PRINCETON ACM / IEEE-CS CHAPTERS
MARCH 2021 JOINT MEETING

Threat Modeling Research and Machine Learning

Current software engineering research is investigating some connections between security analysis and machine learning – both the potential vulnerability of machine learning applications as well as using machine learning in threat modeling analysis.

This talk will focus on recent threat modeling research as it relates to machine learning. After briefly revisiting our prior threat modeling research, new results from a 2018 student project on machine learning will be discussed. In this project, students assessed the robustness of machine learning models against adversarial examples. Recently, we have been considering the use of machine learning to identify attacker types in specific domains. So, on the one hand, we examined whether machine learning models are vulnerable to attack, and on the other hand, whether machine learning can help to identify attacker types.

Nancy Mead is a Fellow of the Software Engineering Institute (SEI), and an Adjunct Professor of Software Engineering at Carnegie Mellon University. Her research areas are security requirements engineering and software assurance curricula. Prior to joining the SEI, Nancy was a senior technical staff member at IBM Federal Systems, where she spent most of her career in the development and management of large real-time systems. Nancy has more than 150 publications and invited presentations. She is a Life Fellow of the IEEE, a Distinguished Member of the ACM, and was named the 2015 Distinguished Educator by IEEE TCSE. She received her PhD in mathematics from the Polytechnic Institute of New York.

Date: Thursday, March 18, 2021, 8:00pm
Place: **ONLINE MEETING** – **registration required**
How to register:

- Send email to **PrincetonACM@gmail.com**
- OR Register on **Meetup.com** (**http://meetup.com/IEEE-Princeton-Central-Jersey-Section**)

Information: Dennis Mancl (908) 285-1066
On-line info: **http://PrincetonACM.acm.org**

All Princeton ACM / IEEE-CS meetings for fall/winter 2020-21 will be held "on-line". When you register for the meeting, you will receive an email with instructions for how to connect to the talk.

All Princeton ACM / IEEE-CS meetings are open to the public. Students and their parents are welcome. There is no admission charge.