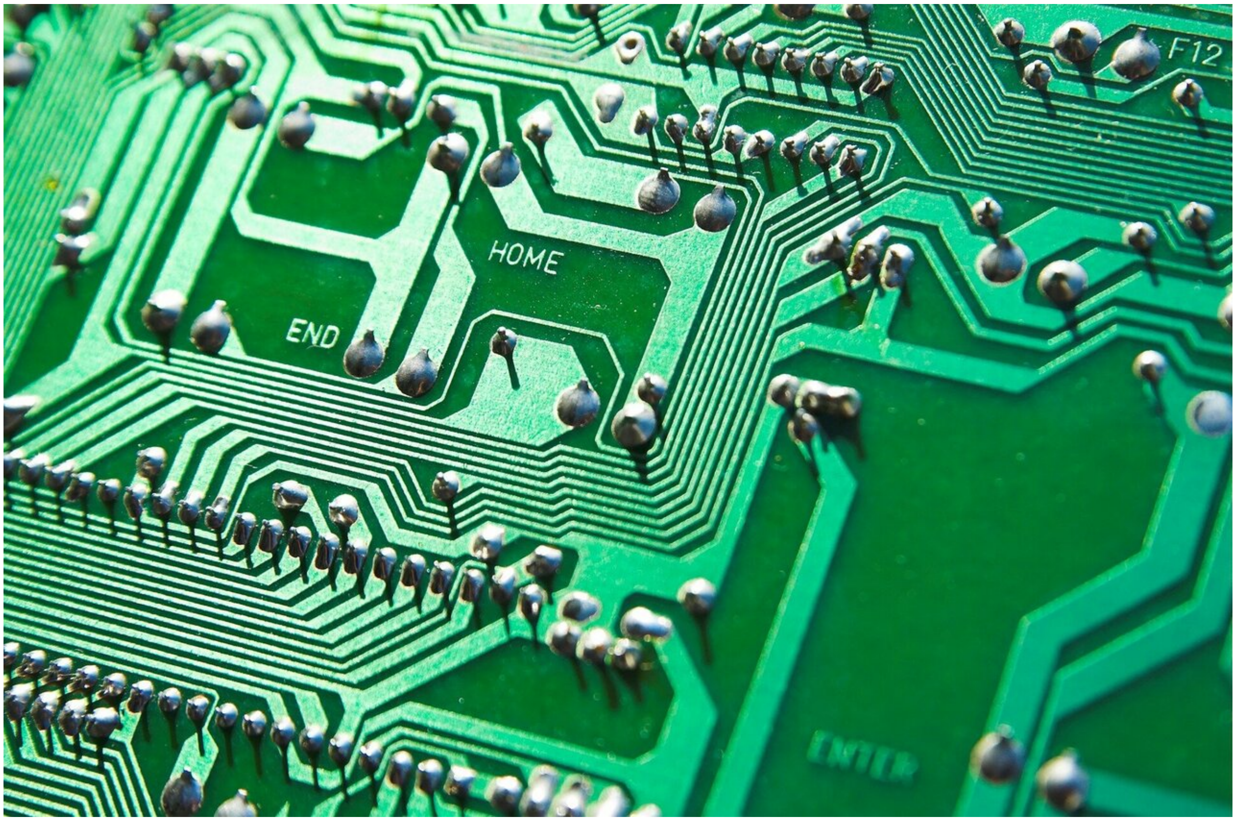
PHYS.ORG

Researcher using computer vision, machine learning to ensure the integrity of integrated circuits

January 21 2019, by Steve Martin



Credit: CC0 Public Domain

David Crandall is an associate professor in the School of Informatics, Computing and Engineering at Indiana University Bloomington. He, Sara

Skrabalak and Martin Swany are the first IU researchers whose work is being advanced through the Indiana Innovation Institute, or IN3.

IN3, a statewide applied research institute, is composed of top leaders from academia, government and industry. It seeks to solve real-world problems that impact industry and the U.S. Department of Defense in a faster, more efficient and cost-effective way. Currently, it is engaged in projects focused on trusted microelectronics, hypersonics, electro-optics and target machine learning.

Crandall was kind enough to answer questions about his work with computer vision and machine learning and about the benefits of connecting with IN3.

Q: Tell us about your work on trusted microelectronics.

David Crandall: Our role in this project is to use computer vision and machine learning techniques to help ensure the integrity of the supply chain around microelectronics. One way is to use computer vision to inspect integrated circuits to see whether there is something suspicious that might suggest they are damaged or counterfeit.

The goal of computer vision is for computers to be able to understand the visual world the way people do. Computers have been able to take and store pictures for decades, but they haven't been able to know what is in a photo—what objects and people are in it, what is going on, and what is about to happen. People do this automatically, almost instantly, and we think nothing of it. It's really hard for a computer. But computer vision is changing that, and the field has made huge progress in the last few years.

The challenge of the computer vision work we're doing with IN3—and with a lot of real-world problems—is that it requires very fine-grain analysis. We're not trying to distinguish cats from dogs or cars from pedestrians; we're trying to find very subtle differences in integrated circuits that might signal a problem. That's really the challenge: to bring techniques that have been successful in the last few years in consumer photography to this new field that has unique challenges.

Q: Why is it important to monitor integrated circuits?

DC: Integrated circuits form the foundation of all devices we use on a daily basis, from cellphones to critical national infrastructure. It's really important that the circuits in these devices are reliable, that they do what they say and that they're built to the specifications that we need them to be built to.

Electronic devices and integrated circuits are manufactured in plants throughout the world. They traverse a complicated supply chain to get between where they're manufactured and where they're placed into devices. A lot can go wrong in that process. Integrated circuits can be swapped or replaced for various reasons—people wanting to make a bit of a profit by substituting a cheaper device for one that's more expensive, or for more nefarious reasons like hacking. We want to ensure the integrity of the integrated circuits so that the devices built out of them do what they are supposed to do.

The problem is really important. Modern society depends on the safe, secure, reliable operation of digital devices. If they can't be trusted, that rips apart a lot of what our society is based on. We—researchers in the state of Indiana—are in a unique position to attack this problem because of Purdue's expertise in microelectronics; Naval Surface Warfare Center Crane's capabilities; and IU's expertise with chemistry, machine learning and engineering. We're in the right place at the right time to have a real impact on this problem.

Q: How do you monitor integrated circuits? What challenges are there?

DC: My understanding is that current approaches to detecting counterfeit devices are either limited in their accuracy or must be done by hand, which is expensive and time-consuming. If we can create new automated techniques that could complement or improve these approaches, we can potentially ensure that more devices are inspected.

There are many possible approaches. One is to use computer vision to inspect the surface of a package of an integrated circuit, checking the part number and looking for suspicious visual features that might indicate it has been modified. Another approach uses Sara Skrabalak's work in adding uncloneable fingerprints to integrated circuit packages and using computer vision techniques to verify that they are authentic. We can also inspect the internal circuitry of the integrated circuit using various imaging techniques.

Q: How have your connections with IN3 benefited your work?

DC: An exciting vision of IN3 is to bring together groups of people working in different areas, who might not otherwise have thought to collaborate with one another, in order to jointly solve big problems that none of us could address individually. It's not only bringing together groups at IU, but also creating stronger connections between IU and Purdue, Notre Dame and NSWC Crane.

I work in computer vision and artificial intelligence. We're looking for ways to apply these techniques to new, important, exciting problems. As we apply them, we discover new technical challenges, which leads us to go back to the drawing board to create new, better algorithms. I don't have deep expertise in microelectronics, so I wouldn't be able to impact this field alone. Collaborating with experts via IN3 will be the way we impact their field and bring back important, interesting problems for us to work on as well.

Q: What might some end results be when the tech is widely adopted?

DC: The end goal is to help transform microelectronics security so we can have more faith in the devices that we depend on, from voting machines to cellphones to laptop computers to critical infrastructure across the country. There was a recent story in Bloomberg about critical hardware that perhaps had been hacked. Whether or not that story was true, the motivation behind our project is to make sure something like that doesn't happen in the future.

Provided by Indiana University

Citation: Researcher using computer vision, machine learning to ensure the integrity of integrated circuits (2019, January 21) retrieved 18 April 2024 from https://phys.org/news/2019-01-vision-machine-circuits.html