UC SANTA BARBARA

THE Current

May 4, 2023

Sonia Fernandez

UC Santa Barbara to lead NSF-funded research institute for next-level AI-powered cybersecurity

Malware. Ransomware. Zero-day exploits. There's no rest when it comes to protection from cyberattacks. And in an increasingly connected world, with expanding digital spaces and access to tools like artificial intelligence, attacks are likely going to become more sophisticated and numerous.

That's why a group of the nation's best computer scientists and engineers have come together to form the National Science Foundation-funded Institute for Agent-based Cyber Threat Intelligence and OperatioN (ACTION), an effort that brings the continuous learning — and now, reasoning — of AI to the constant situational awareness that is fundamental to cybersecurity.

Vigna and UC Santa Barbara colleagues Chris Kruegel, João Hespanha and Ambuj Singh will be joined by more than 20 collaborators from UC Berkeley, Purdue University, Georgia Tech, The University of Chicago, University of Washington, University of Illinois Chicago, Rutgers, Norfolk State University, University of Illinois and University of Virginia.

"The ACTION Institute will help us better assess the opportunities and risks of rapidly evolving AI technology and its impact to DHS missions," said Dimitri Kusnezov, Under Secretary for Science and Technology at the Department of Homeland Security. This group of researchers and their ambition to push the limits of fundamental AI and apply new insights represents a significant investment in cybersecurity defense. These partnerships allow us to collectively remain on the forefront of leading-edge research for AI technologies.”

“UC Santa Barbara is excited to be working at the intersection of artificial intelligence and cybersecurity in a way that is responsive to the needs of and advances the well-being and security of our local, national and global society,” said UCSB Chancellor Henry T. Yang. “This highly competitive award from the National Science Foundation is a strong indication of the cutting-edge and nationally renowned research that our Computer Science colleagues and collaborating universities are already conducting in this area. We are proud that Professor Vigna will be heading this multidisciplinary NSF-funded project that involves several of our campus colleagues and those from peer institutions across the country as they work together on novel and innovative approaches. Heartiest congratulations to our UC Santa Barbara faculty and their collaborators on the overwhelming success of their proposal.”

Stacked Security

Here’s a possible scenario: Cybercriminals gain access to software used by a fictional smart city, a municipality whose water and power distribution infrastructure are automated and integrated. They introduce a software vulnerability that is both complex and too evasive to set off any alarms. From there they use this vulnerability to conduct a supply-chain attack that progressively compromises parts of the system in ways that may seem like glitches and unusual connections, but nothing the threat detection system has been trained to identify. Eventually, they gain access to control systems that allow them to shut down the water and power, effectively paralyzing the city. All this, by seemingly trivial actions through encrypted connections that are unnoticed by the intrusion detection systems.

It's not an entirely hypothetical situation. In fact, such a hacking campaign was orchestrated in 2021 that compromised several U.S. government agencies by breaching applications monitoring software created by vendor SolarWinds. This type of attack, according to the researchers, is why a more sophisticated type of AI-powered cybersecurity is needed.

“There’s this concept of an AI ‘stack,’” Vigna explained. “Imagine multiple layers of functionality that support artificial intelligence in various ways, such as reasoning, learning, strategic planning and interaction.” This stack will enable the creation of autonomous “agents” that will be able to not only identify a potential attack but also the attacker, and can also mount a response and conduct recovery.

The collaborators will begin by conducting research along four main thrusts: learning and reasoning with domain knowledge; human-agent interaction; multi-agent collaboration and strategic gaming and tactical planning. These research areas act as the foundation of knowledge that can grow to handle large data sets, while extracting meaning and promoting inference and reasoning based on the best techniques available.

“Human and AI agents process information in different ways: How they recognize threats, deal with underspecified systems, learn unsecure behaviors from history and predict future consequences of actions,” said Singh, whose research involves AI/human interactions. Merging AI with human expertise is a best-of-both-worlds security scenario, he said. “Building a joint human-AI system that complements each other with capabilities, such as presenting a human expert with risk-reward options derived from an AI-learned model, are some of the ways in which the institute will lead the frontier of future research in AI-cybersecurity.”

Another novel approach the institute will take toward cybersecurity stems from the realization that security systems can be viewed as a stage where multiple agents interact, each with their own motivations, goals and abilities, Hespanha added. “Designing security systems must involve reasoning about how the actions of one agent will affect the behavior of another agent,” he said. “This type of reasoning is needed to make sure that whatever protection mechanisms we deploy to protect our system against one type of attack do not unintentionally create a completely new vulnerability.”

Importantly, the foundational AI research stack involves a layer of defense, which goes beyond dealing with anticipated cyberattacks, into understanding the context of the attack and the attackers in a rapidly evolving, high-volume landscape of information.

The AI research informs the cybersecurity element, in which agents are developed for the assessment, detection and attribution of attacks.

The rubber meets the road in the final security thrust, which focuses on the analysis and containment of cyberattacks, as well as the planning and adaptation of response and recovery. This includes the knowledge gained from the activities of the assessment, detection and attribution agents to predict and contain attacks, to fix and restore operations where possible, and to learn hacking strategies that could be used for future attacks and rare methods of cyber-intrusion.

Vigna likens the overall strategy to the defense used in soccer, in which the goalkeeper must observe the strategies and tactics of the opposite team and decide where to concentrate defense efforts.

“You cannot cover everything 100% all of the time, but having these hints allows you to focus or change your security posture,” he said. The use of AI allows the defenders to reason at large scales, predict how the attack might unfold and respond rapidly.

In addition to developing next-generation cybersecurity, the ACTION Institute will implement programs to engage K-12 students as well as undergraduate, graduate and postdoctoral students for education and workforce development, with an emphasis on outreach to underrepresented communities.

“We have an incredible need for people who know how to use security and know how to interact with and program AI,” Vigna said. Just as crucially, the institute will create a network of industry collaborators who can apply ACTION’s methods and research results to real-world settings.

And the results might even go beyond cybersecurity, with the methods and agents developed for this project able to inform other areas with large and rapidly evolving datasets, such as medical diagnostics and epidemiology. “That would be one of our metrics for success,” Vigna said.

Tags
Artificial Intelligence

Media Contact

Sonia Fernandez

Senior Science Writer

(805) 893-4765

sonia.fernandez@ucsb.edu

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.