Developing Models for Physical Attacks in Cyber-Physical Systems Security and Privacy

Submitted by awhitesell on Fri, 07/13/2018 - 2:37pm

Title	Developing Models for Physical Attacks in Cyber-Physical Systems Security and Privacy
Publication Type	Conference Paper
Year of Publication	2017
Authors	Carmen Cheh, University of Illinois at Urbana-Champaign, Ken Keefe, University of Illinois at Urbana-Champaign, Brett Feddersen, University of Illinois at Urbana-Champaign, Binbin Chen, Advanced Digital Sciences Center Singapre, William G. Temple, Advance Digital Science Center Singapore, William H. Sanders, University of Illinois at Urbana-Champaign
Conference Name	ACM Workshop on Cyber-Physical Systems Security and Privacy
Date Published	November 2017
Publisher	ACM
Conference Location	Dallas, TX
Keywords	attack graph, Cyber-physical systems, Monitoring, Fusion, and Response for Cyber Resilience, NSA SoS Lablets Materials, Ontology, Physical attack, Resilient Architectures, science of security, UIUC
Abstract	In this paper, we analyze the security of cyber-physical systems using the ADversary VIew Security Evaluation (ADVISE) meta modeling approach, taking into consideration the efects of physical attacks. To build our model of the system, we construct an ontology that describes the system components and the relationships among them. The ontology also deines attack steps that represent cyber and physical actions that afect the system entities. We apply the ADVISE meta modeling approach, which admits as input our deined ontology, to a railway system use case to obtain insights regarding the system's security. The ADVISE Meta tool takes in a system model of a railway station and generates an attack execution graph that shows the actions that adversaries may take to reach their goal. We consider several adversary proiles, ranging from outsiders to insider staf members, and compare their attack paths in terms of targeted assets, time to achieve the goal, and probability of detection. The generated results show that even adversaries with access to noncritical assets can afect system service by intelligently crafting their attacks to trigger a physical sequence of efects. We also identify the physical devices and user actions that require more in-depth monitoring to reinforce the system's security.
Citation Key	node-54924

Attachment	Taxonomy	Kind	Size

Developing Models for Physical Attacks in Cyber-Physical Systems	Science of Security attack graph cyber-physical systems Monitoring, Fusion, and Response for Cyber Resilience NSA SoS Lablets Materials Ontology Physical attack Resilient Architectures Science of Security UIUC Resilient Architectures Monitoring, Fusion, and Response for Cyber Resilience UIUC UIUC NSA SoS Lablets Materials	PDF document	673.43 KB	Download Preview

Science of Security attack graph cyber-physical systems Monitoring, Fusion, and Response for Cyber Resilience NSA SoS Lablets Materials Ontology Physical attack Resilient Architectures Science of Security UIUC UIUC NSA SoS Lablets Materials Resilient Architectures UIUC Resilient Architectures UIUC Monitoring, Fusion, and Response for Cyber Resilience