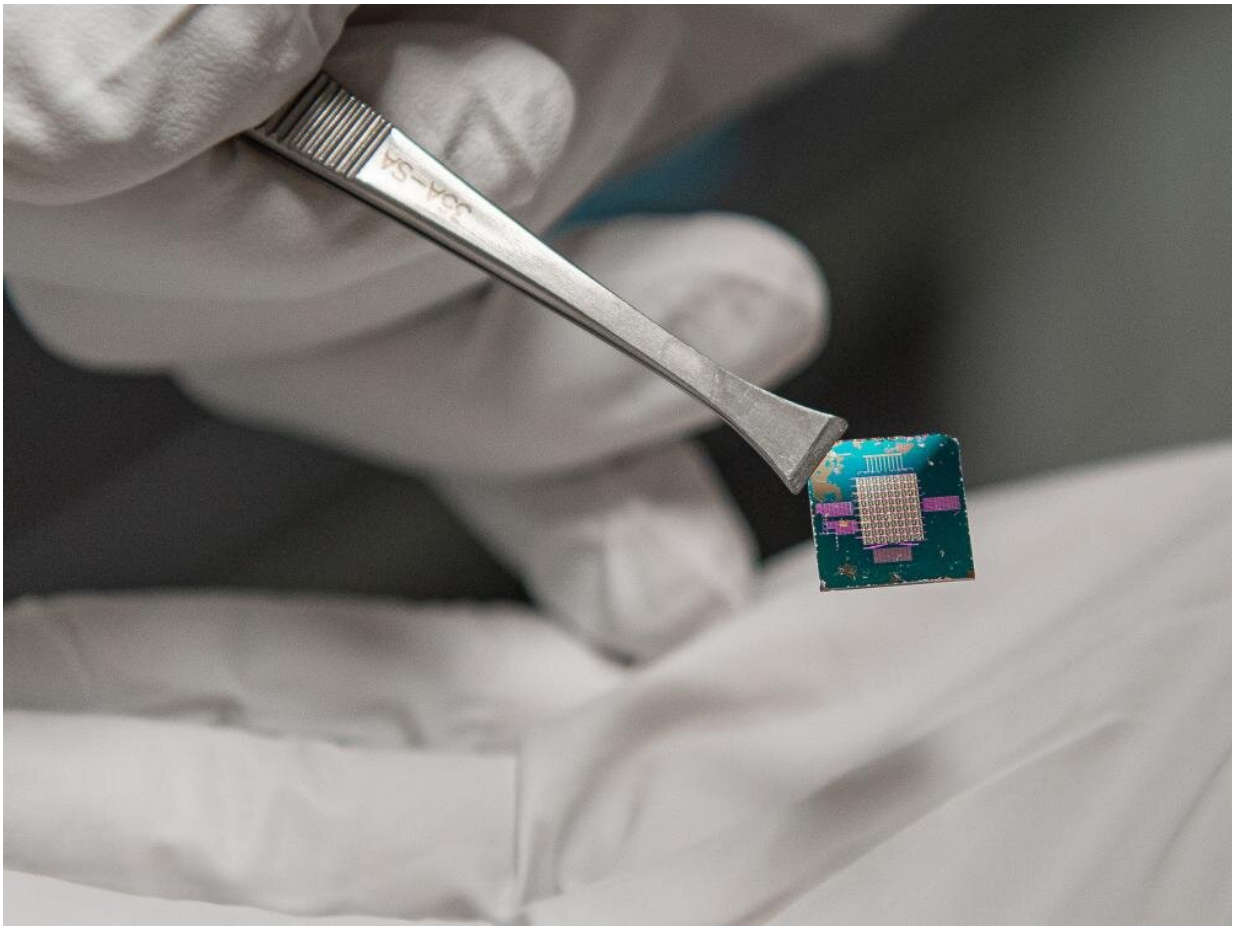
Smart chip senses, stores, computes and secures data in one low-power platform

July 20 2022, by Mariah Chuprinski



Penn State materials science and engineering researchers used molybdenum disulfide, a 2D material, to create a low-power cryptographic chip less than one nanometer thick. Credit: Kelby Hochreither/Penn State

Digital information is everywhere in the era of smart technology, where data is continuously generated by and communicated among cell phones, smart watches, cameras, smart speakers and other devices. Securing digital data on handheld devices requires massive amounts of energy, according to an interdisciplinary group of Penn State researchers, who warn that securing these devices from bad actors is becoming a greater concern than ever before.

Led by Saptarshi Das, Penn State associate professor of engineering science and mechanics, researchers developed a smart hardware platform, or chip, to mitigate energy consumption while adding a layer of security. The researchers published their results on June 23 in *Nature Communications*.

"Information from our devices is currently stored in one location, the cloud, which is shared and stored in large servers," said Das, who also is affiliated with the Penn State School of Electrical Engineering and Computer Science, the Materials Research Institute and the College of Earth and Mineral Sciences' Department of Materials Science and Engineering. "The security strategies employed to store this information are extremely energy inefficient and are vulnerable to data breaches and hacking."

Cloud encryption is a current mode of security that converts data into a code to prevent unauthorized access. Popular messaging system WhatsApp, for example, uses the method, theoretically ensuring only the devices involved in the chat can access private messages. However, in practice, cloud encryptions are vulnerable to data leaks and are frequent targets for adversaries, according to researchers.

"Although software-based security modules are powerful, there exists a multitude of challenges with them," said first author Akhil Dodda, a Penn State engineering science and mechanics doctoral student. "We

developed a cryptographic platform using a two-dimensional material to overcome these security limitations."

Commonly used to make transistors used in cellphones, silicon would not work to build a transistor small enough to save on energy use, researchers said. Instead, they turned to 2D materials, specifically molybdenum disulfide (MoS2), which is less than one nanometer thick, to create a low-power cryptographic chip. Penn State collaborators Joan Redwing, distinguished professor of materials science and engineering and electrical engineering, and Nicholas Trainor, a doctoral student in materials science and engineering, worked together to synthesize the MoS2 needed to create the chip.

The chip employs 320 MoS2 transistors that each have a sensing unit, a storage unit and a computing unit to encrypt the data. To test the strength of the encryption process, researchers used machine learning algorithms, which allowed them to study the output patterns and predict input information.

"We found that the advanced machine learning techniques couldn't decode the encrypted information, reinforcing the resilience of the encryption process against machine learning attacks," Das said. "Without prior knowledge of the information channels and decoding variables, it is extremely difficult to decode the information."

Additionally, the researchers said, the energy consumed in encrypting the information was significantly less than silicon-based security methods. The result was a low-power, all-in-one chip that could sense, store, compute and communicate information among connected devices—a potential solution for users who want added security but cannot afford to drain their handheld device batteries in day-to-day use.

"In the near future, we plan to reach out to federal agencies and private

corporations who specialize in smart security to extend and expand the scope of our work," Das said.

More information: Akhil Dodda et al, All-in-one, bio-inspired, and low-power crypto engines for near-sensor security based on two-dimensional memtransistors, *Nature Communications* (2022). DOI: 10.1038/s41467-022-31148-z

Provided by Pennsylvania State University

Citation: Smart chip senses, stores, computes and secures data in one low-power platform (2022, July 20) retrieved 17 June 2024 from https://techxplore.com/news/2022-07-smart-chip-low-power-platform.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.