Stopping the silent snitches of the smart world

Batteryless devices are everywhere; Ozgur Ozmen and team are working to make sure they don’t spill your secrets

By Kelly deVos, ASU News
May 22, 2025

The world is full of small batteryless devices. And they don’t mind their own business.

That solar-powered sensor by the window? Great at harvesting light — and maybe leaking your occupancy habits at the same time.

Water sensors meant to save the day? A hacker could trick them into reporting leaks that never happened — or worse, silence them entirely.

Even wildfire detectors, designed to alert us at the first sign of danger, can be taken offline by a determined cybercriminal.

These devices might not stay powered long enough to get security updates, and enforcing privacy rules can take more energy than they’ve got. Batteryless devices may be convenient — but they may also be just one glitch away from betrayal.

Thankfully, Ozgur Ozmen is here to protect us.

Ozmen is an assistant professor of computer science and engineering in the School of Computing and Augmented Intelligence, part of the Ira A. Fulton Schools of Engineering at Arizona State University. He studies the systems used to protect the myriad of increasingly common batteryless devices that can be found in homes and offices.

“It’s critical for privacy and safety that we protect these devices,” he says. “Batteryless devices are in widespread use in hospitals, factories and industrial settings. If hackers gain access to them, it creates vulnerabilities in those environments.”

Ozmen is also a researcher in the Secure, Trusted, and Assured Microelectronics Center, or STAM Center — a consortium of six laboratories at ASU working to prepare students for challenging careers in securing microelectronics.

Keeping devices under cryptographic lock and key

In his STAM Center role, Ozmen is creating research experiences for students at all levels, preparing them to secure batteryless devices from increasingly sophisticated hackers.

Hui Zhuang is one such student. The rising junior studying computer science worked with Ozmen on a project that explored the use of cryptographic keys to secure batteryless devices.

“I’ve always had an above-average sense of paranoia,” Zhuang says, jokingly. “While I was taking CSE 230: Computer Organization and Assembly Language Programming, I thought a lot about how easy it would be to hack certain systems and what hackers could achieve in the process.”

That feeling led Zhuang to seek out undergraduate research opportunities. For the project, she set up a series of batteryless light sensors connected to the solar panels designed to be their only power source, mimicking the kinds of setups in use by streetlights and in hotels. Her goal was to develop a system wherein the devices could communicate securely with each other while resisting unauthorized access.

Working under Ozmen’s supervision and with computer science doctoral student Nges Brian Njungle, Zhuang studied three big areas: making sure batteryless devices could communicate securely, keeping private information from accidentally leaking, and protecting the devices from attacks that disrupted their energy supply.

She then turned her attention to making sure the devices could communicate only when using a cryptographic key.

A cryptographic key is a type of digital tool that transforms data like a high-tech blender, turning readable plain text into encrypted mush, or ciphertext, that only an authorized user or device can decode.

Zhuang researched the two main types of keys: symmetric, where both sides use the same key, like a shared secret handshake; and asymmetric, where one key locks access to the device and a different one unlocks it, like a digital padlock.

“The goal was to create a secure way of communicating,” Zhuang says. “We wanted to have the information that the devices were transmitting be meaningless unless the user had the key.”

Over the course of the semester, Zhuang tackled tough technical challenges, finding both inspiration and difficulty in a relatively new area of research. She encountered real-world problems during her testing: The sensors were very sensitive to light; they didn’t necessarily charge at the same rate; they weren’t always active at the same time.

After spending the semester getting the system up and running, Zhuang presented her work at the spring 2025 Fulton Forge Student Research Expo, which showcases projects that are part of the Fulton Undergraduate Research Initiative, or FURI.

Low power, high security

Ozmen and the team also authored a research paper that was published at the Sensors Security and Privacy Workshop, part of the Cyber-Physical Systems and Internet-of-Things Week conference held in Irvine, California, earlier this month. For this work, Ozmen collaborated with Habiba Farrukh, an assistant professor of computer science at the University of California, Irvine.

Batteryless devices are here to stay — and their benefits are clear. But to unlock their full potential, Ozmen says we must rethink how we approach cybersecurity and privacy in a world where the devices can't always be counted on to stay powered on.

He says he is proud of Zhuang's work and excited to provide students with impactful research opportunities.

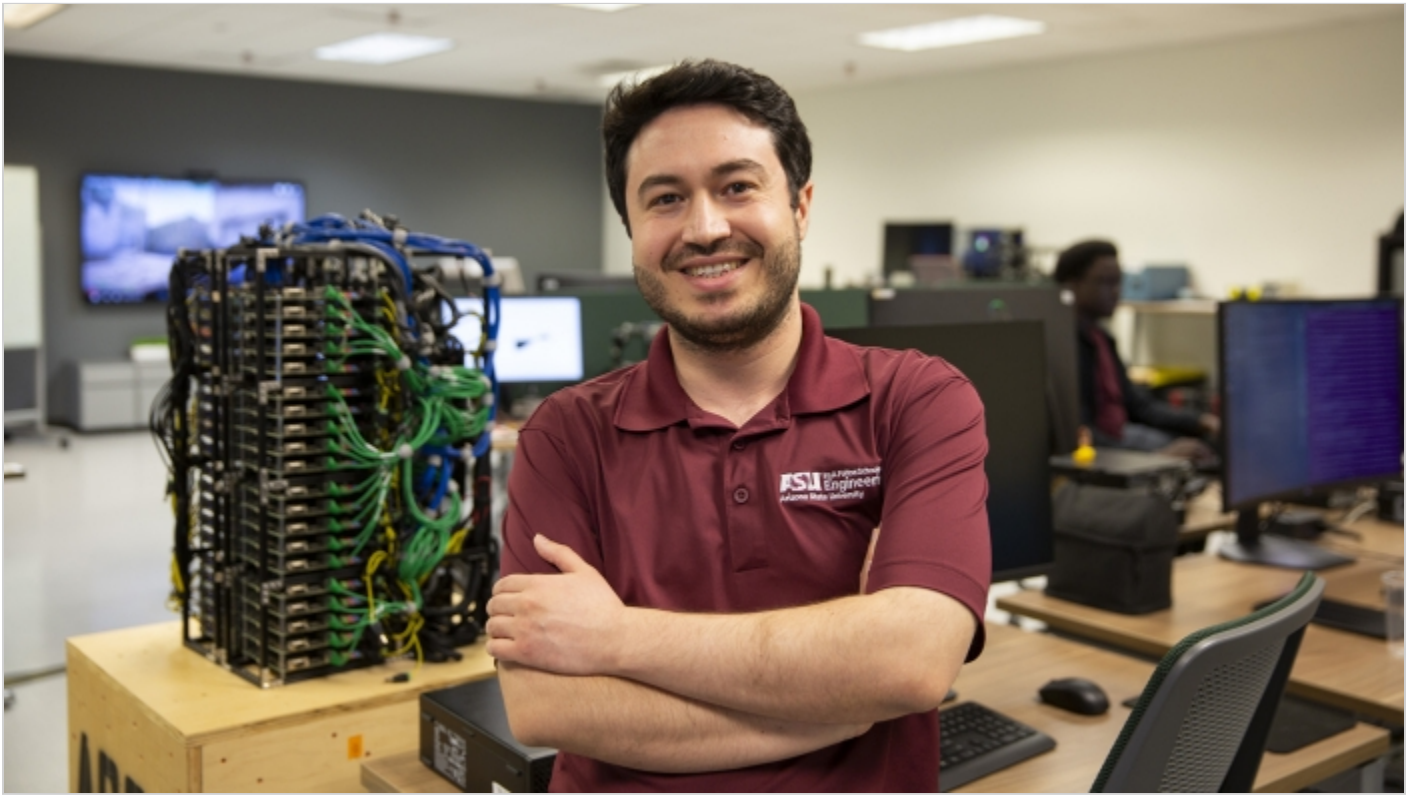
Zhuang hopes that the team's work will make a real difference for real people, creating unhackable homes, secure C-suites and sensor-hardened factories where safety and privacy can't be switched off with the lights.

She is also happy to remain a technologist who's skeptical of technology.

"Sometimes I think, 'How can we even trust technology?'" she says with a laugh. "That's why I like to design and test my own stuff."

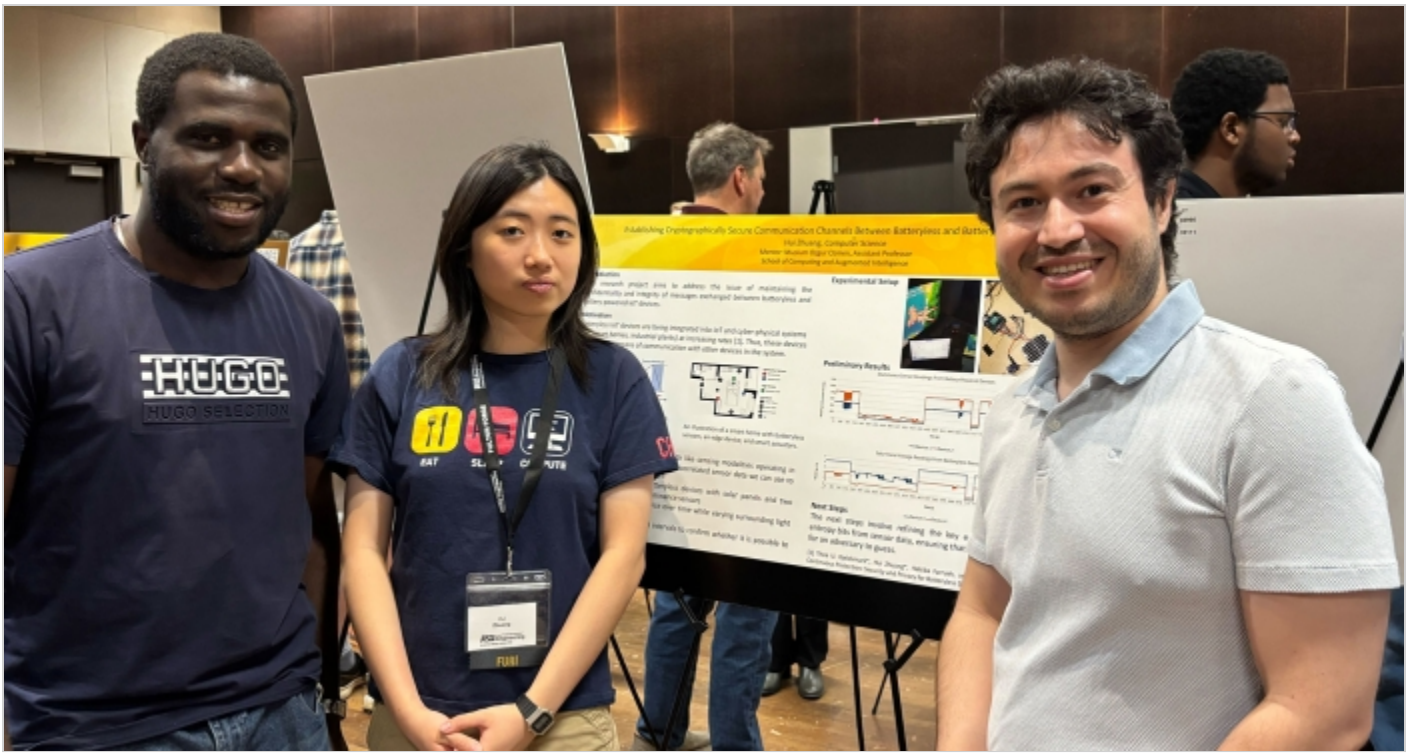
This story originally appeared on ASU News.

Main image



Ozgur Ozmen poses for a photo in the Secure, Trusted, and Assured Microelectronics Center, or STAM Center — a consortium of six laboratories focused on preparing students for roles in the microelectronics sector. Ozmen is an assistant professor of computer science and engineering in ASU's School of Computing and Augmented Intelligence, where he is guiding students through research projects to secure batteryless devices. Photo by Erika Gronek/ASU

Text image(s)



(From left) Computer science doctoral student Nges Brian Njungle, computer science undergraduate student Hui Zhuang and Assistant Professor Ozgur Ozmen. The team displays the results of their research project at the spring 2025 Fulton Forge Student Research Expo. Photo courtesy of Ozgur Ozmen