CECS
CENTER FOR EMBEDDED & CYBER-PHYSICAL SYSTEMS
UNIVERSITY OF CALIFORNIA · IRVINE

CECS Seminar

"Security of Additive Manufacturing: New Frontiers"

Mark Yampolskiy

Assistant Professor, University of South Alabama, Mobile, Alabama

Friday, October 19th
10:00 a.m.- 11:00 a.m.
Engineering Hall 2430

Abstract: Additive Manufacturing (AM), a.k.a. 3D printing, is a rapidly growing multibillion-dollar industry that is increasingly used to manufacture functional parts, including components of safety critical systems in the aerospace, automotive, and other industries. However, reliance on the IT infrastructure and the high degree of computerization of the manufacturing machines make AM susceptible to a variety of cyber and cyber-physical attacks.
AM Security is a fairly new and highly inter-disciplinary field of research that aims to address the novel threats emerging for this manufacturing technology. This talk will first provide an introduction to the field. Focusing on AM sabotage, one of the identified threat categories, Dr. Mark Yampolskiy will then introduce emerging frontiers: sabotage of composite material parts, AM forensics, and detection of sabotage attacks via side-channel measurements. The talk will conclude with a summary of identified research gaps in the current state of the art.

Biography: Mark Yampolskiy received Ph.D. in Computer Science from Ludwig-Maximilians University of Munich, Germany in 2009. He currently holds an Assistant Professor position at the University of South Alabama. Since his post-doctoral appointment at Vanderbilt University (2012-2013), Mark Yampolskiy is performing research on Security of Cyber-Physical Systems (CPS). Mark Yampolskiy was among the researchers who pioneered Security of Additive Manufacturing (AM, a.k.a. 3D Printing) around 2014. AM Security remains his major research focus, and he is currently one of the leading experts in this field. His work is predominantly associated with two threat categories, sabotage of 3D-printed functional parts and theft of intellectual property. He has numerous seminal publications in the field, ranging from attacks on/with AM up to novel approaches for the detection of such attacks. AM Security is a highly interdisciplinary field of research. In order to address this challenge, Mark Yampolskiy actively collaborates with experts from different disciplines. His major collaboration partners are affiliated with Lawrence Livermore National Laboratory (LLNL), Ben Gurion University of the Negev (BGU) in Israel, Singapore University of Technology and Design (SUTD), Auburn University (AU), and University of Tennessee at Chattanooga (UTC).