White House offers prize money for hacker-thwarting AI

August 9 2023

White House Office of Science and Technology Policy Director Arati Prabhakar expects thousands of hackers to test the security and safety of artificial intelligence models at Def Con in Las Vegas.

The White House on Wednesday launched a competition offering millions of dollars in prize money for creating new artificial intelligence

systems that can defend critical software from hackers.

Competitors vying for some of the $18.5 million in [prize money](#) will need to design novel AI systems that quickly find and fix software vulnerabilities in electric grids, subways or other key networks that could be exploited by hackers, President Joe Biden's administration said.

"This competition will be a clarion call for all kinds of creative people in organizations to bolster the security of critical software that American families and businesses and all of our society relies on," the director of the White House Office of Science and Technology Policy, Arati Prabhakar, told a briefing.

To boost participation, the Defense Advanced Research Projects Agency (DARPA) running the competition will put $7 million into funding [small businesses](#) that want to compete, according to the White House.

DARPA is collaborating with AI tech titans Anthropic, Google, Microsoft, and ChatGPT-maker OpenAI, which will provide expertise and technology for the [competition](#), Prabhakar said.

The [challenge](#) is intended to "bring together diverse thinkers from all across the nation to think about how we can use AI to dramatically improve cybersecurity," Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger said in the briefing.

The challenge was announced in Las Vegas at a cyber security conference ahead of a Def Con gathering where hackers will attempt to penetrate various AI systems.

"We'll have thousands of people over two and a half days red teaming leading AI models to see how they stack up," Prabhakar said.

Red teaming is a tech industry reference to testing systems by fiercely attacking them the way hackers would.

"In cybersecurity, there's always a race between offense and defense," Neuberger said.

"We see the promise of AI in enabling defense to be one step ahead."

Biden evoked AI's "enormous" risk and promise last month at a White House meeting with tech leaders who committed to guarding against everything from cyber-attacks to fraud as the sector revolutionizes society.

Standing alongside top representatives from Amazon, Anthropic, Google, Inflection, Meta, Microsoft and OpenAI, Biden said the cutting-edge companies had made commitments to "guide responsible innovation" as AI rips ever deeper into personal and business life.

© 2023 AFP