NEWS

CMU undergraduate harnesses AI to simplify cybersecurity testing

No supercomputer needed

October 23, 2024 | Author: Robert Wang | Media Contact: Robert Wang

Share

Jonathan Gregory, a computer science undergraduate student at Central Michigan University, has been working on a project with Dr. Qi Liao, using artificial intelligence (AI) to make cybersecurity easier. Their research focuses on automating penetration testing — simulating a cyberattack where ethical hackers find weaknesses in computer systems to help secure them before hackers can exploit them.

Instead of using AI models from big companies like OpenAI, Gregory and Dr. Liao used an open-source model called Mistral 7B, running it on a regular laptop with free software. They added specific security knowledge to the AI and successfully had it identify vulnerabilities in a test system. The cool part? It shows you don't need fancy, expensive equipment for AI to be helpful in cybersecurity.

Their goal is to make it easier for people to get into penetration testing, which usually takes years of experience. By automating some of the work with AI, they hope to speed things up and make security testing more accessible for beginners.

The results are promising: the AI can help find weak spots using just a laptop. But while the tech is promising, there's still a long way to go before it can fully automate the process. Plus, there are concerns that hackers could use this same tech for bad purposes.

Their research paper, "Autonomous Cyberattack with Security-Augmented Generative Artificial Intelligence" was recently published in the conference proceedings of the 2024 (Institute of Electrical and Electronics Engineers (IEEE) International Conference on Cyber Security and Resilience.

Next, Jonathan and the team plan to test even more advanced AI models, hoping to improve their system and one day make penetration testing fully automated—helping make cybersecurity faster, easier, and more effective.

VIEW LATEST NEWS

Share

Related News