Scientists harness chaos to protect devices from hackers

April 7 2021, by Jeff Grabmeier

Credit: CC0 Public Domain

Researchers have found a way to use chaos to help develop digital fingerprints for electronic devices that may be unique enough to foil even the most sophisticated hackers.

Just how unique are these fingerprints? The researchers believe it would take longer than the lifetime of the universe to test for every possible combination available.

"In our system, chaos is very, very good," said Daniel Gauthier, senior author of the study and professor of physics at The Ohio State University.

The study was recently published online in the journal *IEEE Access*.

The researchers created a new version of an emerging technology called physically unclonable functions, or PUFs, that are built into computer chips.

Gauthier said these new PUFs could potentially be used to create secure ID cards, to track goods in supply chains and as part of authentication applications, where it is vital to know that you're not communicating with an impostor.

"The SolarWinds hack that targeted the U.S. government really got people thinking about how we're going to be doing authentication and cryptography," Gauthier said.

"We're hopeful that this could be part of the solution."

The new solution makes use of PUFs, which take advantage of tiny manufacturing variations found in each computer chip—variations so small that they aren't noticeable to the end user, said Noeloikeau Charlot, lead author of the study and a doctoral student in physics at Ohio State.

"There's a wealth of information in even the smallest differences found on computers chips that we can exploit to create PUFs," Charlot said.

These slight variations—sometimes seen only at the atomic level—are used to create unique sequences of 0s and 1s that researchers in the field call, appropriately enough, "secrets."

Other groups have developed what they thought were strong PUFs, but research showed that hackers could successfully attack them. The problem is that current PUFs contain only a limited number of secrets, Gauthier said.

"If you have a PUF where this number is 1,000 or 10,000 or even a million, a hacker with the right technology and enough time can learn all the secrets on the chip," Gauthier said.

"We believe we have found a way to produce an uncountably large number of secrets to use that will make it next to impossible for hackers to figure them out, even if they had direct access to the computer chip."

The key to creating the improved PUF is chaos, a topic that Gauthier has studied for decades. No other PUFs have used chaos in the way demonstrated in this study, he said.

The researchers created a complex network in their PUFs using a web of randomly interconnected logic gates. Logic gates take two electric signals and use them to create a new signal.

"We are using the gates in a non-standard way that creates unreliable behavior. But that's what we want. We are exploiting that unreliable behavior to create a type of deterministic chaos," Gauthier said.

The chaos amplifies the small manufacturing variations found on the chip. Even the smallest differences, when amplified by chaos, can change the entire class of possible outcomes—in this case, the secrets that are being produced, according to Charlot.

"Chaos really expands the number of secrets that are available on a chip. This will likely confuse any attempts at predicting the secrets," Charlot said.

One key to the process is letting the chaos run just long enough on the chip, according to Gauthier. If you let it run too long, it becomes—well, too chaotic.

"We want the process to run long enough to create patterns that are too complex for hackers to attack and guess. But the pattern must be reproducible so we can use it for authentication tasks," Gauthier said.

The researchers calculated that their PUF could create 1077 secrets. How big is that number? Imagine if a hacker could guess one secret every microsecond—1 million secrets per second. It would take the hacker longer than the life of the universe, about 20 billion years, to guess every secret available in that microchip, Gauthier said.

As part of the study, the researchers attacked their PUF to see if it could be successfully hacked. They attempted machine learning attacks, including deep learning-based methods and model-based attacks—all of which failed. They are now offering their data to other research groups to see if they can find a way to hack it.

Gauthier said the hope is that PUFs like this could help beef up security against even state-sponsored hacker attacks, which are generally very sophisticated and backed up with a lot of computer resources.

For example, Russia is suspected of backing the SolarWinds hack that was uncovered in December. That hack reportedly gained access to email accounts of officials in the Department of Homeland Security and the department's cybersecurity staff.

"It is a constant battle to come up with technology that can stay ahead of hackers. We are trying to come up with technology that no hacker—no matter your resources, no matter what supercomputer you use—will be able to crack."

The researchers have applied for an international patent for their PUF device.

The goal of the team is to move beyond research and to move quickly to commercialize the technology. Gauthier and two partners recently founded Verilock, with a goal of bringing a product to market within a year.

"We see this technology as a real game changer in cybersecurity. This novel approach to a strong PUF could prove to be virtually un-hackable," said Jim Northup, CEO of Verilock.

More information: Noeloikeau Charlot et al. Hybrid Boolean Networks as Physically Unclonable Functions, *IEEE Access* (2021). DOI: 10.1109/ACCESS.2021.3066948

Provided by The Ohio State University

Citation: Scientists harness chaos to protect devices from hackers (2021, April 7) retrieved 26 April 2024 from https://techxplore.com/news/2021-04-scientists-harness-chaos-devices-hackers.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.