BINGHAMTON UNIVERSITY
STATE UNIVERSITY OF NEW YORK | Computer Science

COMPUTER SCIENCE RESEARCH SEMINAR

System Call Anomaly Detection in Multi-Threaded Programs

Dr. Marcus Pendleton
Cybersecurity Researcher
Air Force Research Laboratory, Rome, NY

Friday, April 27th at noon in room R15, Engineering Building

Abstract: System calls, or syscalls, are a popular data source for intrusion detection systems (IDSs) because they have strong security semantics and their collection imposes low performance overhead. However, existing solutions fall short in modeling, and thus protecting, real-world complex programs. In particular, they fall short in dealing with highly multi-threaded programs, especially those which contain diverse thread behaviors. Motivated by this problem, the present dissertation takes a holistic approach and makes three contributions.

The first contribution is a syscall dataset collector which enables the production of custom datasets for syscall host intrusion systems (HIDSs). With aging datasets, current syscall HIDS solutions are pigeonholed into using their limited characteristics, thus, limiting their effectiveness when applied to real-world programs and systems. We provide an extensible syscall dataset collector which includes structural and contextual information regarding syscalls, yet allows for researchers to easily add their own features. This dataset collector can aid researchers in widening the solution space of syscall HIDS.

The second contribution is a methodology to identify thread behaviors in complex programs. Due to the flat, interleaved structure of syscall patterns from simple programs in existing datasets, the problem of effectively modeling, and thus, monitoring complex multi-threaded programs remains largely unaddressed. Providing thread-wise sequences from complex, multi-threaded programs is a step in the right direction. However, threads are often anonymous and do not lend themselves to easy identification. Therefore, we propose clustering thread behaviors, which are represented by graphs, as a preprocessing step that can be used as a means for thread behavior classification.

The third contribution is an anomaly detection technique leveraging the identified groups of program behaviors from the second contribution. As mentioned earlier, modeling and monitoring complex multi-threaded programs in syscall HIDS is challenging because threads may exhibit different behaviors, each emitting a distinct syscall pattern. Therefore, a “one size fits all” approach in capturing the diverse behaviors confounds the monolithic models of previous approaches. We present detection logic utilizing the clusters of behaviors to automatically determine thresholds between normal and anomalous behaviors. The result is an accurate detection model.

Bio: Dr. Marcus Pendleton is a former combat systems and cyberspace operations officer (CSO/-COO) for the United States Air Force. He is currently a cybersecurity researcher at the Air Force Research Laboratory in Rome, New York. There, he will continue to leverage his experiences in operations from the military, high-performance computing as an administrator at Ames Laboratory (Iowa State University), and cybersecurity as a research assistant for the Institute of Cyber Security (The University of Texas at San Antonio) to help develop state-of-the-art cyber solutions to protect our critical infrastructures.

This event is funded by GSOCS, a subsidiary of GSO, using Student Activity Fee funds

Refreshments will be provided!