1. Record Nr. UNINA9910349301503321

Titolo	Adversarial and Uncertain Reasoning for Adaptive Cyber Defense : Control- and Game-Theoretic Approaches to Cyber Security / / edited by Sushil Jajodia, George Cybenko, Peng Liu, Cliff Wang, Michael Wellman
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2019
ISBN	3-030-30719-0
Edizione	[1st ed. 2019.]
Descrizione fisica	1 online resource (VII, 263 p. 120 illus., 45 illus. in color.)
Collana	Security and Cryptology, , 2946-1863 ; ; 11830
Disciplina	005.8
Soggetti	Computer crimes Computer engineering Computer networks Computers Computer science - Mathematics Mathematical statistics Computer Crime Computer Engineering and Networks Computing Milieux Computer Communication Networks Probability and Statistics in Computer Science
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Overview of Control and Game Theory in Adaptive Cyber-Defenses -- Control Theoretic Approaches to Cyber-Security -- Game-Theoretic Approaches to Cyber-Security: Issues and Challenges and Results -- Reinforcement Learning for Adaptive Cyber Defense against Zero-day Attacks -- Moving Target Defense Quantification -- Empirical Game-Theoretic Methods for Adaptive Cyber-Defense -- MTD Techniques for Memory Protection against Zero-Day Attacks -- Adaptive Cyber Defenses for Botnet Detection and Mitigation -- Optimizing Alert Data Management Processes at a Cyber Security Operations Center -- Online and Scalable Adaptive Cyber Defense.

Sommario/riassunto	Today’s cyber defenses are largely static allowing adversaries to pre-plan their attacks. In response to this situation, researchers have started to investigate various methods that make networked information systems less homogeneous and less predictable by engineering systems that have homogeneous functionalities but randomized manifestations. The 10 papers included in this State-of-the Art Survey present recent advances made by a large team of researchers working on the same US Department of Defense Multidisciplinary University Research Initiative (MURI) project during 2013-2019. This project has developed a new class of technologies called Adaptive Cyber Defense (ACD) by building on two active but heretofore separate research areas: Adaptation Techniques (AT) and Adversarial Reasoning (AR). AT methods introduce diversity and uncertainty into networks, applications, and hosts. AR combines machine learning, behavioral science, operations research, control theory, and game theory to address the goal of computing effective strategies in dynamic, adversarial environments. .