knowledge about the working of SCADA networks. Devices that are designed to operate in safety-critical environments are usually designed to failsafe, but security vulnerabilities could be exploited by an attacker to disable the fail-safe mechanisms. Thus, these devices must not only be designed for safety but also for security. Because of so many vulnerabilities encryption Schemes are applied to secure the communication between the SCADA components. This paper presents a study on the comparison of different Encryption Schemes for Securing SCADA Component Communication. The encryption schemes such as Symmetric Key Encryption in Wireless SCADA Environment, Asymmetric-key Encryption to Internet SCADA, and the Cross Crypto Scheme Cipher to secure communications for SCADA are analyzed and the outcome is evaluated.

Acknowledgements

"This work is supported by FEDER Funds through the "Programa Operacional Factores de Competitividade - COMPETE" program and by National Funds through FCT "Fundação para a Ciência e a Tecnologia" under the project: FCOMP-01-0124-FEDER-PEst-OE/EEI/UI0760 /2011