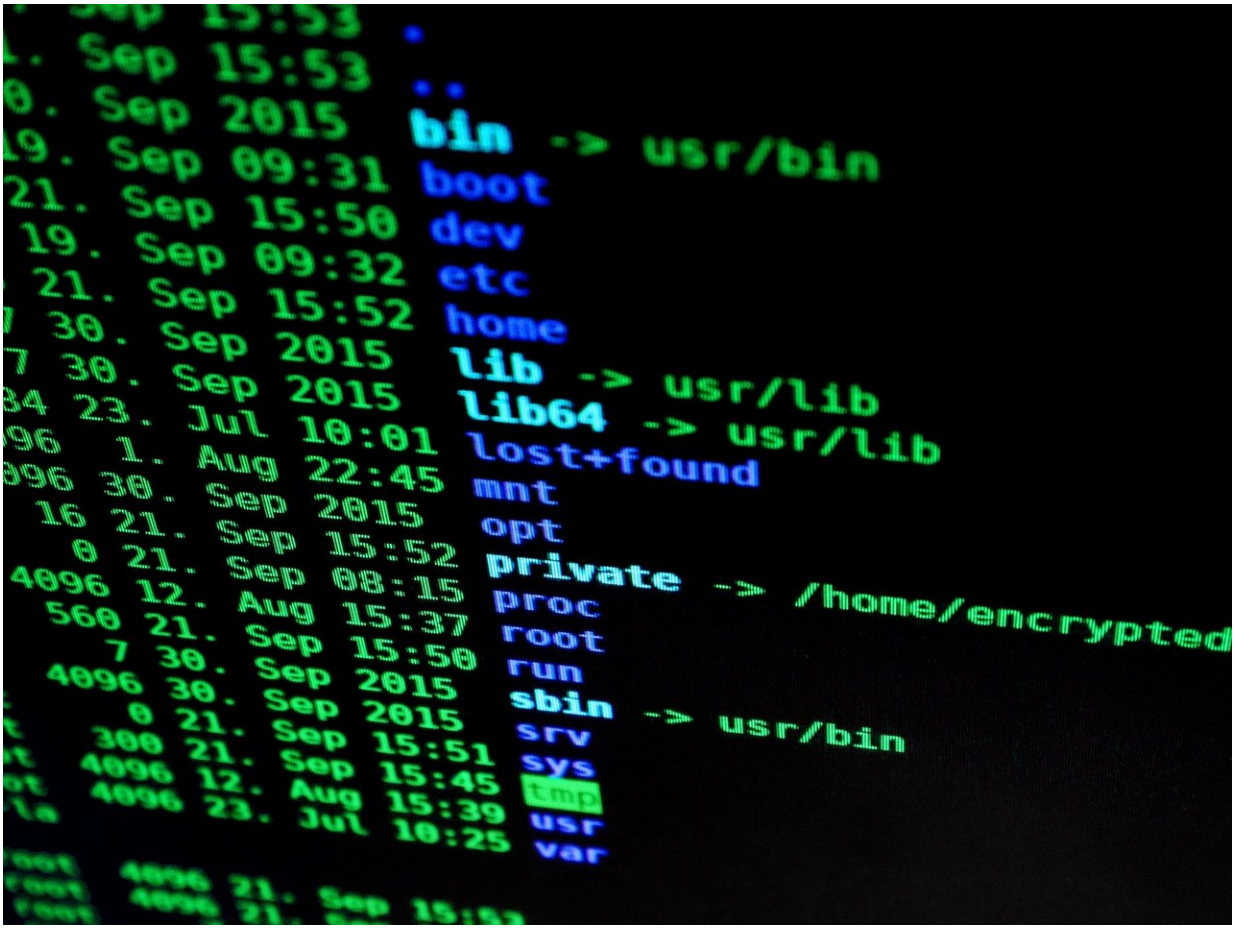
CyberGraph: mapping cyber threats to prevent the next attack

June 10 2020, by Tatyana Hopkins



Credit: CC0 Public Domain

Although nearly every aspect of our lives relies on technology, our

current cybersecurity infrastructure is not prepared to effectively defend our social, economic and political organizations from advancing cyberattacks, said Howie Huang, a professor of electrical and computer engineering in the George Washington University School of Engineering and Applied Science.

"The thing is, in cybersecurity, if you are a defender, you need to be correct 100 percent of the time, but if you're an attacker, you only need to be successful once," he said.

So, Dr. Huang along with Benjamin Bowman and Craig Laprade—doctoral and master's students of computer engineering in Dr. Huang's Graph Computing Lab—are developing an artificial intelligence system designed to work collaboratively with cybersecurity analysts to provide stronger security for enterprise networks through their startup, CyberGraph.

Dr. Huang pointed out that a talent shortage within the field of cybersecurity—more than 2 million unfilled positions—and currently available tools that create high volume, low fidelity alerts—an average of 10,000 alerts each day—make it "really easy" for cybersecurity analysts to miss important alerts because using current tools they often are too overwhelmed to recognize high-risk threats that indicate a coordinated attack.

"What we provide is a contextualized incident story, where we highlight the most critical alerts so cybersecurity analysts can look and quickly see the things they need to focus on," Dr. Huang said.

Unlike traditional cybersecurity tools, which define rules based on past experiences and triggers alerts based on any variation from those rules, CyberGraph's proprietary patent-pending graph technology, which combines machine learning and graph theory, is able to capture the

complexity of network user behavior, trigger high fidelity alerts of potentially malicious activity and generate comprehensive incident stories for cybersecurity analysts that connect the dots to show causal relationships between entities and events in a network.

The team's CyberGraph research has been supported by the Defense Advanced Research Projects Agency (DARPA) and the National Science Foundation (NSF) grants totaling $2.5 million. Recently, their research paper titled "Detecting Lateral Movement in Enterprise Computer Networks with Unsupervised Graph AI" has been accepted to appear in the International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020). They were also finalists in the 2020 GW New Venture Competition.

"CyberGraph's tool will enable more entry-level cybersecurity analysts to operate at a high effectiveness, opening up more people to these desirable positions, since there is a huge shortage of cybersecurity professionals now," said Jim Chung, GW's associate vice president for research, innovation and entrepreneurship. "With the upheaval and new cybersecurity risks caused by the pandemic, these positions will continue to be in high demand. CyberGraph opens up many more people to be eligible, allowing them to do their jobs faster and better."

A recipient of the prestigious NSF CAREER Award, Dr. Huang has also won numerous awards for his research in graph computing, most recently, a Champion Award and a Student Innovation Award at the Graph Challenge of 2018 Institute of Electrical and Electronics Engineers (IEEE) High-Performance Extreme Computing conference.

"Graph is a fundamental concept, yet it is extremely powerful," Dr. Huang said.

He said there are countless real-world applications that are best modeled

using graph technology.

"If you imagine Facebook as a graph, each one of us is a node and our friends, likes and comments are edges," Dr. Huang said. "Using graph analytics, you can understand the relationship between different people and different behaviors in the social network." Dr. Huang's GraphLab is also collaborating with researchers in the Institute for Data, Democracy and Politics, a GW research hub that tracks the spread of digital misinformation.

To Dr. Huang, student mentoring and training in research, leadership and entrepreneurship is an integral part of the CyberGraph project.

"It has helped me shape my research in such a way that it will be truly impactful," Mr. Bowman said, "We are trying to do our part and contribute to cyber defense with this project."

Mr. Laprade added, "CyberGraph has the potential to make network defense a lot easier for the average organization. It gives cybersecurity teams a form of digital intuition that normally takes years to develop."

Dr. Huang is hopeful that there is great potential for CyberGraph in the $250 billion cybersecurity market. His team hopes to capture $50 million in the company's first five years by offering their service to customers with large-scale networks for a monthly subscription fee.

With the project still in the prototyping phase, the CyberGraph team plans to spend the summer developing a minimum viable product to test on some of the dozens of organizations they interviewed as part of GW Accelerate I-Corps program. They have already deployed a research prototype to a federal government agency.

Soon, the CyberGraph team will explore the possibility of raising funds

from potential investors as well as apply to various national programs such as U.S. Department of Defense I-Corps program, NSF Partnerships for Innovation and Small Business Innovation Research programs.

Provided by George Washington University