NSA, Morgan State University Use Ghidra to Mitigate Vehicle Cyber Vulnerabilities

/ Published May 14, 2021
FT. MEADE, Md.,

The National Security Agency recently partnered with Morgan State University to use Ghidra — an NSA-created reverse-engineering tool — to help identify cyber weaknesses in vehicles and improve their resistance to cyber threats.

NSA spent many years developing Ghidra before publicly releasing it in 2019.

“Modern vehicles have become both transportation and data collection systems,” said Brian Knighton, a member of NSA’s Ghidra Team who helped initiate the partnership. “The data collected and recorded is quite broad and includes vehicle speed, passenger count, GPS routes, images from backup cameras, and [personally identifiable information] from connected cell phones. This information stays locally on the vehicle forever and in most cases is uploaded to the [original equipment manufacturer]. Those systems also control critical safety items like brakes. If left unprotected both privacy and lives could be at risk.”

Knighton added that vehicles are now part of the Internet of Things (IoT). Most IoT is only supported by vendors for around five years, while some vehicles have an operating life of 15-plus years. There is currently nothing in place to secure these systems long-term.

NSA, university partner

To help accelerate and broaden the application of Ghidra, The NSA Research Directorate’s Vehicle Systems Software Analysis team partnered with the Morgan State’s Cybersecurity Assurance and Policy (CAP) Center, led by Dr. Kevin Kornegay.

Dr. Kornegay, an electrical and computer engineering professor at Morgan State, is the founder of CAP and the university’s Internet of Things (IoT) Security Research Lab. He is also the Agency’s principal CAP research partner.

“This research project leverages our core competency in hardware reverse engineering,” said Dr. Kornegay of his CAP research team. Under his guidance, the team partners with NSA to leverage Ghidra’s technology to mitigate vulnerabilities.

To support this research, NSA’s Vehicle Systems Software Analysis team is developing a generalized vehicle cybersecurity platform that will support vulnerability discovery and mitigations using virtualization and reverse engineering. The team uses this

From left, Albert Sweets, Dr. James Whitney, Dr. Kevin Kornegay, Vinton Morris, and Aaron Edmund are part of Morgan State University’s Cybersecurity Assurance and Policy research team. The team has partnered with NSA researchers to use Ghidra, a NSA-made tool, to mitigate vehicle cyber capabilities (Photo courtesy of Morgan State University)

research to develop countermeasures to secure systems against sensitive data extraction, disruption, diversion, and obfuscation.

“The mission of the Vehicle Systems Software Analysis team is to conduct vulnerability research against the electronic control units (ECUs) contained within modern vehicles, including cars, trucks, motorcycles, RVs, boats, and aircraft,” said Knighton.

The team conducts vulnerability research by extracting firmware from the ECUs and utilizing Ghidra to analyze it. The reverse-engineering software performs decompilation — producing source code understandable to engineers from compiled code. Ghidra can do this on a wide array of microprocessors, making it valuable for the diverse hardware environments of modern vehicles.

Knighton explained that most ECUs are equipped with IoT technologies such as sensors, cameras, and wireless systems. The main purpose of this technology is to gather, store, transmit, and receive data for entertainment, engine performance, safety, and emissions regulations.

“While this technology adds value from a consumer perspective, it also creates many security risks in the mission space: namely privacy, cybersecurity, malware, and geolocation vulnerabilities,” said Dr. Kornegay.

Part of a larger strategy

The research project is the culmination of a five-year effort led by NSA Cybersecurity Senior Strategist and Cybersecurity Academic Liaison to the university, Dr. Eric Clemons.

Dr. Kevin Kornegay (front) founder of Morgan State University’s Cybersecurity Assurance and Policy Center, and Aaron Edmond, graduate research assistant, review Ghidra firmware analysis. (Photo courtesy of Morgan State University)

“I approached the NSA Computer Systems Research Group in 2019 about inviting Ghidra Team members to provide a demonstration of the tool during a cybersecurity training workshop for local universities led by Morgan State,” said Dr. Clemons.

Clemons and Technical Director of NSA Cybersecurity, Neal Ziring, toured the CAP center in 2020 and saw how a research partnership could benefit NSA and the university.

“This partnership and strategy is part of a larger NSA academic engagement strategy that can help the Agency expand its connections and relationships with institutions of higher education,” said Ziring. “NSA continues to advance the Director’s top priority of talent recruitment and retention by establishing partnerships with universities and researchers like Dr. Kornegay. All of these efforts further our research and mission to protect the Nation.”

The partnership is exactly what Knighton and his team had in mind when they released the reverse-engineering software in 2019.

“One of the motivations for releasing Ghidra was to foster external collaboration in cybersecurity with industry and academia,” said Knighton. “Not just in the adoption of Ghidra into school curricula or the development of new features, but also solving some of the hard cybersecurity problems facing NSA and the U.S. Government. This partnership will allow us to advance this critical vehicle research we do on behalf of the Nation.”