Notice of the Final Oral Examination
for the Degree of Master of Applied Science
of
HONGRUI WANG

BSc (Southeast University, 2014)

“Online Intrusion Detection Design and Implementation for SCADA Networks”

Department of Electrical and Computer Engineering

Wednesday, February 1, 2017
1:30 P.M.
Engineering Office Wing
Room 430

Supervisory Committee:
Dr. Xiaodai Dong, Department of Electrical and Computer Engineering, University of Victoria (Co-Supervisor)
Dr. Tao Lu, Department of Electrical and Computer Engineering, UVic (Co-Supervisor)
Dr. Issa Traore, Department of Electrical and Computer Engineering, UVic (Member)

External Examiner:
Dr. Sudhakar Ganti, Department of Computer Science, UVic

Chair of Oral Examination:
Dr. Hossein Nassaji, Department of Linguistics, UVic

Dr. David Capson, Dean, Faculty of Graduate Studies
Abstract

The standardization and interconnection of supervisory control and data acquisition (SCADA) systems has exposed the systems to cyber attacks. To improve the security of the SCADA systems, intrusion detection system (IDS) design is an effective method. However, traditional IDS design in the industrial networks mainly exploits the predefined rules, which needs to be complemented and developed to adapt to the big data scenario. Therefore, this thesis aims to design an anomaly-based novel hierarchical online intrusion detection system (HOIDS) for SCADA networks based on machine learning algorithms theoretically and build a testbed for implementing the theoretical idea of the anomaly-based intrusion detection. The theoretical design of HOIDS by utilizing the server-client topology while keeping clients distributed for global protection, high detection rate is achieved with minimum network impact. We implement accurate models of normal-abnormal binary detection and multi-attack identification based on logistic regression and quasi-Newton optimization algorithm using the Broyden-Fletcher-Goldfarb-Shanno approach. The detection system is capable of accelerating detection by information gain based feature selection or principle component analysis based dimension reduction. By evaluating our system using the KDD99 dataset and the industrial control system datasets, we demonstrate that our design is highly scalable, efficient and cost effective for securing SCADA infrastructures. Besides the theoretical IDS design, a testbed is implemented for SCADA network security research. It simulates the working environment of SCADA systems with the functions of data collection and analysis for intrusion detection. The testbed is implemented to be more flexible and extensible compared to the existing related work on the testbeds. In the testbed, Bro network analyzer is introduced to support the anomaly-based intrusion detection. Besides, a generic Linux-based host is used as the container of different network functions and an HMI together with the supervising network is set up to simulate the control center. The testbed can be effectively used, modified or expanded for the future work about SCADA network security.