UC SANTA BARBARA

THE Current

October 24, 2019
Harrison Tasoff

The Changing Face of Cyber Security

Cyber security is constantly evolving as security experts and their adversaries develop and adapt new techniques to their trade. Researchers, companies and professionals from the security community discussed emerging trends in the field during the 8th semiannual UC Cyber Security Summit, hosted by UC Santa Barbara.

“The purpose of the conference is to raise people’s awareness and understanding of the threats and the type of technologies that can defend against those threats,” said Sam Horowitz, the university’s chief information security officer.

Speakers covered topics such as creating, weaponizing and detecting deep fakes, an issue of utmost importance, especially as the presidential race kicks into gear. They also addressed threats to critical infrastructure as well as phishing, the focus of UC Santa Barbara’s Cyber Security Awareness Month campaign this year.

Giovanni Vigna, a professor of computer science and director of the campus’s Center for CyberSecurity and co-director of the Security Lab, delivered the keynote address, discussing how artificial intelligence is changing the security landscape.

“Giovanni is at the leading edge of not only how to detect threats, but how to defend against things that prevent you from detecting threats,” said Horowitz.

According to Vigna, detecting threats and managing network security is challenging and time consuming. People are looking to AI to automate and systematize their efforts while also expanding their scale.

AI can efficiently categorize computer activity and even learn to classify it, streamlining this repetitive work, he explained. It makes anomaly detection feasible at a scale, scope and efficiency unimaginable when the concept was developed in the 1980s. It can even allow security experts to go on the offensive: proactively gathering intel and developing tools to combat attacks their network hasn't experienced yet.

But AI is not a clear-cut solution to our security challenges. "The problem is that these techniques have been developed in domains that are not security," Vigna said. "The most effective machine learning algorithms have been developed in image recognition and natural language processing.

"And guess what, these environments are not adversarial," he continued. "In security, you're applying these algorithms to a domain where there is an adversary who's actually working to resist your attempt to capture their behavior."

Malicious actors are well known for running insidious false-flag attacks that can confuse AI.

"What's more, the adversary can pollute the dataset from which you're learning," Vigna said, like putting out decoys. As an analogy, he mentioned the antics of those who tag inanimate objects as people in images they post on Facebook. This compromises the data the company's software uses to learn.

Incorporating AI into cyber security doesn't change the fact that security workers still need to keep their methods safe from attackers. In fact, machine learning makes this even more crucial, and more difficult.

Researchers have revealed a flaw that allows an individual to steal what a system has learned. It's basically a technique for reverse engineering an AI algorithm based on the answers it provides. "If I can query you as an oracle about what you think about my data and what you've learned, then I can steal anything you ever learned," said Vigna.

"In my lab we're focusing on machine learning in many different ways, and not only to catch stuff," he added. "For example, we use machine learning to identify which parts of the code are more prone to contain vulnerabilities."

The use of AI will not end the challenge of cyber security. AI is just another tool, and its effects will be only as good or as bad as the intentions of the individuals employing it. “The bad guys are using artificial intelligence, too,” Vigna pointed out.

He also warned that the security community tends to assume that anomalous activity corresponds to malicious activity. But this isn’t necessarily the case. Some attacks look innocuous, while other, normal activity looks suspicious. Combining AI anomaly detection with systems set up by humans to distinguish good and bad actions appears to offer the best of both techniques.

Humans are still a vital part of cyber security. “You can elevate the level of discourse using artificial intelligence, but certain decisions still require humans to interpret and create context in order to fully address the threat,” Vigna said. We’re the ones who make the value judgments about what our software finds.

Horowitz echoed this sentiment. “The real reason we’re here today is to equip the humans to be able to function in a system of more sophisticated adversaries and more sophisticated automated defenses,” he said. “In this way, we can protect ourselves and protect our organizations.”

Tags
Artificial Intelligence

About UC Santa Barbara

The University of California, Santa Barbara is a leading research institution that also provides a comprehensive liberal arts learning experience. Our academic community of faculty, students, and staff is characterized by a culture of interdisciplinary collaboration that is responsive to the needs of our multicultural and global society. All of this takes place within a living and learning environment like no other, as we draw inspiration from the beauty and resources of our extraordinary location at the edge of the Pacific Ocean.