ADVANCES in NATURAL and APPLIED SCIENCES

ISSN: 1995-0772
EISSN: 1998-1090
2016 Special 10(14): pages 279-286

Published BY **AENSI Publication**
http://www.aensiweb.com/ANAS
Open Access Journal

A Testbed For Anomaly-Based Fault Detection In Pervasive Computing System

[1]V. Rajinikanth and [2]Dr. S. Dharmalingam

[1]Assistant prof / ECE, Adhi College of Engineering and Technology, kanchipuram – 631605
[2] Dean, Rathinam Technical Campus, Coimbatore.

Received 7 June 2016; Accepted 12 October 2016; Available 20 October 2016

Address For Correspondence:
V. Rajinikanth, Assistant prof / ECE, Adhi College of Engineering and Technology, kanchipuram – 631605

ABSTRACT

The critical infrastructures of our society are in the process of being modernized. Most significantly impacted are the industrial control systems through replacement of old electromechanical systems with advanced computing and communication technologies. This modernization has introduced new vulnerabilities to those infrastructures. Securing critical infrastructures is a challenging research problem, as these control systems were not designed with security in mind. This paper presents a testbed designed to study and simulate the various available techniques for securing and protecting Supervisory Control and Data Acquisition (SCADA) systems against a wide range of cyber attacks. The testbed is also used to evaluate the detection rate, false alerts and effectiveness of the protection techniques. We present preliminary results on using the testbed to detect a selected set of cyber attacks and the impact of the protection techniques on the operations of the system.

KEYWORDS: SACAD Systems, SCADA Cyber Attacks, Autonomic Software Protection System (ASPS)

INTRODUCTION

Supervisory control and data acquisition (SCADA) systems are widely used to control critical energy infrastructures (gas, oil, and electrical power). These systems were originally designed to work through isolated networks without connectivity to corporate or external networks. However, this assumption is not valid any more with the trend to build what is referred to as "Smart Grid" that uses advanced computing and communications technologies to bring knowledge to power grid so it can operate more efficiently.

Consequently, SCADA networks become a prime target for cyber attacks due to the profound and catastrophic impacts they can inject to our economy and all aspects of our life.

Traditional detection methods have focused on detecting network attacks, but have provided no real effective solutions to protect against attacks on the application layer. Attack detection techniques can be classified into two categories:

Signature-based and *anomaly-based detection.* Signature based detection is the more common of the two. To be effective, signature-based systems rely on large databases containing the digital signatures of known attacks, which require continuous updates as new exploits are identified. If an attack does not match closely enough a known signature, the signature-based system will miss it entirely. Anomaly-based systems are "trained" using data representing normal system behavior profiles. Activity that is "outside the norm" can then be detected. While anomaly-based systems are good at detecting new or unknown exploits, they require collecting large body of data to build their models of normal behavior.

With the explosive increase in the number, complexity and the speed of malicious attacks it is no longer feasible to identify all types of attacks and build defenses against them. As highlighted before, current security

To Cite This Article: V. Rajinikanth and Dr. S. Dharmalingam., A Testbed For Anomaly-Based Fault Detection In Pervasive Computing System. **Advances in Natural and Applied Sciences.** 10(14); Pages: 279-286