SAND2016-8694C

Vincent (Vince) Urias

Vincent (Vince) Urias was selected as a 2016 Luminary Honoree for the Hispanic Engineer National Achievement Awards Conference (HENAAC) awards. Luminary honorees represent professionals in science, technology, engineering and mathematics who initiate, collaborate and lead key programs and research within their companies. These individuals have made significant contributions to the Hispanic technical community.

Vince began his work at Sandia as a high school student intern working in the Lab's Computer Support Unit. He earned his B.S. in electrical engineering and technical communications and his M.S. in computer science from New Mexico Tech. He is currently pursuing his Ph.D. in computer science at New Mexico Tech. As a principal member of the technical staff in the Cyber Analysis Research and Development Solutions Department, Vince has made major contributions to Sandia's cyber defense programs, especially in the simulation of complex networks, in developing innovative cyber security methods, and in designing exercise scenarios that test the limits of current network security. He has achieved notable success in the research and implementation of large-scale modeling and simulation environments (Emulytics™). Vince's research is well known throughout the research community, where his technologies are used during exercises to directly support the warfighter and the security of our nation. Vince collaborates with colleagues across national laboratories, defense contractors, and the armed services.

Vince serves on the board of directors for Creative Programs of New Mexico and is the stewardship chair for the United Way of Central New Mexico's Hispano Philanthropic Society. He's also driven a number of pilot project adoptions for Big Brothers, Big Sisters, the Boys & Girls Clubs, and the National Hispanic Cultural Center. Vince has worked with over 25 student interns, providing individual support toward their desired professional goals.

Vince will be formally recognized at the Great Minds in STEM (GMiS) / HENAAC conference in Anaheim, CA on October 7th.

Sandia National Laboratories Cyber Team Recognized by US Secretary of Navy

Five Sandians were part of a team selected for The Commander's Award for Innovation, Lon Dawson, Mitch McCrory, John Mulder, Alex Roesler, and Phil Turner. This award recognizes innovative solutions to the Naval Sea System Command's most complex problems. The Project Longhorn Team delivered a capability to the Fleet addressing a major cyber threat. The award states, "This was an agile, fast, high return on investment solution that harnessed the best and brightest minds, focused resources, and targeted intelligence."

Cyber security and cyber threats are a top concern for the United States, and particularly for the Department of Defense (DoD). The Department of the Navy (DON) recognizes this real threat to the Fleet; and the Project Longhorn Team is no exception. Understanding the standard approach to doing business would not be effective when a significant cyber threat was identified, the Project Longhorn Team, led by Keith Archbold for the DON, benchmarked and then partnered with best of breed technology providers both inside and outside of the DON, employing proven cutting-edge product development strategies applied to the Navy Research and Development Establishment (NRDE). This was an agile, fast, high return on investment solution that harnessed the best and brightest minds, focused resources, and targeted intelligence. All of the team members were involved in critical decision making and were true catalysts leading to accelerated development times and a superior end product. As a direct result of the team's dedicated efforts, Project Longhorn delivered critical capability to the Fleet in less than two years from white board concept to functional deployed capability; addressing a major cyber threat for a relatively meager sum. What is most innovative about this effort is how that capability was architected and delivered (a full description of the capability itself is available on SIPR).

Commander, Naval Sea Systems Command presented the Project Longhorn Team, comprised of members from Naval Undersea Warfare Center Division, Keyport, Naval Surface Warfare Center

Philadelphia Division, and Department of Energy partners at Sandia National Laboratories, with the prestigious Commander's Award for Innovation for their achievements in mitigating a serious cyber threat to the United States Fleet. The cutting-edge capability was delivered in a significantly abbreviated time frame, eradicating the identified threat. The success of the team stems from the innovative approach of leveraging cutting-edge technology employed by the best performers across disparate technology and organizational boundaries, which has culminated to provide significant positive benefit to the Department of the Navy and Department of Defense. These accomplishments reflect great credit upon the team and are in keeping with the highest traditions of the Department of the Navy in defense of the nation.

Adrian Chavez

Adrian Chavez is a principal member of staff at Sandia National Laboratories. Adrian specializes in cybersecurity focused on enhancing the security of our nation's critical infrastructure systems with over 16 years of experience. Adrian has led and contributed to several cybersecurity research projects, many of which have transitioned to fielded commercial products. In one project named "Lemnos", Adrian developed a security architecture that provides end-to-end cryptographically secure communications, secure remote engineering access, high fidelity execution of critical software, built-in situational awareness and a framework that is capable of harnessing next generation security technologies. An IEEE specification for this security architecture has been developed and is available for industry wide adoption. Over 10 industry vendors have adopted this security architecture and have been deployed in several operational settings. Each of the security vendors implementing this security architecture are interoperable with one another so that utilities are not tied to one specific vendor.

More recently, Adrian is focusing his research in the space of Software Defined Networking (SDN) technology, which allows new security protections to be built directly into the network itself through a project titled "Artificial Diversity and Defense Security (ADDSec)". The SDN technology is being leveraged to create moving target defenses and dynamic defenses that add additional layers of defense to critical energy delivery systems. This research project is focused on increasing the adversarial workload by introducing randomness into these critical infrastructure networks to continuously change the attack surface while also maintaining the strict operational constraints. ADDSec has several partners that include vendors to transition the technology to market, national laboratories that provide testbeds to evaluate the technology, and a DoD partner to provide a microgrid for operational testing at the conclusion of the project.

Adrian is also researching new techniques to improve the high availability requirements of critical infrastructure software and hardware. This research project titled "Real-Time Upgrades for Critical Infrastructure" is focused on minimizing the amount of downtime incurred through regular software updates. Typically, when software is patched or upgraded, the said software must be brought offline for a short amount of time until the upgrade process is complete. However, in many cases, zero downtime can be afforded within critical infrastructure environments. Currently a prototype has been developed to demonstrate the feasibility of the framework that is under development.

Additionally, Adrian regularly volunteers his time to mentor, teach and increase interests in STEM related fields for the next generation of scientists and engineers. His volunteer activities span the entire spectrum from Kindergarten to graduate students where he focuses on underrepresented at-risk students. He has taught students about computer hardware and software, how to program and interact with embedded systems, and how to defend and securely configure computer systems. Several computer security modules have been developed to introduce students to the complex challenges and opportunities available within STEM based fields.

Adrian was awarded the Presidential Early Career Award for Scientists and Engineers (PECASE) in 2014. Adrian was nominated by the Office of Electricity Delivery & Energy Reliability at the Department of Energy for his cybersecurity innovations in energy delivery systems. Adrian earned a B.S. degree in Computer Science from the University of New Mexico and an M.S. degree in Computer Science from the University of Colorado at Boulder. Adrian is currently a Ph.D. computer science candidate at the University of California, Davis and is researching moving target and dynamic defense techniques to provide additional protections within a control system environment to complement his research at SNL.