# Computer Science

Colloquium Series

**Date:** Thursday, November 29, 2018
**Time:** 3:30pm
**Location:** 1230 Communications

## Integrating Security in Cyber-Physical Systems

Modern embedded control architectures have moved from isolated systems to open architectures, such as new automotive systems with services that include remote diagnostics, code updates, and vehicle-to-vehicle communication. However, this increasing set of functionalities, network interoperability, and system design complexity have also introduced security vulnerabilities that are easily exploitable, since current embedded and cyber-physical systems have not been built with security in mind. Furthermore, the tight interaction between information technology and physical world makes these systems vulnerable to malicious attacks beyond the standard cyber-attacks, while relying exclusively on conventional security techniques may be unfeasible due to resource-constraints and long system lifetime.

Consequently, there is a need to change the way we reason about security in cyber-physical systems, and start designing platform-aware attack-resilient components and architectures capable of dealing with various attacks on the systems and its environment. In this talk, I will present our recent efforts in this domain, starting from cyber-physical security techniques that (a) capture effects of attacks on system performance, (b) introduce attack resilience into control algorithms and facilitate attack detection, and (c) enable mapping of the desired Quality-of-Control (QoC) under attack guarantees into real-time performance requirements on the underlying OS and networks. In addition, I will introduce a physics-aware design framework for securing resource-constrained CPS, that supports design-time tradeoffs between QoC in the presence of attacks and system resources used by the deployed security mechanisms, such as message authentication. This design framework has been used to add strong security guarantees in several existing automotive system. Finally, for systems with varying levels of autonomy and human interaction, I will show how we can exploit human power of inductive reasoning and the ability to provide context, to improve the overall security guarantees.

Part of the Computer Science Seminar Series

Iowa State University
**Department of Computer Science**
www.cs.iastate.edu

Miroslav Pajic is the Nortel Networks Assistant Professor in Department of Electrical and Computer Engineering, Duke University, with a secondary appointment in the Computer Science Department. He received the Dipl. Ing. and M.S. degrees from the University of Belgrade, Serbia, in 2003 and 2007, as well as the M.S. and Ph.D. degrees from the University of Pennsylvania, Philadelphia, in 2010 and 2012, respectively. His research interests focus on design and analysis of cyber-physical systems (CPS) and in particular on model-based design of CPS, real-time and embedded systems, high-assurance distributed and networked control systems, and high-confidence medical devices and systems.

Dr. Pajic received various awards including NSF CAREER Award, ONR Young Investigator Program Award, ACM SIGBED Frank Anger Memorial Award, Joseph and Rosaline Wolf Best Dissertation Award from Penn Engineering, IBM Faculty Award, as well as six Best Paper and Runner-up Awards, such as the Best Paper Awards at the 2017 ACM SIGBED International Conference on Embedded Software (EMSOFT) and 2014 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), and the Best Student Paper award at the 2012 IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS). He is an associate editor of the ACM Transactions on Computing in Healthcare (ACM HEALTH) and a co-chair of the 2019 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS'19).