UCF DEPARTMENT OF COMPUTER SCIENCE

Spring 2016 Distinguished Speaker Series

EVERYTHING YOU CODE CAN AND WILL BE RE-USED AGAINST YOU

FRIDAY FEBRUARY 5, 2016 • 10:00 AM – HEC 450

One may wonder why memory-corruption vulnerabilities–a decades old problem–remain a persistent source of threats against modern software. The main problem is that modern software still contain vast amounts of unsafe, legacy code written in the error-prone C and C++ languages. Moreover, exploitation techniques are rapidly evolving and incorporate increasingly sophisticated techniques such as code reuse and can bypass widely deployed countermeasures like data execution prevention (DEP) and layout randomization (ASLR). The recent vulnerabilities (e.g., “StageFright" and "One Class to Rule them All") affect hundreds of millions of Android systems, and are just the latest entries in a long series of incidents that show the magnitude of the problem.

The good news is that researchers in both academia and industry have spent considerable effort to improve defenses against modern code-reuse exploits. Even though these solutions raise the bar for exploitation substantially, attackers continually discover new bypasses. This talk gives a brief overview of the exciting arms race between code-reuse attacks and mitigation techniques. We highlight the main challenges of recent defenses aimed at addressing the longstanding problems of memory corruption and memory disclosure vulnerabilities. The game is not over yet.

DR. AHMAD-REZA SADEGHI

Center for Advance Security Research Darmstadt

Prof. Dr.-Ing. Ahmad-Reza Sadeghi is the head of the System Security Lab at the Center for Advance Security Research Darmstadt (CASED), Technische Universität Darmstadt. Since January 2012 he is the Director of Intel Collaborative Research Institute for Secure Computing (ICRI-SC) at TU Darmstadt, Germany.

He received his PhD in Computer Science with the focus on privacy protecting cryptographic protocols and systems from the University of Saarland in Saarbrücken, Germany. Prior to academia, he worked in Research and Development of Telecommunications enterprises, amongst others Ericson Telecommunications. He has been leading and involved in a variety of national and international research and development projects on design and implementation of Trustworthy Computing Platforms and Trusted Computing, Security Hardware, Physically Unclonable Functions (PUF), Cryptographic Privacy-Protecting Systems, and Cryptographic Compilers (in particular for secure computation). He has been continuously contributing to the IT security research community and serving as general or program chair as well as program committee member of many conferences and workshops in Information Security and Privacy, Trusted Computing and Applied Cryptography. He served on the editorial boards of the ACM Transactions on Information and System Security (TISSEC). Currently he is on the editorial board of ACM Books and acts as guest editor of the IEEE Transactions on Computer-Aided Design (Special Issue on Hardware Security and Trust).

Prof. Sadeghi has been awarded with the renowned German prize “Karl Heinz Beckurts” for his research on Trusted and Trustworthy Computing technology and its transfer to industrial practice. The award honors excellent scientific achievements with high impact on industrial innovations in Germany. Further, his group received the second prize of German IT Security Competition Award 2010.

Hosted by: Dr. Gary T. Leavens

UCF

4328 Scorpius Street Room 346 Orlando, FL 32816

WWW.CS.UCF.EDU