Mizzou Cyber Range to Focus on Cyber Pretense Strategies

September 16, 2020
in CERI, Computer Science, Cyberdefense, Cybersecurity, Electrical Engineering & Computer Science, Research, Research Centers & Programs
by Janese Heavin

Hackers are getting smarter about ways to steal sensitive information from the cloud. Now, a new “Mizzou Cyber Range” will train the next generation of cybersecurity professionals to fight back using cyber pretense strategies.

Armed with new grant funding from the National Security Agency, Prasad Calyam and his team are building the Mizzou Cyber Range through the MU Center for Cyber Education, Research and Infrastructure. Calyam is director of the center, an associate professor of electrical engineering and computer science and Robert H. Buescher Faculty Fellow.

A cyber range is a virtual environment that allows students to practice defense strategies in realistic, but isolated and safe settings. The military, government agencies and large companies such as IBM and VMware have cyber ranges to keep up with ever-evolving hacking techniques.
“Commercially, they can cost hundreds of thousands of dollars,” Calyam said. “We are building ours in house. It is a minimum platform now, but with the NSA grant, we will develop more realistic scenarios and advanced cyber defense learning exercises for hands-on training.”

### A New Paradigm of Cyber Defense by Pretense

The Mizzou Cyber Range will build on Calyam’s research into a new strategy known as cyber defense by pretense.

The techniques used in this strategy are collectively named as ‘Dolus,’ a Greek word for the spirit of trickery. The Dolus techniques are designed to trick hackers into thinking they’ve successfully gained access to sensitive information, when in reality, the compromised information goes into a quarantined state while the real data is shifted to a better-protected system.

“The attacker is cornered into cutting ties with a compromised asset because it seems to show no benefit and attacker feels that too much time and effort is being spent on communicating with the targeted asset,” Calyam said. “In the best case scenario, Dolus techniques make the attacker feel it’s not worth the time, effort to target the asset, and will make the attacker just buzz away.”

If the attacker doesn’t, the Dolus techniques distract the attacker long enough for a company to deploy stronger defense strategies to shield the information.

### Educational Modules Becoming Available

The first phase of the grant will allow for research into pretense strategies to develop more sophisticated Dolus techniques. Specifically, researchers are learning to better protect media content, financial information and medical records.

“These decoys will be realistic for gaming, video streaming, health care and financial applications,” Calyam said. “Then, in the second phase, we will be converting research-inspired products to basic and advanced learning modules for the Mizzou Cyber Range. Students who use the learning modules will be trained using a
‘learn-apply-create’ pedagogy. This will help students ultimately become critical thinkers and problem solvers for cyber defense scenarios pertaining to real-world applications in consumer media, manufacturing, finance and healthcare.”

Already, the Mizzou Cyber Range has four learning modules up and running that Calyam is using in his cyber defense class this semester for undergraduate and graduate students. Earlier this summer, one of the learning modules was adapted to host a virtual “Hacker Tracker” summer camp for high-school students to learn about coding, cloud computing and cybersecurity.

Eventually, these modules will be openly available to students across campus and ultimately to instructors and students at any university. As part of the National Security Agency project efforts, the project team has plans to disseminate the Mizzou Cyber Range outcomes via workshops and tutorials to the NSA-designated National Centers for Academic Excellence University Community.

“Mizzou is hosting the cyber range we’re currently implementing on NSF cloud infrastructure, but it can be downloaded by other people and deployed on their own hosting infrastructure or on public clouds such as Google Cloud,” said Songjie Wang, a cyberinfrastructure engineer for Calyam’s center. “Students can register and log in, then choose which learning modules they’re interested in. We’ll also have step-by-step instructions where people can create virtual machines and software-defined network controllers to execute the labs and learn cyber defense by pretense skills. They will get real-time feedback on their learning in terms of badges. And a relative peer standing via a ranking dashboard will motivate them to try harder to improve their skills.”

Read more about Calyam’s research into pretense by defense strategies here.  

---

https://engineering.missouri.edu/2020/09/mizzou-cyber-range-to-focus-on-cyber-pretense-strategies/