SAND2008-7887P

Reviewed by: Navid Jam, Corbin Stewart, Ed Talbot, Len Napolitano, LeAnn Miller

**National Security Agency honors Navid Jam for videoconferencing security work**
By Patti Koning

This fall, Navid Jam (8965) was chosen as one of three finalists for the National Security Agency's (NSA) 2008 Frank B. Rowlett Award, which recognizes outstanding organizational and individual excellence in the field of information systems security.

“Navid represented a team that found critical vulnerabilities in common off-the-shelf video conference systems that are widely used by government agencies,” says Len Napolitano (8900), director of computer science and information systems. “They identified the problem and then Navid carried the message outside the Lab. Now the government is using their work as a standard, to the point that they are holding up procurements.”

Navid was awarded an honorable mention for his contributions, but this is a case in which being a finalist is truly a remarkable achievement. The Rowlett Award typically stays within the armed services. Navid was the only non-uniform individual nominee this year and there has never been an individual winner from outside of the Department of Defense (DoD).

Navid says that at the ceremony he was surprised and pleased by the positive feedback he received from people in high-level positions with a variety of government agencies. “Seeing the breadth and depth of customers and the impact we have had was rewarding,” he says. “I think this shows the recognition of the important role National Laboratories play in information assurance and cyber security for the nation and also recognition of this new, important area in which a National Lab has had an impact, across many areas including the government, vendors, and the standards community.”

Navid and Len attended the awards ceremony in Washington, DC on Oct. 30. Before the ceremony began, all six nominees sat down privately with NSA director LTG Keith B. Alexander to discuss their work. The ceremony itself featured a four-minute video on the work of each nominee.

Sandia’s videoconferencing work began four years ago as an internal, operational project. Corbin Stewart (8947), a technologist in the Videoconferencing and Collaborative Technologies department, discovered a security issue with videoconferencing software. “I was trying to update a feature and discovered that it did not require authentication,” he says. “That was a red flag.”

Jim Berry, (8944), who was manager of the department at the time, decided the potential security issues surrounding videoconferencing were worth investigating. Using funding from Jim’s department, Corbin, Steve Hurd (8965), a Sandia computer scientist and program manager for lab’s Center for Cyber Defenders (CCD), and a group of college interns in the CCD initiated a risk analysis nearly four years ago that focused on commercial codecs. Navid was one of those interns.

“He really stood out, and took the lead to advertise these types of vulnerabilities in embedded communication applications,” says Corbin. “It’s gratifying to see that the work we have done is benefitting so many others.”

He adds that while one reason for turning to the CCD was because as interns, they were inexpensive, it wound up bringing new, fresh insights to the problem.

Another former CCD student, Elliot Proebstel (8965), has also contributed to the work. “We are really impressed with Elliot,” says Corbin. “During his second summer with the CCD, he was able to circumvent access controls on the evaluation device and recover the administrative password in only a few hours.

Sandia’s primary concern was analyzing and mitigating security risks on its own network, risks that were addressed and rectified immediately after security holes were found. The research team evaluated hardware from several industry sources. After analyzing the devices and related hardware and software, the team developed “attack trees” (step-by-step tactics) and performed a variety of attacks in order to demonstrate vulnerabilities. The objective was to attempt system compromises, independently assess vulnerabilities that were found to exist, and develop “best practices” and tools to aid users.

This internal project developed into a full-fledged program with WFO funding from vendors of videoconferencing and embedded communications systems and government agencies using such systems. “For external customers, we approach the problem from two perspectives,” says Navid. “Sandia acts as a consultant for various government agencies, advising them on architecture, setups, and potential vulnerabilities. We also work with vendors to help them analyze some of the risks and vulnerabilities that are apparent with their systems.”

Getting to this point was not easy. Navid recalls several years when no one would take him seriously. “When we raised these concerns, they fell on deaf ears initially. We didn’t give up and began sharing what we had learned with our government contacts and partners. We felt strongly that this was an important issue that needed to be addressed, not swept under the rug. No one was concerned about it and the vendors weren’t listening to Sandia. That was something that was putting the nation at risk.”

Mitigating the risks is actually fairly simple. A problem, explains Corbin, is that people often don’t think of these videoconferencing devices as computers, and having the same kind of web services and ftp services as your computer, and as a result, the same need for security.

“Some vendors continue to tout the latest features, benefits, and productivity gains that videoconferencing technology offers, but not enough thought or effort has been placed in securing these devices,” says Navid. “The irony is that it isn’t rocket science. It’s really akin to home PCs. By now, most people connected to the Internet understand the need to have anti-virus software. Similarly, people responsible for videoconferencing events should understand that a Video conferencing device operates much like a PC and therefore requires protection such as a firewall program. But there are a lot of companies out there who overlook that need.”

He began giving talks at DOE, DoD, and public internet security conferences. Basically, he says he talked to anyone and everyone that was willing to listen about the risks of embedded collaboration systems. A breakthrough came in 2006 at a Sandia Red Team conference, when he met with the NSA Red Team and shared the issues Sandia had identified and the tools and techniques to mitigate those issues.

“The NSA Red Team has been a terrific partner. They really championed our cause and helped us gain fairly high visibility throughout the government,” says Navid. Recently the Defense Information Systems Agency (DISA) released Security Technical Implementation Guide (STIG) for videoconferencing based on Sandia’s work.

Sandia set up the Center for Collaborative Security (CCS), to educate companies and organizations about videoconferencing vulnerabilities and the need for industry-wide fixes. This virtual team is comprised of a wide swath of computer and security experts, including network operators, vulnerability researchers, IT architects, and systems analysts and spans many directorates across Sandia, including 8900, 8100, and 5600.

The CCS conducts research and development on security issues related to collaboration systems such as distributed information sharing applications and Instant Messaging (IM) solutions. It provides basic tools and information on security vulnerabilities found in all types of collaboration devices, as well as best practices to enhance the security of collaborative systems. The CSS also provides a method for external partners to establish Work-for-Others business agreements with Sandia, which can perform company-specific evaluations and assessments.

Navid continues to drive broad acceptance of Sandia's work, working with standards bodies and meeting with more potential customers.

He's enjoying his role, which could be described as a spokesman, salesman, interface, or as he jokes, "just the pretty face." Navid says his key strength is being able to bridge both the technical and business aspects and understanding all the issues that come to play—understanding how the business works.

--30—