TEMPLE
UNIVERSITY®

Spring 2020 Colloquium

Department of Computer and Information Sciences

Distinguished Lecture

Toward Secure and Safe Learning-Enabled Autonomous Cyber-Physical Systems

Dr. Insup Lee

Cecilia Fitler Moore Professor
PRECISE Center, Department of Computer and Information Science
University of Pennsylvania
lee@cis.upenn.edu, www.cis.upenn.edu/~lee/

Friday, February 21st, 11 AM, SERC 306

Abstract: Machine learning provides a potentially revolutionary way for extracting semantic meaning suitable for higher-level autonomy. Unfortunately, our current lack of understanding of when and how machine learning works makes it challenging to provide guarantees for learning-enable components (LECs) in safety critical systems. Despite this limitation, given the impressive experimental results of machine learning, researchers have quickly incorporated learning in perception-action loops even in driverless cars and aerial vehicles, where the safety requirements are very high. This has resulted in unreliable behavior and public failures (e.g., Tesla and drone crashes, Uber running a red light) that may lead to loss of trust in autonomy.

There are many challenges in developing and assuring learning-enabled autonomous cyber-physical systems that are safe and secure. This talk will present several specific problems and various techniques and tools that we have developed to address some of these problems. They include techniques for resilient sensor-fusion to deal with sensor attacks and techniques for verifying closed-loop systems with DNN components.

Bio: Insup Lee is Cecilia Fitler Moore Professor of Computer and Information Science, Co-Director of Penn Health-Tech Center since 2017, and Director of PRECISE Center since 2008 at the University of Pennsylvania. He also holds a secondary appointment in the Department of Electrical and Systems Engineering. His research interests include cyber-physical systems (CPS), real-time systems, embedded systems, high-confidence medical device systems, formal methods and tools, run-time verification, software certification, and trust management. The theme of his research activities has been to assure and improve the correctness, safety, and timeliness of life-critical embedded systems. His papers received the best paper awards in IEEE RTSS 2003, CEAS 2011, IEEE RTAS 2012, IEEE RTSS 2012, ACM/IEEE ICCPS 2014, IEEE CPSNA 2016, IEEE ISORC 2918, IEEE RTAS 2019, and MEMOCODE 2019. Recently, he has been working in Internet of Medical Things, security of cyber physical systems, and safe autonomy.

He has served on many program committees, chaired many international conferences and workshops and served on various steering and advisory committees of technical societies. He is founding co-Editor-in-Chief of the new ACM Transactions on Computing for Healthcare (HEALTH, 2018) and founding co-Editor-in-Chief of KIISE Journal of Computing Science and Engineering (JCSE, 2007). He has also served on the editorial boards on the several scientific journals, including Journal of ACM, ACM Transactions on Cyber-Physical Systems, IEEE Transactions on Computers, Formal Methods in System Design, and Real-Time Systems Journal. He was Chair of ACM Special Interest Group on Embedded Systems (SIGBED, 2015-2019) and Chair of IEEE TC on Real-Time Systems (TCRTS, 2003-2004). He was a member of Technical Advisory Group (TAG) of President's Council of Advisors on Science and Technology (PCAST) Networking and Information Technology (2006-2007). He was a member of the National Research Council’s committee on 21st Century Cyber-Physical Systems Education (2014-2015). He received IEEE TC-RTS Outstanding Technical Achievement and Leadership Award in 2008. He received an appreciation award from Ministry of Science, IT and Future Planning, South Korea in 2013. His work received the Runtime Verification (RV) Test-of-Time award in 2019. He is ACM fellow and IEEE fellow.