News Center News Articles Collection

2017-08-08

NPS Cyber Graduate Detects Active Vulnerability Through His Thesis Research

Dionne, Patrick

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/55721

NPS Cyber Graduate Detects Active Vulnerability Through His Thesis Research

my.nps.edu /-/nps-cyber-graduate-detects-active-vulnerability-through-his-thesis-research

By MC2 Patrick Dionne | August 8, 2017

While completing research for his master's degree thesis in computer science, NPS graduate Francisco Tacliad discovered an active vulnerability in a commonly-used programmable logic controller. Tacliad, who attended NPS through the National Science Foundation's Scholarship for Service program, currently works for the Space and Naval Warfare Systems Command (SPAWAR) in San Diego, Calif.

The mission of the Naval Postgraduate School's (NPS) Department of Computer Science is to advance the combat effectiveness of the U.S. and allied armed forces through unique graduate education programs and associated research in areas such as cyber-physical systems security, network security, cyber systems and operations, and other related fields.

However, for September 2016 graduate Francisco Tacliad, classroom education quickly became a real-world scenario when he discovered an active vulnerability in the Allen Bradley MicroLogix 1100 Programmable Logic Controller (PLC) while performing research for this NPS thesis. PLCs are vital components for the operation of industrial control systems (ICS) that manage critical infrastructure services.

"It all started when I developed a fuzz testing tool to find vulnerabilities as part of my thesis. Basically, the tool sends inputs to the system under test while looking for undefined behavior or denial of service errors," said Tacliad. "From there, we can determine whether that was caused by something the fuzzer had sent."

Fuzzing is a penetration-testing technique used to discover coding errors and security loopholes in software. It involves feeding massive amounts of random data, called fuzz, to the test subject in an attempt to make it crash.

"The way fuzzers work is you just set it and let it run. So, I set it, and an hour or two later I noticed a red light on the

MicroLogix 1100 that indicated a fault," said Tacliad. "The device was unresponsive and the only way to get it to function again was a hard reboot. This proved an incredible way to apply my thesis in a tangible matter, and to prove that this tool can find vulnerabilities."

Titled "ENIP Fuzz: A Scapy-Based Ethernet/IP Fuzzer for Security Testing," Tacliad's thesis largely centered on building a tool that could find vulnerabilities in industrial network protocols used in control systems.

The vulnerability that Tacliad discovered was an improper input validation which sends commands to the controller. The vulnerability would have allowed an attacker to launch a denial-of-service attack by sending a maliciously-crafted packet to the PLC to cause it to stop responding to new requests.

"I feel fuzzing has got a lot more traction as far as a way to find vulnerabilities in devices," said Tacliad. "With the increased use of the Internet as part of our daily life, this field is really growing and fast. The fuzzer that I made is a good proof of concept that people can take a specification of a protocol and analyze it in such a way that they will be able to find bugs and vulnerabilities in these types of devices."

"Our group focuses on security issues relating to industrial control systems on ships, which are used for many functions onboard a ship including machinery control, ventilation and propulsion, and that's what makes Tacliad's research so applicable," added NPS Research Associate Thuy D. Nguyen, who co-advised and worked closely with Tacliad on his thesis. "One thing that he found is there is an embedded protocol where by sending custom packets an attacker can silence the PLC, so imagine if that PLC was used for fire control and someone exploited it."

Tacliad attended NPS as part of the Scholarship for Service (SFS) program which is sponsored by the National Science Foundation. NPS has been part of the program since 2001, with the intent of infusing new cybersecurity talent into the government. Students receive paid tuition and an annual stipend as well as an allowance for books and other related expenses in exchange for their obligation to work in the federal government for two years.

Says Distinguished Professor of Computer Science Dr. Cynthia E. Irvine, lead for the Scholarship for Service program on campus, "People love this program because not only do students receive a master's degree in computer science, but because we are working in a government culture at NPS, students arrive with the skills necessary to thrive in a government job."

The SFS program is also unique in its ability to bring in students from diverse backgrounds, preparing them for success in the rapidly changing field of cybersecurity.

"I graduated with a bachelor's degree in political science and economics in 2008, afterwards I worked with a couple start-up companies until I realized I wanted to go back to school, and this was a great opportunity for me," said Tacliad. "NPS was unique because it allowed candidates to come in without an undergraduate degree in computer science. And my dad was also in the Navy so being around that community felt very comfortable. That, along with the reputation of NPS, made me realize that this would be perfect for me."

Following the standard responsible disclosure practice, the vulnerability Tacliad discovered was reported to the Industrial Control Systems Computer Emergency Response Team (ICS-CERT). Part of the Department of Homeland Security, ICS-CERT works to reduce critical infrastructure risks by partnering with law enforcement agencies and the intelligence community, while coordinating efforts among federal, state, local and tribal governments, and control system owners and operators. ICS-CERT contacted the affected vendor, Rockwell Automation, and after the vendor released an official firmware patch to remediate the vulnerability in July 2017, ICS-CERT issued a security advisory informing the general public of the potential exploit.

"Finding the vulnerability really helped me in the long run as it demonstrated to the management of my new job at the Space and Naval Warfare Systems Command (SPAWAR) what I am capable of," said Tacliad. "At SPAWAR, my duties include looking at similar vulnerabilities in industrial control systems that the Navy uses and other similar types of embedded devices that work the same way."

Based in San Diego, SPAWAR functions as the Navy's technical authority and acquisition command for command, control, communications, computers, intelligence, surveillance and reconnaissance.

"This is the best job I have ever had," said Tacliad. "I can see myself staying in this industry for the foreseeable future, and this experience as a whole has helped me realize what I want to do and set me up for it."