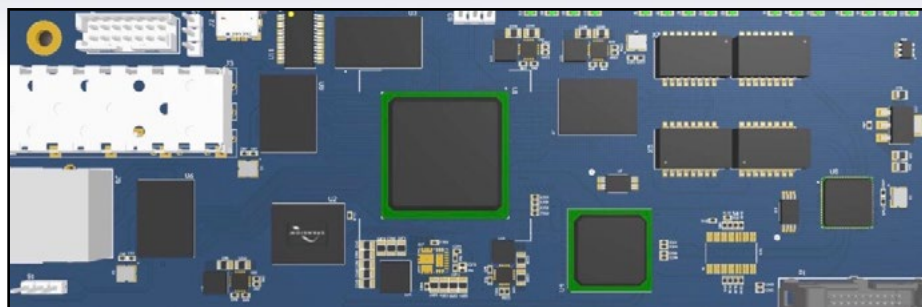




SandTech Licenses Air Force Patent, Forges Potential R&D Agreement



IRIS consists of an Enhanced Ethernet Network Interface Card to interface with a host and a network, which includes an internal network interface controller and a Field Programmable Gate Array (center, green outline) configured to intercept data from the host and/or network, preventing a multitude of attack methodologies such as advanced malware, spyware, and botnets. (Image courtesy of 318th Cyberspace Operations Group, Joint Base San Antonio-Lackland)

WRIGHT-PATTERSON AIR FORCE BASE, Ohio — When the average consumer thinks of cybersecurity, the immediate thought usually centers around anti-virus programs, malware protection, or other cyber defense software designed to protect their computer or network from outside threats. A quick check for operating system capability and the star rating from laboratory testing seemingly becomes the deciding factor of purchase. One question that may be overlooked is what happens if the threat bypasses the software? As cyber threats evolve and malware detection databases are updated, one thing that remains constant when renewing an annual subscription is the computer's hardware. The question now becomes how do I protect my computer inside the firewall?

With an ever-increasing obsession by adversaries and hackers to disrupt the DoD network infrastructure, a team of Air Force engineers in San Antonio, Texas designed a security system that operates as an independent hardware interface to the host system to combat their attacks. The Integrated Remote Interrogation System, or IRIS, was invented by Jim Collins, Robert Kaufman, and Chet Wall, and is comprised of software capabilities operating on systems which reside on the underlying hardware device known as the Enhanced Ethernet Network Interface Card (EENIC).

"IRIS is a low-cost, re-programmable embedded system technology designed to combat the advanced persistent threat (APT) within segmented/deployed network enclaves," explains Wall. "Selected hosts and servers within distributed network enclaves will be outfitted with this APT detection and reporting system."

Wall stated there was a need for network defense at the host where enterprise defense and protection were not available. These enclave networks regularly provided the majority of mission support within deployed regions, but were unprotected. IRIS contains the capability to enable that protection and also provide situational awareness to bigger enterprise defense analysts and assets.

Kaufman, who was the director of the Air Force Computer Emergency Response Team (AFCERT) in the early 2000s, understood both the threat and shortfalls in Air Force Enterprise Defense. He had several discussions in 2011-2012 with Collins and Wall on how best to overcome one of their critical enclave defensive shortfalls against APTs.

"When I was working in the AFCERT," says Kaufman, "Chet and Jim had been key to working several operational support efforts, so we had a close relationship on network defense improvement visions. After some initial brainstorming, I gave direction to Chet and Jim to develop what ended up being the IRIS prototype. Jim was the principal investigator, Chet and I provided technical process refinements and operational perspective to bring the project from idea to prototyping."

Those project ideas and prototypes evolved into patent application filings as Host-Based, Network Enabled, Integrated Remote Interrogation System with the United States Patent and Trademark Office (USPTO) in 2015 and 2017, and became official patents in 2018 under USPTO numbers 9,860,258 and 10,104,096.

Wall and Kaufman, who work with 26th Cyberspace Operations Group within the 688th Cyberspace Wing (688 CW) and 318th Cyberspace Operations Group within the 67th Cyberspace Wing (67 CW), respectively, are on the verge of seeing their idea become an actual product. A Patent License Agreement (PLA) was signed in September between the 67 CW and a San Antonio cyber-security company named Sandoval Technology Solutions, or SandTech, to allow full productive use of IRIS.

"The goal is to successfully transfer the IRIS technology to SandTech," explains Eric Rosenberg, 67 CW's Chief of Cyber Intellectual Property Law. "First, we signed the nonexclusive patent license agreement with SandTech on September 9, 2021, and we are very close to finalizing a Cooperative Research and Development Agreement (CRADA) with SandTech, which would facilitate ongoing support for the integration of IRIS into SandTech's products."

Continued >



Rosenberg spearheaded the wing's previous two PLAs earlier this year, which were the first of such agreements in the 16th Air Force's history, and is the driving force behind this first-ever hardware PLA in their history.

"We reached the decision to commercialize IRIS after considering various equities and balancing risks and benefits. Especially because IRIS is not being used operationally, it makes sense to license such defensive cyber technology. It is a morale booster for the wing's inventors and developers when the fruits of their labor are utilized for the betterment of society and are not sitting on a shelf," Rosenberg added. "Plus, 67 CW will share the patent license agreement's royalties and revenues with the inventors as well as other personnel who have increased the technical value of the technology. These payments will further incentivize continued cutting-edge innovation and participation in technology transfer activities."

SandTech is a growing Development, Security, and Operations/Information Technology services provider to the Air Force, headed by Chief Executive Officer Jose Sandoval. The company focuses on leveraging their unique experience in supporting Air Force cyber protection teams, cyber weapon systems sustainment, and weapon system development to create and deliver effective, sustainable protective effects to their customers through and from cyberspace.

Greg McCulley, SandTech Chief Operating Officer, participates in the Air Force's Small Business Innovation Research and Small Business Technology Transfer program and, in doing that research, discovered the patent for the IRIS technology and believed it could augment his company's capabilities. "We discovered that Project IRIS fit our requirement quite well," said McCulley. "The Air Force will benefit from our investment in personnel, research, and testing activities; our commercial customers will benefit from the enhanced cyber security capabilities developed."

"SandTech already employs a custom cyber security appliance in use across our commercial IT customer base. With 67 CW, we plan to incorporate novel technology in a way that bolsters and extends the capabilities of our current hardware offering," insists McCulley.

Rosenberg agrees, believing the partnership bears potential to benefit DoD and civilian consumers alike. "The commercialization of IRIS may help protect U.S. companies and consumers in an environment that features growing threats from malicious cyber actors. In addition, under the likely CRADA, the Air Force will be able to take advantage of improvements that SandTech makes to IRIS's code."

The inventors view this as a vast step forward, describing how the years of research and development may not have been viewed as a high priority by some government entities in the decade leading up to this PLA and pending CRADA.

"The only roadblock to the capability was it was ahead of its time in receiving advocacy and funding. The concept began exploration in 2011 and [was] difficult to acquire necessary funding and deployment considerations in competing with other priorities. This capability, fairly inexpensive in procurement, could have saved more costs, eliminating many of the big network enterprise integration challenges still in quest for solutions today. IRIS was never deployed within the Air Force," Wall contends.

"Honestly, I believe the IRIS concept was far ahead of any operational concept the Air Force was exploring or contemplating," adds Kaufman. "The Air Force requirements process struggles with innovative leading-edge changes and

IRIS has suffered, within the Air Force, because of that. The recent Chief of Staff of the Air Force's 'Accelerate Change or Lose' culture gives hope that ideas like IRIS can benefit Air Force processes, but we have a requirements/acquisition system mired in the industrial processes of the 1960s. IRIS definitely had immediate use in commercial sectors; so, early on, Collins, Wall, and I discussed the patent and how we might transfer the technology to commercial partners to overcome the lethargic Air Force requirements/acquisition process."

That discussion led them to the Air Force Technology Transfer and Transition (T3) Program, which makes transferring Air Force-derived technologies to the private sector for development and commercialization easier and more accessible. PLAs and CRADAs are two of the mechanisms available through T3 and are held in high regards by Rosenberg. "67 CW views technology transfer as a retention tool for our highly skilled 'software craftsmen,'" he states. "Technology transfer mechanisms such as patent license agreements and open-source software licensing are great opportunities for Air Force developers to receive much deserved public recognition for their hard work, which is often classified."

Rosenberg also offers a few words of wisdom to those interested in a partnership through the T3 program. "First, I would recommend trying to be flexible. Second, I would recommend bringing your attorneys into the process relatively early so they have enough time to understand these types of agreements, which may look different than the agreements they usually see in the private sector."

McCulley offered a similar sentiment, stating, "understanding the legal vernacular took some focus and attention." According to him, SandTech's journey to this point involved a few challenges but was pretty painless overall. He advises anyone interested in partnering with the Air Force to take advantage of the opportunities offered by T3 and do as much research as possible.

"Companies or organizations should maintain healthy and frequent communications with Air Force organizations to best understand their requirements," McCulley suggests, "Be able to spot opportunities for the Air Force to leverage the speed of innovation that maturing small businesses offer. Communication was a key enabler to our success in establishing this agreement."

Kaufman recognizes and appreciates the T3 program, but also extends gratitude to Lt Gen Timothy Haugh (then Colonel Haugh) and Col Michael Convertino, the two group commanders who encouraged him and his team to be persistent. "Colonel Convertino gave us the initial top-cover to push forward on the IRIS innovation and Colonel Haugh gave us the right words of encouragement when we encountered naysayers. They always embraced innovation despite the risk adverse nature of our Air Force," he concluded.

Patent License Agreements are offered through the Air Force Research Laboratory's Technology Transfer and Transition (T3) program office, enabling inventions developed and patented by Department of Defense laboratories to be transferred to the private sector for full productive use. Cooperative Research and Development Agreements enable research collaborations with private sector companies, universities, industry associations, and other organizations. A comprehensive suite of T3 mechanisms for partnering with industry and academia are offered through the office. To find out how you can partner with the T3 Program, please visit <https://www.aft3.af.mil>.



PARTNERING WITH A SHARED VISION

U.S. AIR FORCE TECHNOLOGY TRANSFER & TRANSITION PROGRAM OFFICE
AF.TECHTRANSFER@US.AF.MIL | [HTTPS://WWW.AFT3.AF.MIL](https://www.aft3.af.mil)