Graphene Key for Novel Hardware Security

2021-05-15

As more private data is stored and shared digitally, researchers are exploring new ways to protect data against attacks from bad actors. Current silicon technology exploits microscopic differences between computing components to create secure keys, but artificial intelligence (AI) techniques can be used to predict these keys and gain access to data. Now, Penn State researchers have designed a way to make the encrypted keys harder to crack.

Led by Saptarshi Das, assistant professor of engineering science and mechanics, the researchers used graphene — a layer of carbon one atom thick — to develop a novel low-power, scalable, reconfigurable hardware security device with significant resilience to AI attacks. They published their findings in Nature Electronics.

“There has been more and more breaching of private data recently,” Das said. “We developed a new hardware security device that could eventually be implemented to protect these data across industries and sectors.”

The device, called a physically unclonable function (PUF), is the first demonstration of a graphene-based PUF, according to the researchers. The physical and electrical properties of graphene, as well as the fabrication process, make the novel PUF more energy-efficient, scalable, and secure against AI attacks that pose a threat to silicon PUFs.

A team of Penn State researchers has developed a new hardware security device that takes advantage of microstructure variations to generate secure keys.

The team first fabricated nearly 2,000 identical graphene transistors, which switch current on

and off in a circuit. Despite their structural similarity, the transistors' electrical conductivity varied due to the inherent randomness arising from the production process. While such variation is typically a drawback for electronic devices, it's a desirable quality for a PUF not shared by silicon-based devices.

After the graphene transistors were implemented into PUFs, the researchers modeled their characteristics to create a simulation of 64 million graphene-based PUFs. To test the PUFs' security, Das and his team used machine learning, a method that allows AI to study a system and find new patterns. The researchers trained the AI with the graphene PUF simulation data, testing to see if the AI could use this training to make predictions about the encrypted data and reveal system insecurities.

"Neural networks are very good at developing a model from a huge amount of data, even if humans are unable to," Das said. "We found that AI could not develop a model, and it was not possible for the encryption process to be learned."

This resistance to machine learning attacks makes the PUF more secure because potential hackers could not use breached data to reverse engineer a device for future exploitation, Das said. Even if the key could be predicted, the graphene PUF could generate a new key through a reconfiguration process requiring no additional hardware or replacement of components.

"Normally, once a system's security has been compromised, it is permanently compromised," said Akhil Dodda, an engineering science and mechanics graduate student conducting research under Das's mentorship. "We developed a scheme where such a compromised system could be reconfigured and used again, adding tamper resistance as another security feature."

With these features, as well as the capacity to operate across a wide range of temperatures, the graphene-based PUF could be used in a variety of applications. Further research can open pathways for its use in flexible and printable electronics, household devices and more.

Read the original article on Penn State University.