BIML Releases First Risk Framework for Securing Machine Learning Systems

Research will help developers build security into applications from the start

BERRYVILLE, VA, UNITED STATES, February 14, 2020 /EINPresswire.com/ -- The Berryville Institute of Machine Learning (BIML), a research think tank dedicated to safe, secure and ethical development of AI technologies, today released the first-ever risk framework to guide development of secure ML. The “Architectural Risk Analysis of Machine Learning Systems: Toward More Secure Machine Learning” is designed for use by developers, engineers, designers and others who are creating applications and services that use ML technologies.

Early work on ML security focuses on specific failures, including systems that learn to be sexist, racist and xenophobic like Microsoft’s Tay, or systems that can be manipulated into seeing a STOP sign as a speed limit sign using a few pieces of tape. The BIML ML Security Risk Framework details the top 10 security risks in ML systems today. A total of 78 risks have been identified by BIML using a generic ML system as an organizing concept. The BIML ML Security Risk Framework can be practically applied in the early design and development phases of any ML project.

“The tech industry is racing ahead with AI and ML with little to no consideration for the security risks that automated machine learning poses,” says Dr. Gary McGraw, co-founder of BIML. “We saw with the development of the internet the consequences of security as an afterthought. But with AI we have the chance now to do it right.”

For more information about An Architectural Risk Analysis of Machine Learning Systems: Toward More Secure Machine Learning, visit https://berryvilleiml.com/results/.

About BIML
The Berryville Institute of Machine Learning was created in 2019 to address security issues with ML and AI. The organization was founded by Gary McGraw, author, long-time security expert and CTO of Cigital (acquired by Synopsys); Harold Figueroa, director of Machine Intelligence Research and Applications (MIRA) Lab at Ntrepid; Victor Shepardson, an artist and research engineer at Ntrepid; and Richie Bonett, a systems engineer at Verisign. BIML is headquartered in Berryville, Virginia. For more information, visit https://berryvilleiml.com/.

Gary McGraw
Berryville Institute of Machine Learning
+1 703-395-8414
email us here