Game theoretic modeling of cyber deception in the Internet of Battlefield Things

Speaker: Dr. Charles A. Kamhoua
US Army Research Lab
Friday, Nov 30, 2018
10AM – 11AM, T3

Abstract

Most sophisticated cyberattacks follow the well-known cyber kill chain. The first step of the cyber kill chain is the reconnaissance phase where attacker probe the network in search of weakness, misconfiguration, vulnerabilities, and identify potential targets before the actual attack start. To this end, the attacker needs to collect important information about the characteristics of each device (i.e., hardware, operating system, applications), the network topology, the different subnet, firewall rules, access control, privilege, the communication protocol at each layer, and the machine learning algorithm on each IoBT device. The attacker reconnaissance can be summarized by an attack graph in which the node represents vulnerable IoBT devices and the edge shows their associated vulnerabilities.

This work investigates cyber deception as a complex game in which each player has three concurrent and interdependent objectives. Each player imperfectly monitors (partial observation) other players’ action to find out each player’s identity, strategies, payoff, available information, capability, and to continuously predict their intent. Each player strategically selects to which players to hide particular information (e.g., camouflage). Each player judiciously manipulates other players’ perception (e.g., decoy) based on his observed action, estimated capability, and predicted intent. This work examines from the defender’s perspective several deception games on an attack graph. The defender goal is to stop the attacker early in the cyber kill chain and prevent the subsequent more dangerous phases.
Biography

**Dr. Charles A. Kamhoua** is a researcher at the Network Security Branch of the U.S. Army Research Laboratory (ARL) in Adelphi, MD, where he is responsible for conducting and directing basic research in the area of game theory applied to cyber security. Prior to joining the Army Research Laboratory, he was a researcher at the U.S. Air Force Research Laboratory (AFRL), Rome, New York for 6 years and an educator in different academic institutions for more than 10 years. He has held visiting research positions at the University of Oxford and Harvard University. He has co-authored more than 150 peer-reviewed journal and conference papers. He is a co-inventor of a patent, 6 patent application, and co-editor of 3 books at IEEE Press. He has presented over 40 invited keynote and distinguished speeches and has co-organized over 10 conferences and workshops. He has mentored more than 60 young scholars, including students, postdocs, and Summer Faculty Fellow. He has been recognized for his scholarship and leadership with numerous prestigious awards, including the 2018 ARL Achievement Award for leadership and outstanding contribution to the ARL Cyber Camo (cyber deception) project, the 2018 Fulbright Senior Specialist Fellowship, the 2017 AFRL Information Directorate Basic Research Award “For Outstanding Achievements in Basic Research,” the 2017 Fred I. Diamond Award for the best paper published at AFRL’s Information Directorate, 40 Air Force Notable Achievement Awards, the 2016 FIU Charles E. Perry Young Alumni Visionary Award, the 2015 Black Engineer of the Year Award (BEYA), the 2015 NSBE Golden Torch Award—Pioneer of the Year, and selection to the 2015 Heidelberg Laureate Forum, to name a few. He has been congratulated by the White House and US Congress for those achievements. He received a B.S. in electronics from the University of Douala (ENSET), Cameroon, in 1999, an M.S. in Telecommunication and Networking from Florida International University (FIU) in 2008, and a Ph.D. in Electrical Engineering from FIU in 2011. He is currently an advisor for the National Research Council postdoc program, a member of the FIU alumni association and ACM, and a senior member of IEEE.