PHOTO ILLUSTRATION BY JOHN HARMAN/STAFF

networks but not people and data," he said. "The insider threat is all about people."

Reidy, Swift and Caputo discussed the effort at a defense industry convention in Washington, D.C., on April 4.

The 'Pre-Crime' division

Private industry and the Defense Advanced Research Projects Agency are among the entities that have technological solutions in various stages of progress.

Raytheon's SureView software captures any security breach or policy violation it's programmed to find and can "replay the event like a DVR," for a local administrator or others to view, according to the company's website. The software's trigger is programmable and can be set to any behavior considered suspicious or not.

Working with Raytheon, a group of cadets from the U.S. Military Academy at West Point last year conducted a simulation of an insider attack at a forward operating base. Cadets looked at how to fine-tune the way SureView detects potential threats and eliminate false positives for innocuous behavior, said West Point computer science professor Col. Greg Conti.

"It was very powerful, very flexible and allowed you to monitor with very fine resolution activities on the desktop, and the real trick becomes how you detect anomalous behavior," Conti said. "Predictive models are kind of the holy grail. When you see that no one else has done something but bad guys, you can start being predictive."

At SAIC, which is testing a behavior analytics system, Beard likened behavioral modeling to the Pre-Crime unit from the science fiction movie "Minority Report." Instead of using psychics to stop crimes before they occur, the software would be programmed to detect behavior that has preceded malicious acts in the past.

In real life, researchers are examining the behavior of malicious insiders to see what actions they took before they acted out. That in turn would be used to teach the software what behavior to flag.

"We may want to administer policies that say, 'Gee, gosh, why do you really want to download 300 [megabytes] of stuff or a gig of data in a single session,'" Beard said. "We look for the antecedents of behavior that would suggest based on past history that bad things are going to take place."

That could be visiting restricted websites, requesting access to information outside of one's job description or asking for large amounts of storage media — or likely some combination of the above. Individually, the actions may not seem problematic, but combined and in the context of human intelligence, they could raise alarms.

"We start taking those things and recombining them to say, 'What is going on in the environment?'" Beard said. "Any one of those things independently can be totally innocuous and innocent, but when you put them together — plus their job, plus their access, plus the things they are working on — you may be looking at it as a counterintel kind of thing."

Drawbacks and challenges

Cybersecurity expert Michael Tanji, an Army veteran who has spent nearly 20 years in the U.S. intelligence community, said he sees potential drawbacks and unanswered policy questions. He asked how the Army would implement such technology without unintentionally stifling cross-disciplinary collaboration among soldiers.

Knowing they are being monitored, personnel might avoid enterprising or creative behavior for fear it would be flagged by monitoring software, he said.

Tanji also predicted the technology would come at a considerable financial cost, both to warehouse the data collected by the software and to pay the added staff needed to monitor the reports it generates.

"A brigade-sized element that uses computers on a regular basis would probably need a company-sized element just to keep up with the data that comes in," he said.

Reidy, the FBI official, said such concerns were valid. Because software may report benign behavior as malicious and vice versa, he cautioned against using technical solutions alone to solve insider threats.

"After a major incident, and no offense to any vendors, but the charlatanism always goes up," he said. "It's absolutely amazing how many phone calls I get from people who say they have solved the WikiLeaks problem or solved this or that problem. Everybody's got to eat, but it's simply not true."

Finding bad behavior amid the vast sea of keystrokes, downloads and Web browsing on military computers is no easy task, DARPA acknowledges.

A DARPA solicitation for Suspected Malicious Insider Threat Elimination, or SMITE, announces it is attempting to recognize "moving targets" — telltale patterns of behavior amid "enormous amounts of noise (observational data of no immediate relevance)."

The program, based in behavioral science, would have to distinguish anomalous behavior from normal behavior, and deceptive and malicious behavior from anomalous behavior, the solicitation reads.

A solicitation for another program — Anomaly Detection at Multiple Scales, or ADAMS — uses accused Fort Hood shooter Maj. Nidal Hasan to frame the problem. It asks how to sift for anomalies through millions of data points — the emails and text messages on Fort Hood, for instance — using a unique algorithm, to rank threats and learn based on user feedback.

The program is trying to look beyond computers to spot the point when a good soldier turns, whether that means homicidal or suicidal or ready to dump stolen data.

"When we look through the evidence after the fact, we often find a trail — sometimes even an 'obvious' one," the solicitation states. "The question is, can we pick up the trail before the fact, giving us time to intervene and prevent an incident? Why is that so hard?" □

AKO splits into two to increase security

By Joe Gould
jgould@militarytimes.com

To become more secure, the Army's intranet, Army Knowledge Online, has been divided into two versions: one full of sensitive but unclassified information for soldiers, and another unrestricted version for reservists, retirees and family members, Army officials said.

Army Cyber Command ordered the move to stave off potential attacks from would-be hackers who scan AKO for vulnerabilities "constantly," said Army Cyber Command spokesperson Jennifer Downing via email.

Before the change, AKO was getting attention from Army Cyber Command for security breaches, and now it is getting accolades, AKO Product Director Kenneth Fritzche said.

"The weakest link on AKO was the user who winds up having his access information compromised, letting some bad guy from some nation-state halfway around the world log in and see what this legitimate user can see," Fritzche said. "It was a constant battle finding them and deactivating those accounts."

The partitioning of AKO, which took effect March 28, means users may only access sensitive data if they have a military-issued smart card, the Common Access Card, and a computer equipped with a CAC reader.

Users without a CAC may log in using a username/password combination. They will no longer have access to many documents considered "For Official Use Only." The term applies to information not available under the Freedom of Information Act, such as documents that contain personally identifiable information or that might potentially hinder operations.

What is designated FOUO is up to the users, Fritzche said. Content uploaded by users who log in with a CAC is classified FOUO by default. Content uploaded by users who log in with a username and password will default to non-FOUO.

Fritzche acknowledged that this arrangement has created hardship for some users who have to do Army business but are not issued CACs.

However, most of the few complaints he has heard have come from users who now need to obtain a CAC reader for their home computers. Fritzche said AKO's CAC Resource Center offers help setting up CAC readers, and the software is free.

Although the decision ultimately limits access to information, Downing asserted there would be minimal impact on users.

"Our goal was to reduce the residual risk to the lowest possible level on the AKO file shares and not interrupt or break any critical business processes," she said. "We believe our team approach to this problem has been successful and we will continue to monitor this transition for operational impact." □