Fighting the next generation of cyberattacks

16 April 2015

Suresh Venkatasubramanian, left, and Matt Might, both associate professors of computer science at the University of Utah, have received a $3 million government grant to produce software that can sniff out the next generation of computer vulnerabilities. These attacks, called algorithmic vulnerabilities, are harder to detect and can do a great amount of damage on computer systems. Credit: University of Utah College of Engineering

The next generation of cyberattacks will be more sophisticated, more difficult to detect and more capable of wreaking untold damage on the nation's computer systems.

So the U.S. Department of Defense has given a $3 million grant to a team of computer scientists from the University of Utah and University of California, Irvine, to develop software that can hunt down a new kind of vulnerability that is nearly impossible to find with today's technology.

The team is tasked with creating an analyzer that can thwart so-called algorithmic attacks that target the set of rules or calculations that a computer must follow to solve a problem. Algorithmic attacks are so new and sophisticated that only hackers hired by nation states are likely to have the resources necessary to mount them, but perhaps not for long.

"The military is looking ahead at what's coming in terms of cybersecurity and it looks like they're going to be algorithmic attacks," says Matt Might, associate professor of computer science at the University of Utah and a co-leader on the team.

"Right now, the doors to the house are unlocked so there's no point getting a ladder and scaling up to an unlocked window on the roof," Might says of the current state of computer security. "But once all the doors get locked on the ground level, attackers are going to start buying ladders. That's what this next generation of vulnerabilities is all about."

Typically, software vulnerabilities today rely on programmers making mistakes while creating their programs and hackers will exploit those mistakes. For example, the software will receive a programming input crafted by a hacker and use it without automatically validating it first. That could result in a vulnerability giving the hacker access to the computer or causing it to leak information.

Algorithmic attacks don't need to find such conventional vulnerabilities. They can, for instance, secretly monitor how an algorithm is running or track how much energy a computer is using and use that information to glean secret data that the computer is processing. Algorithmic attacks can also disable a computer by forcing it to use too much memory or driving its central processing unit to overwork.

"These algorithmic attacks are particularly devious because they exploit weaknesses in how resources like time and space are used in the algorithm," says Suresh Venkatasubramanian, U associate professor of computer science and co-leader on the team.

Most hackers currently are not using algorithmic attacks because they are costly, extremely complex, and take the most amount of time. So attackers take the easier route of exploiting current vulnerabilities.

The team will be developing software that can perform an audit of computer programs to detect algorithmic vulnerabilities or "hot spots" in the code. This analyzer will perform a mathematical simulation of the software to predict what will happen in the event of an attack.

"Think of it as a spellcheck but for cybersecurity," Might says.

The project is one of 10 funded by the Defense Advanced Research Projects Agency in a new initiative called STAC, or Space/Time Analysis for Cybersecurity. The University of Utah team will be comprised of 10 faculty members, postdoctoral and graduate students. Of the $3 million DARPA grant, which is over four years, $2 million will go to the U team and $1 million to UC Irvine.

Provided by University of Utah