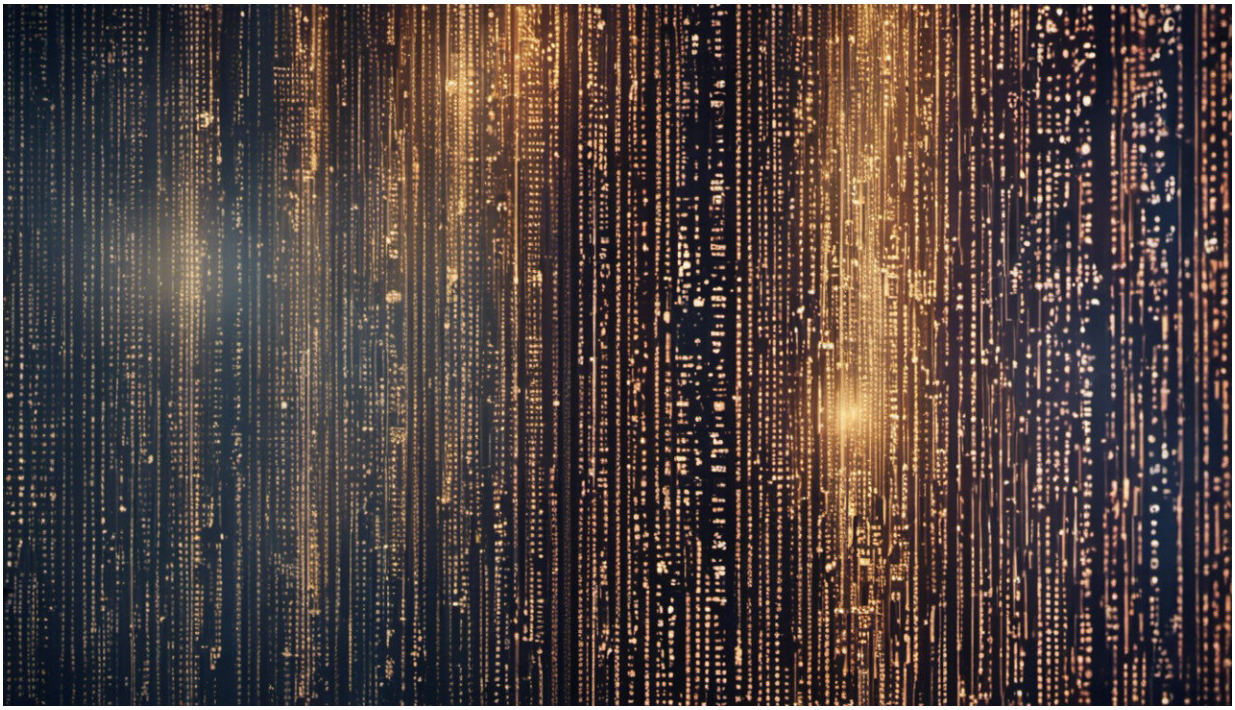
Cybersecurity research looks to guard networks from 'insider threats'

October 16 2015, by Robert J. Margetta



Credit: AI-generated image (disclaimer)

Even the best-protected, most sensitive computer networks resemble castles: They have walls to ward off outside threats, but their interiors are full of weak points. That's why the "insider threat"—someone within a system who, out of malice or naiveté puts a system at risk—is considered one of the most serious risks in the cybersecurity world.

"The insider threat is clearly a challenge for organizations, because most countermeasures were developed for external attacks," says Jingguo Wang, information systems and operations management professor at the University of Texas at Arlington.

Wang and H. Raghav Rao, a management science and systems professor at the State University of New York at Buffalo, are working to help organizations map out the spots most vulnerable to insiders and, eventually, develop countermeasures aimed directly at those threats. With support from the National Science Foundation's Secure and Trustworthy Cyberspace (SaTC) initiative, they are conducting one of the first large-scale studies of how insiders behave on a network that allows them to view sensitive information.

"This is a first step to studying the insider threat," Wang says.

Critically, it's also a step that doesn't distinguish between any potentially threatening insider's motivations. The research team is looking for vulnerabilities that could be exploited by spies and criminals as well as those who could jeopardize a company through negligence—the equivalent of someone forgetting to lock the office doors at night, allowing a burglar to sneak in.

"Some systems might be vulnerable because they have a lot of value or because people might be curious," Rao said. "The point is that people are looking around in areas where they shouldn't."

For the project, Wang, Rao and their collaborators partnered with a financial institution, which gave them a rare resource: anonymized access records for every interaction on their computer networks by several thousand internal users.

The researchers focused mainly on behavior logs, anonymized so they

could follow employees' actions without knowing who they were. By studying almost half a year's worth of data, they were able to see how the institution's staff behaved on its network. Some of that behavior included occasions when employees were able to access information that should have been off-limits.

Those incidents of improper access could involve flaws in system security, or problematic access controls that allowed people to get into areas of the network that should have been walled-off to them. For example: some companies store private customer data that only a small subset of employees is supposed to handle. A malicious attacker could obviously misuse that information. But even an insider with no ill-intent could cause a company serious problems by copying that data to an unsecure location or forwarding it to someone else.

Rao and Wang said a financial institution was the perfect setting for modeling a computer network's vulnerability to insider threats. These companies are exactly the types of environment where insiders could cause catastrophic damage, intentionally or unintentionally.

"They're highly reliant on information technology for the work they do," Wang said. "And they have information—customer data, account data—that's sensitive and valuable."

The team has completed stage one of their research, assessing the risk levels of different types of information assets and defining the vulnerabilities in a system that might serve as opportunities for predators. Stage two, currently in progress, involves looking at the circumstances in which inside users are likely to wind up exploring places in a network where they shouldn't be allowed.

Eventually, Rao and Wang say, their research could help build access-control tools, as well as means to effectively detect insiders poking

around forbidden areas.

Getting to that point won't be easy—the researchers found it was difficult to even determine how insiders might approach information assets. But rigorous research designed to understand human behavior can help lay the foundation for systems that could place checks on insiders, taking a well-known threat and offering some solutions.

"Lots of people point to insider threat as a big problem," Rao said. "Not too many people are familiar with what to do about it."

Provided by National Science Foundation