Integrated Data Space Randomization and Control Reconfiguration for Securing Cyber-Physical Systems

Submitted by akarns on Wed, 03/20/2019 - 2:06pm. Contributors:
Bradley PotteigerZhenkai ZhangXenofon Koutsoukos

ABSTRACT

Non-control data attacks have become widely popular for circumventing authentication mechanisms in websites, servers, and personal computers. Moreover, in the context of Cyber-Physical Systems (CPS) attacks can be executed against not only authentication but also safety. With the tightly coupled nature between the cyber components and physical dynamics, any unauthorized change to safety-critical variables may cause damage or even catastrophic consequences. Moving target defense (MTD) techniques such as data space randomization (DSR) can be effective for protecting against various types of memory corruption attacks including non-control data attacks. However, in terms of CPS it is also critical to ensure the timely Cyber-Physical interactions after attacks thwarted by MTD. This paper addresses the problem of maintaining system stability and security properties of a CPS in the face of non-control data attacks by developing a DSR approach for randomizing binaries at runtime, creating a variable redundancy based detection algorithm for identifying variable integrity violations, and integrating a control reconfiguration architecture for maintaining safe and reliable operation. Our security framework is demonstrated utilizing an autonomous vehicle case study.

Bradley Potteiger is a PhD student in the Department of Electrical Engineering at Vanderbilt University with a research affiliation at the Institute for Software Integrated Systems. He received his MS. degree from Vanderbilt University in Electrical Engineering and his BS. degree in Computer Engineering from the University of Maryland, Baltimore County. His research at Vanderbilt is focused on Cyber Physical System (CPS) security with respect to protecting safety critical systems. Through his research he has worked with various research organizations within the government sector and industry.

Bradley Potteiger | Zhenkai Zhang | Xenofon Koutsoukos

Preview: Preview | Thumbnail | Medium | Image

Other available formats:

Integrated Data Space Randomization and Control Reconfiguration for Securing Cyber-Physical Systems

Presentation Session 2