Computer scientists' new tool fools hackers into sharing keys for better cybersecurity

February 27 2020, by Kim Horner

Dr. Latifur Khan (left), professor of computer science, and Gbadebo Ayoade MS'14, PhD'19, shown at Ayoade's doctoral hooding ceremony in December, are co-authors of a study that promotes the benefits of crook-sourcing. Credit: UT Dallas

Instead of blocking hackers, a new cybersecurity defense approach

developed by University of Texas at Dallas computer scientists actually welcomes them.

The method, called DEEP-Dig (DEcEPtion DIGging), ushers intruders into a decoy site so the computer can learn from hackers' tactics. The information is then used to train the computer to recognize and stop future attacks.

UT Dallas researchers presented a paper on their work, "Improving Intrusion Detectors by Crook-Sourcing," at the annual Computer Security Applications Conference in December in Puerto Rico. They presented another paper, "Automating Cyberdeception Evaluation with Deep Learning," in January at the Hawaii International Conference of System Sciences.

DEEP-Dig advances a rapidly growing cybersecurity field known as deception technology, which involves setting traps for hackers. Researchers hope that the approach can be especially useful for defense organizations.

"There are criminals trying to attack our networks all the time, and normally we view that as a negative thing," said Dr. Kevin Hamlen, Eugene McDermott Professor of computer science. "Instead of blocking them, maybe what we could be doing is viewing these attackers as a source of free labor. They're providing us data about what malicious attacks look like. It's a free source of highly prized data."

The approach aims to solve a major challenge to using artificial intelligence for cybersecurity: a shortage of data needed to train computers to detect intruders. The lack of data is due to privacy concerns. Better data will mean better ability to detect attacks, said Gbadebo Ayoade MS'14, Ph.D.'19, who presented the findings at the recent conferences.

"We're using the data from hackers to train the machine to identify an attack," said Ayoade, now a data scientist at Procter & Gamble Co. "We're using deception to get better data."

Hackers typically begin with their simplest tricks and then use increasingly sophisticated tactics, Hamlen said. But most cyberdefense programs try to disrupt intruders before anyone can monitor the intruders' techniques. DEEP-Dig will give researchers a window into hackers' methods as they enter a decoy site stocked with disinformation. The decoy site looks legitimate to intruders, said Dr. Latifur Khan, professor of computer science at UT Dallas.

"Attackers will feel they're successful," Khan said.

Governmental agencies, businesses, nonprofits and individuals face a constant threat from cyberattacks, which cost the U.S. economy more than $57 billion in 2016, according to a report to the White House from the Council of Economic Advisers.

As hackers' tactics change, DEEP-Dig could help cybersecurity defense systems keep up with their new tricks.

"It's an endless game," Khan said.

While DEEP-Dig aims to outsmart hackers, is it possible that hackers could have the last laugh if they realize they have entered a decoy site and try to deceive the program?

Maybe, Hamlen said. But that possibility does not worry him.

"So far, we've found this doesn't work. When an attacker tries to play along, the defense system just learns how hackers try to hide their tracks," Hamlen said. "It's an all-win situation—for us, that is."