Using Anomalies to Defend Against Insiders

SALVATORE J. STOLFO

Professor of Computer Science

If your credit card company ever called to confirm a purchase, you have entered Salvatore Stolfo's world. Stolfo specializes in detecting anomalies, events that stray too far from expected patterns. In addition to fraud, anomaly detection can be used to monitor engineered systems, sensor networks, ecosystems, and computer security.

Stolfo entered the field after inventing an algorithm that let marketers merge lists of consumers and purge bad records. "I realized I was aiding and abetting people who pierced personal privacy. It was an ethical dilemma," he recalled.

His interest in privacy led to cybersecurity and eventually to the study of insider attacks. "Most security breaches are the fault of the humans. Someone didn't implement something, or stole an identity, or had a grudge against an organization," Stolfo said.

This differs from most security research, which aims to keep out hackers. University researchers are more ambitious, developing inherently secure programming languages and self-repairing systems. "These are important aspects of security, but they don't matter if your adversary is already inside," Stolfo said.

"There are many different types of insiders, and they all do things in different ways," he added. "We think of it as a chess game. What if insiders can control system access? If they can blind the system to their actions, they can get away with anything. We want to stop them."

The most common type of insider threats is unintentional users. They may disable security measures to do their job more easily, or inadvertently push two buttons and erase a day's work. "These are the most prevalent and least dangerous insiders," Stolfo said.

Masqueraders include credit card thieves with stolen credentials. "The credentials make them insiders," Stolfo said. He works with banks to model consumer transactions. "We're always looking for ways to use more data to find problems sooner," he said.

Maliciously intentful insiders use their own credentials to copy secret government or corporate documents, steal money, and even sabotage the system. Highly privileged insiders have a similar agenda, but they are the ones responsible for detecting other intruders.

To foil these intruders, Stolfo looks at how their behaviors vary from company norms. By plotting how users interact with software and documents, he hopes to find patterns that suggest malicious intent. He has also developed decoys to ensnare bad guys.

"Ultimately, we want to define metrics for what it means to be secure," he said. "Then we can start to build a science of security."

B.S., Brooklyn College, 1974; M.S., New York University, 1976; Ph.D., NYU, 1979