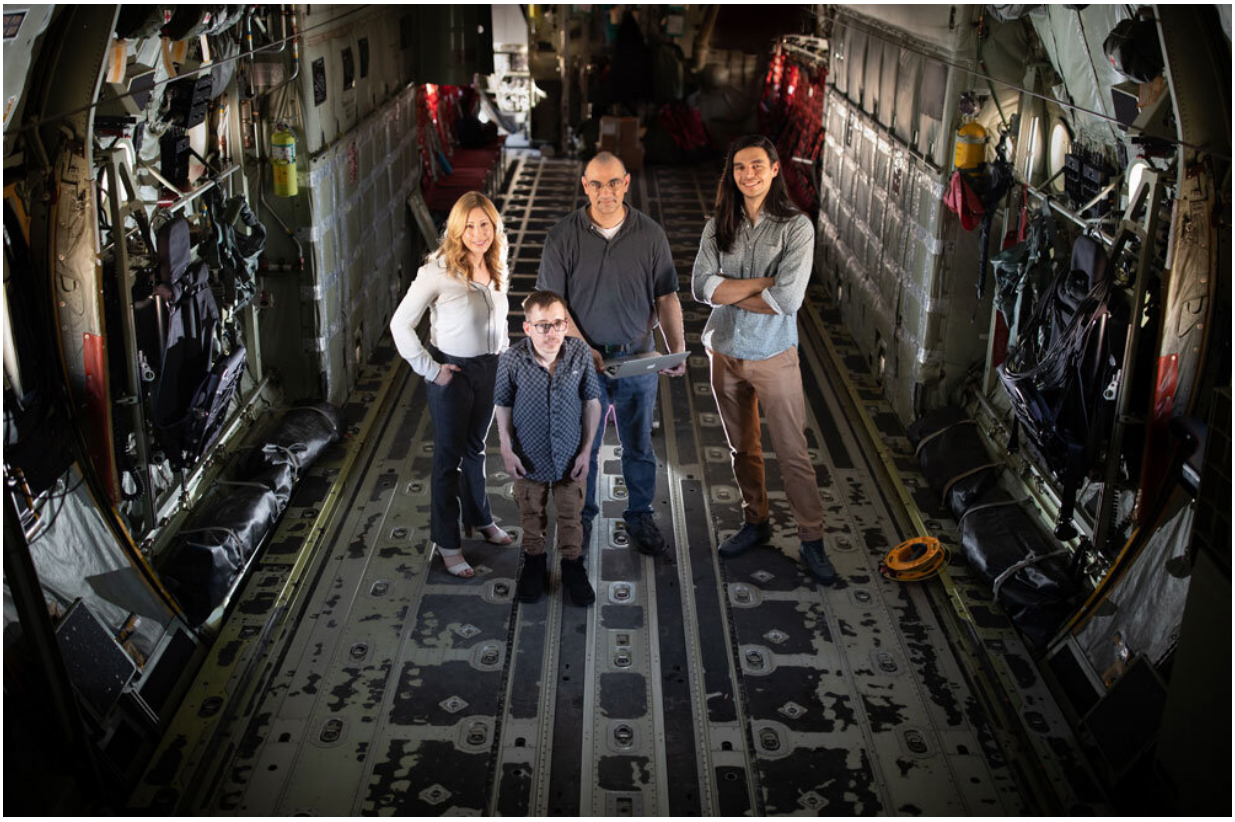
Hackers could try to take over a military aircraft; can a cyber shuffle stop them?

February 23 2023, by Troy Rummler



Aboard the 58th Special Operations Wing's C-130 transport aircraft at Kirtland Air Force Base, Christy Sturgill, Jacob Hazelbaker, Eric Vugrin and Nicholas Troutman, from left to right, were part of the Sandia team working on a moving target defense that makes a computer network commonly used on space and aircraft less vulnerable to cyberattack. Credit: Craig Fritz

A cybersecurity technique that shuffles network addresses like a blackjack dealer shuffles playing cards could effectively befuddle hackers gambling for control of a military jet, commercial airliner or spacecraft, according to new research. However, the research also shows these defenses must be designed to counter increasingly sophisticated algorithms used to break them.

Many aircraft, spacecraft and weapons systems have an onboard computer network known as military standard 1553, commonly referred to as MIL-STD-1553, or even just 1553. The network is a tried-and-true protocol for letting systems like radar, flight controls and the heads-up display talk to each other.

Securing these networks against a cyberattack is a national security imperative, said Chris Jenkins, a Sandia cybersecurity scientist. If a hacker were to take over 1553 midflight, he said, the pilot could lose control of critical aircraft systems, and the impact could be devastating.

Jenkins is not alone in his concerns. Many researchers across the country are designing defenses for systems that utilize the MIL-STD-1553 protocol for command and control. Recently, Jenkins and his team at Sandia partnered with researchers at Purdue University in West Lafayette, Indiana, to test an idea that could secure these critical networks.

Their results, recently published in the scientific journal *IEEE Transactions on Dependable and Secure Computing*, show that done the right way, a technique already known in cybersecurity circles, called moving target defense, can effectively protect MIL-STD-1553 networks against a machine-learning algorithm.

"When we talk about protecting our computer systems, frequently there are two main pieces we rely on," said Eric Vugrin, a Sandia

cybersecurity senior scientist who also worked on the project. "The first approach is just keeping the bad guy out and never permitting access to the system. The physical analogue is to build a big wall and don't let him in in the first place. And the backup plan is, if the wall doesn't work, we rely on detection. Both of those approaches are imperfect. And so, what moving target defense offers as a complementary strategy is, even if those two approaches fail, moving target confuses the attacker and makes it more difficult to do damage."

Moving target defense must keep cyberattackers guessing

Like a game of three-card monte, in which a con artist uses sleight of hand to shuffle cards side-to-side, moving target defense requires randomness. Without it, the defense unravels. Researchers wanted to know whether a moving target defense would work to constantly change network addresses, unique numbers assigned to each device on a network. They weren't sure it would work, because compared to other types of networks, MIL-STD-1553's address space is small and therefore difficult to randomize.

For example, the strategy has proven useful with internet protocols, which have millions or billions of network addresses at their disposal, but 1553 only has 31. In other words, Sandia had to come up with a way to surreptitiously shuffle 31 numbers in a way that couldn't easily be decoded.

"Someone looked me in the face and said it's not possible because it was just 31 addresses," Jenkins said. "And because the number is so small compared to millions or billions or trillions, people just felt like it wasn't enough randomness."

The challenge with randomizing a small set of numbers is that "nothing in computer software is truly random. It's always pseudorandom," said Sandia computer scientist Indu Manickam. Everything must be programmed, she said, so there's always a hidden pattern that can be discovered.

With enough time and data, she said, "A human with an Excel sheet should be able to get it."

Manickam is an expert in machine learning, or computer algorithms that identify and predict patterns. These algorithms, though beneficial to cybersecurity and many other fields of research and engineering, pose a threat to moving target defenses because they can potentially spot the pattern to a randomization routine much faster than a human.

"We're using machine-learning techniques to better defend our systems," Vugrin said. "We also know the bad guys are using machine learning to attack the systems. And so, one of the things that Chris identified early on was that we do not want to set up a moving target defense where somebody might use a machine-learning attack to break it and render the defense worthless."

Sophisticated algorithms don't necessarily spell the end for this type of cyberdefense. Cybersecurity designers can simply write a program that changes the randomization pattern before a machine can catch on.

But the Sandia team needed to know how fast machine learning could break their defense. So, they partnered with Bharat Bhargava, a professor of computer science at Purdue University, to test it. Bhargava and his team had been involved previously in researching aspects of moving target defenses.

For the last seven years, Bhargava said, the research fields of

cybersecurity and machine learning have been colliding. And that's been reshaping concepts in cybersecurity.

"What we want to do is learn how to defend against an attacker who is also learning," Bhargava said.

Test results inform future improvements to cybersecurity

Jenkins and the Sandia team set up two devices to communicate back and forth on a 1553 network. Occasionally, one device would slip in a coded message that would change both devices' network addresses. Jenkins sent Bhargava's research team logs of these communications using different randomization routines. Using this data, the Purdue team trained a type of machine-learning algorithm called long short-term memory to predict the next set of addresses.

The first randomization routine was not very effective.

"We were not only able to just detect the next set of addresses that is going to appear, but the next three addresses," said Ganapathy Mani, a former member of the Purdue team who contributed to the research.

The algorithm had scored 0.9 out of a perfect 1.0 on what's called a Matthews correlation coefficient, which rates how well a machine-learning algorithm performs.

But the second set of logs, which used a more dynamic routine, resulted in a radically different story. The algorithm only scored 0.2.

"0.2 is pretty close to random, so it didn't really learn anything," Manickam said.

The test showed that moving target defense can fundamentally work, but more importantly it gave both teams insights into how cybersecurity engineers should design these defenses to withstand a machine-learning-based assault, a concept the researchers call threat-informed codesign.

Defenders, for example, could "Add fake data into it so that the attackers cannot learn from it," Mani said.

The findings could help improve the security of other small, cyber-physical networks beyond MIL-STD-1553, such as those used in critical infrastructure.

Jenkins said, "Being able to do this work for me, personally, was somewhat satisfying because it showed that given the right type of technology and innovation, you can take a constrained problem and still apply moving target defense to it."

More information: Ganapathy Mani et al, Machine Learning Based Resilience Testing of an Address Randomization Cyber Defense, *IEEE Transactions on Dependable and Secure Computing* (2023). DOI: 10.1109/TDSC.2023.3234561

Provided by Sandia National Laboratories