ABSTRACT

The motivation behind this thesis is to provide an efficient and comprehensive solution to secure Supervisory Control and Data Acquisition (SCADA) systems and Industrial Control Systems (ICS). SCADA/ICS systems used to be on isolated networks. However, due to the increase in popularity and advancements of wireless networking and cloud technologies, SCADA/ICS systems have begun to expand their connectivity to the cloud; the extent of such connectivity can vary from system to system. Benefits of connecting to the internet/cloud are substantial, but such connectivity also makes those system vulnerable, for no longer being isolated.

Device recognition is useful first step in vulnerability identification and defense augmentation, but due to the lack of full traceability in case of legacy SCADA/ICS systems, the typical device recognition based on document inspection is not applicable. leading to the possibility of unaccounted security vulnerabilities in such systems. We propose a hybrid approach involving the mix of communication patterns and passive fingerprinting to identify unknown device types, manufacturers, and models. In addition, our ANDVI implementation maps the identified devices to their known vulnerabilities

To identify how interdependence among existing atomic vulnerabilities may be exploited by an adversary to stitch together an attack that can compromise the system, we propose a model-checking based Automated Attack-Graph Generator and Visualizer (A2G2V). The proposed A2G2V algorithm uses existing model-checking tools, an architecture description tool, and our own code to generate an attack-graph that enumerates the set of all possible sequences in which atomic-level vulnerabilities can be exploited to compromise system security.

Attack-graphs analysis enables security administrators to establish appropriate secu-

rity measurements to secure their system but practical considerations on time and cost can pose limit on their ability to address all system-level vulnerabilities at once. In this thesis, we propose an approach that identifies label-cuts within an attack-graph to automatically identify a set of critical-attacks that, when blocked, renders the system secure. The identification of a minimal label-cut is in general NP-complete, and in order to deal with this computational complexity, we propose a linear complexity approximation utilizing the Strongly-Connected-Components (SCCs) to identify a cut possessing a minimum number of labels and representing a critical-attacks set. Also, we compare our proposed algorithm to an exact minimum label-cut algorithm and to an approximation algorithm, both taken from the literature and report the improvements.

The proposed approaches were tested on real-world case studies, including two IT network systems and a SCADA network for a water treatment cyber-physical system.