UCF DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCEINCE

Fall 2014 Seminar Series

Presented by the CS Division

SECURITY AND INTERDEPENDENCY IN A PUBLIC CLOUD: A GAME THEORETIC APPROACH

WEDNESDAY SEPTEMBER 17, 2014 • 11:00 AM – HEC 450

As cloud computing thrives, many organizations – both large and small – are joining a public cloud to take advantage of its multiple benefits. Especially public cloud based computing, is cost efficient, i.e., a cloud user can reduce spending on technology infrastructure and have easy access to their information without up-front or long-term commitment of resources. Despite those benefits, concern over cyber security is the main reason many large organizations with sensitive information such as the Department of Defense have been reluctant to join a public cloud. This is because different public cloud users share a common platform such as the hypervisor. An attacker can compromise a virtual machine (VM) to launch an attack on the hypervisor which, if compromised, can instantly yield the compromising of all the VMs running on top of that hypervisor. This work shows that there are multiple Nash equilibria of the public cloud security game. However, the players use a Nash equilibrium profile depending on the probability that the hypervisor is compromised given a successful attack on a user and the total expense required to invest in security. Finally, there is no Nash equilibrium in which all the users in a public cloud fully invest in security.

DR. CHARLES KAMHOUA

Air Force Research Laboratory

Charles A. Kamhoua received his B.S. in Electronic from the University of Douala (ENSET), Cameroon in 1999, and the M.S. in Telecommunication and Networking and PhD in Electrical Engineering from Florida International University in 2008 and 2011 respectively. In 2011, he joined the Cyber Assurance Branch of the U.S. Air Force Research Laboratory (AFRL), Rome, New York, as a National Academies Postdoctoral Fellow, became a Research Electronics Engineer in 2012 and a Science & Technology Program Manager in 2013.

Dr. Kamhoua is the principal investigator of the AFRL in-house basic research project, Survivability Through Optimizing Resilient Mechanisms (STORM) funded by the Air Force Office of Scientific Research (AFOSR). He is leading a team of more than 10 researchers including postdocs, summer faculties and graduate and undergraduate students from multiple universities across the United States. His technical expertise is sought from the highest levels within DoD as evidenced by multiple tech transition reviews of DARPA at the Pentagon.

His current research interests cover the application of game theory and mechanism design to cyber security and survivability, with over 30 technical publications. He participated in multiple research visits in the United States and abroad to maintain technological excellence in cyber security research relevant to warfighter and civilian needs. His research was presented in multiple national and international conferences. He is a reviewer of multiple journals and serves on the technical program committees of several international conferences.

Dr. Kamhoua won some of the most prestigious awards including an Air Force Notable Achievement Award, an AFOSR basic research award of nearly a million dollars, the AFOSR Windows on the World Visiting Research Fellowship at Oxford University, UK, a Best Paper Award at the 2013 International Symposium on Foundations of Open Source Intelligence and Security Informatics (FOSINT-SI 2013), a National Academies Postdoctoral Fellowship award, and a National Science Foundation (NSF) PIRE award at Fluminense Federal University, Brazil. He is an advisor for the National Research Council, a member of the National Society of Black Engineer (NSBE) and a Senior Member of IEEE.

Hosted by: Dr. Mainak Chatterjee

UCF

4328 Scorpius Street Room 346 Orlando, FL 32816

WWW.EECS.UCF.EDU