Deniz Aytemiz

March 28- Paper Summaries

1. **Deep Learning-Based Anomaly Detection in Cyber-Physical Systems: Progress and Opportunities**
   In this paper deep learning based anomaly detection methods are examined in terms of anomalies, implementation and evaluation metrics. With the increasing deployment of CPS it is more important to ensure its security. Deep learning based anomaly detection is being used for this so far, however as both infrastructure and attacks gets more complex, anomaly detection methods need to be updated. The paper suggests that these methods should change in terms of threshold selection since the conventional method is prone to errors. Also they should be able to process real-time inputs to take real-time action and be able to locate the anomaly causing device in the CPS environment. In addition they mention the lack of benchmarks to evaluate and compare performances of different methods.
2. **Towards Automated Safety Vetting of PLC Code in Real-World Plants**
   ICS safety is crucial for safety since many attacks aim to give physical damage to the system. In this paper the current limitations of techniques for detecting PLC safety violations are emphasized and a new tool for program analysis is presented. It is stated that different timing between two events may change whether a sequence of events is a potential danger or not. By leveraging this fact VetPLC examines the timed event space for dynamic PLC code vetting. VetPLC is tested in two physically different testbeds and proved its effectiveness.
3. **W32.Stuxnet Dossier**
   In this paper a large and complex malware with multiple functionalities and components named Stuxnex is analyzed in depth. It is a threat designed for targeting ICS by modifying the PLC code and causing the ICS infrastructure to behave as the attacker wants. The many components of this malware are analyzed throughout the paper in addition with the timelines and statistics on its spread. It is discussed how the malware is spreaded, replicated, updated, bypassing security measures and hides the modified PLC code. An attack scenario is presented to highlight the process. The malware aims to spread on PLC controller computers on the LAN and find a suitable computer to run Step 7 which in turn modifies PLC and hides its tracks.