[1] B. Genge, C. Siaterlis, and M. Hohenadel. AMICI: an assessment platform for multi-domain security experimentation on critical infrastructures. In B. M. Hämmerli, N. Kalstad Svendsen, and J. Lopez, editors, *Critical Information Infrastructures Security*, volume 7722 of *Lecture Notes in Computer Science*, pages 228-239. Springer Berlin Heidelberg, 2013. [bib | DOI]

This paper presents AMICI, a new Assessment/analysis platform for Multiple Interdependent Critical Infrastructures (CIs). Its architecture builds on our previous work and uses Emulab to recreate ICT software and hardware components and Simulink to run the physical process models. Our previous framework is extended with software components to provide a set of capabilities that would enable the analysis of complex interdependencies between multiple CIs: flexible integration of multiple physical process models; opened architecture to enable interaction with ad-hoc software; support experimentation with real software/malware; automated experiment management capabilities. The applicability of the approach is proven through a case study involving three CIs: ICT, power grid and railway.

Keywords: Critical Infrastructure; security; experimentation; testbed

[2] B. Reaves and T. Morris. An open virtual testbed for industrial control system security research. *International Journal of Information Security*, 11(4):215-229, 2012. [bib | DOI]

Industrial control system security has been a topic of scrutiny and research for several years, and many security issues are well known. However, research efforts are impeded by a lack of an open virtual industrial control system testbed for security research. This paper describes a virtual testbed framework using Python to create discrete testbed components including virtual devices and process simulators. The virtual testbed is designed such that the testbeds are inter-operable with real industrial control system devices and such that the virtual testbeds can provide comparable industrial control system network behavior to a laboratory testbed. Two virtual testbeds modeled upon actual laboratory testbeds have been developed and have been shown to be inter-operable with real industrial control system equipment and vulnerable to attacks in the same manner as a real system. Additionally, these testbeds have been quantitatively shown to produce traffic close to laboratory systems.

Keywords: Virtual testbed; Industrial control system; SCADA; Cybersecurity

[3] C. Siaterlis, B. Genge, and M. Hohenadel. EPIC: A testbed for scientifically rigorous cyber-physical security experimentation. *IEEE Transactions on Emerging Topics in Computing*, 1(2):319-330, Dec. 2013. [bib | DOI]

Recent malware, like Stuxnet and Flame, constitute a major threat to networked critical infrastructures (NCIs), e.g., power plants. They revealed several vulnerabilities in today's NCIs, but most importantly they highlighted the lack of an efficient scientific approach to conduct experiments that measure the impact of cyber threats on both the physical and the cyber parts of NCIs. In this paper, we present EPIC, a novel cyber-physical testbed, and a modern scientific instrument that can provide accurate assessments of the effects that cyber-attacks may have on the cyber and physical dimensions of NCIs. To meet the complexity of today's NCIs, EPIC employs an Emulab-based testbed to recreate the cyber part of NCIs and multiple software simulators for the physical part. Its main advantage is that it can support very accurate, real-time, repeatable, and realistic experiments with heterogeneous infrastructures. We show through several case studies how EPIC can be applied to explore the impact that cyber-attacks and Information and Communications Technology system disruptions have on critical infrastructures.

Keywords: digital simulation;security of data;EPIC testbed;Emulab-based testbed;Flame malware;NCI;Stuxnet malware;cyber parts;cyber threats;cyber-attacks;cyber-physical security experimentation;cyber-physical testbed;heterogeneous infrastructures;information and communications technology system disruptions;networked critical infrastructures;software simulators;Computational modeling;Computer security;Computer viruses;Malware;Mathematical model;Real-time systems;Research and development;Cyber-physical;Emulab;networked critical infrastructures;simulation;testbed

This file was generated by bibtex2html 1.96.