**COLLOQUIUM**

Department of Computer Science and Engineering

University of South Carolina

### **Application of Game Theory to High Assurance Cloud Computing**

**Charles A. Kamhoua**

Date: **September 02, 2016**

Time: **1420-1510 (2:20-3:10pm)**

Place: **Swearingen 2A31**

# Abstract

The growth of cloud computing has spurred many entities, both small and large, to use cloud services for cost savings. Public cloud computing has allowed for quick, dynamic scalability without many overhead or long-term commitments. However, 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 due to three challenging problems. First, the current cloud infrastructures lack provable trustworthiness. Integrating Trusted Computing (TC) technologies with cloud infrastructure shows a promising method for verifying the cloud’s behaviors, which may in turn facilitate provable trustworthiness. Second, public clouds have the inherent and unknown danger stemming from a shared platform - namely, the hypervisor. An attacker that subverts a virtual machine (VM) and then goes on to compromise the hypervisor can readily compromise all virtual machines on that hypervisor. We propose a security-aware virtual machine placement scheme in the cloud. Third, a sophisticated attack in a cloud has to be understood as a sequence of events that calls for the detection/response model to encompass observations from varying dimensions. We discuss a method to automatically determine the best response, given the observations on the system states from a set of monitors.

Game theory provides a rich mathematical tool to analyze conflict within strategic interactions and thereby gain a deeper understanding of cloud security issues. Theoretical constructs or mathematical abstractions provide a rigorous scientific basis for cyber security because they allow for reasoning quantitatively about cyber-attacks. This talk will address the three cloud security challenging problems identified above and report on our latest findings from this body of work.

**Charles A. Kamhoua** received the BS in electronic from the University of Douala (ENSET), Cameroon, in 1999, and the MS in telecommunication and networking and the PhD in electrical engineering from Florida International University (FIU), 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 and became a Research Electronics Engineer in 2012. Prior to joining AFRL, he was an educator for more than 10 years. His current research interests include the application of game theory to cyber security, survivability, cloud computing, hardware Trojan, online social network, wireless communication and cyber threat information sharing. He has more than 60 technical publications in prestigious journals and International conferences along with a Best Paper Award at the 2013 IEEE FOSINTSI. He has mentored more than 40 young scholars at AFRL counting Summer Faculty Fellow, postdoc, and students. He has been invited to more than 30 keynote and distinguished speeches in the USA and abroad. He has been recognized for his scholarship and leadership with numerous prestigious awards including 30 Air Force Notable Achievement Awards, the 2016 FIU Charles E. Perry Young Alumni Visionary Award, the 2015 AFOSR Windows on the World Visiting Research Fellowship at Oxford University, UK, an AFOSR Basic Research Award, the 2015 Black Engineer of the Year Award (BEYA), the 2015 NSBE Golden Torch Award—Pioneer of the Year, selection to the 2015 Heidelberg Laureate Forum, and the 2011 NSF PIRE Award at the Fluminense Federal University, Brazil. He is currently an advisor for the National Research Council, a member of ACM, the FIU alumni association, NSBE and a senior member of IEEE.