How secure is your security camera? Hackers can spy on cameras through walls, new research finds

February 11 2024, by Cody Mello-Klein

Credit: Matthew Modoono/Northeastern University

When it comes to protecting a bank or even your home, security cameras are on one of the first lines of defense. But what if those cameras aren't

as secure as we all think?

New research from Northeastern University confirms that there might be a massive gap in our security infrastructure—and it comes from the very devices designed to protect it.

Kevin Fu, a professor of electrical and computer engineering at Northeastern who specializes in cybersecurity, has figured out a way to eavesdrop on most modern cameras, from home security cameras and dash cams to the camera on your phone. Called EM Eye, short for Electromagnetic Eye, the technique can capture the video from another person's camera through walls in real time. It redefines the idea of a Peeping Tom.

According to Fu, anyone with a few hundred dollars of equipment, a radio antenna and a little bit of engineering know-how could do this. The problem, Fu says, is not the lens but the wires inside most modern cameras.

"With your typical security camera, on the inside there's a camera lens and then there's got to be something else on the inside, like a computer chip, that's got a wireless connection back to the internet," Fu says. "There are wires between two different chips inside [these cameras,] and those wires give off electromagnetic radiation. We pick up that radio, and then we decode it and it just happens to be that we get the real-time encoded video."

The data transmission cable that sends a video as bits and bytes ends up unintentionally acting as a radio antenna that leaks all kinds of electromagnetic information, including those bits and bytes. If someone had the desire and the technical knowledge, they could take that electromagnetic signal and reproduce the real-time video, without audio.

The technique exposes a gap in how manufacturers approach the design and production of cameras.

"The state of modern smartphone cameras is [manufacturers] try really hard to protect the intentional digital interfaces, the actual upload channel to the cloud," Fu says. "They don't appear to put a lot of effort into the leakage of information through unintended channels. They never intended for this wire to become a radio transmitter, but it is."

The version of the video that Fu and his team get is initially distorted—it looks almost like an X-ray—due to pixel loss in the process of being transmitted. However, using machine learning, Fu and his team were able to clean up the video to appear much closer to the original.

Fu and his team have tested EM Eye on 12 different kinds of cameras, including smartphone cameras, dash cams and home security cameras. Results vary on how far away someone would have to be in order to eavesdrop on these different devices. For some, a peeping Tom would have to be less than 1 foot away; for others, they could be as far away as 16 feet.

However, he says, if someone had enough technical know-how, it would take very little to extend that range.

"A sophomore or junior in college could probably do it, but it does get into electrical and computer engineering skills to boost that distance," Fu says.

More importantly, since EM Eye eavesdrops on the wires, not a computer recording footage to a hard drive, your camera doesn't actually have to be recording in order for someone to eavesdrop on it.

"If you have your lens open, even if you think you have the camera off,

we're collecting," Fu says. "Basically, anywhere there's a camera, now there's a risk of that live real-time feed being collected by someone as close as a meter or so through walls."

For consumers, Fu says a plastic lens cover might not be guaranteed to protect you—infrared signals can still get through them—but it is a good first step to battling this kind of cyberthreat.

"There's the classic: Be aware of your surroundings," Fu says. "Maybe you don't want to put this [camera] on your wall you share with your neighbor."

As for camera manufacturers, Fu hopes these findings are a wake-up call.

"It's nice that we have all this software and these … devices, but at the end of the day, they [emit] electrons and they can get out," Fu says. "If you want to have a complete cybersecurity story, yes, do the good science, but you also have to do the computer engineering and the electrical engineering if you want to protect against these kinds of eavesdropping surveillance threats."

More information: EM Eye: Characterizing Electromagnetic Side-channel Eavesdropping on Embedded Cameras. www.ndss-symposium.org/wp-cont … 024_f552_paper-1.pdf

Provided by Northeastern University