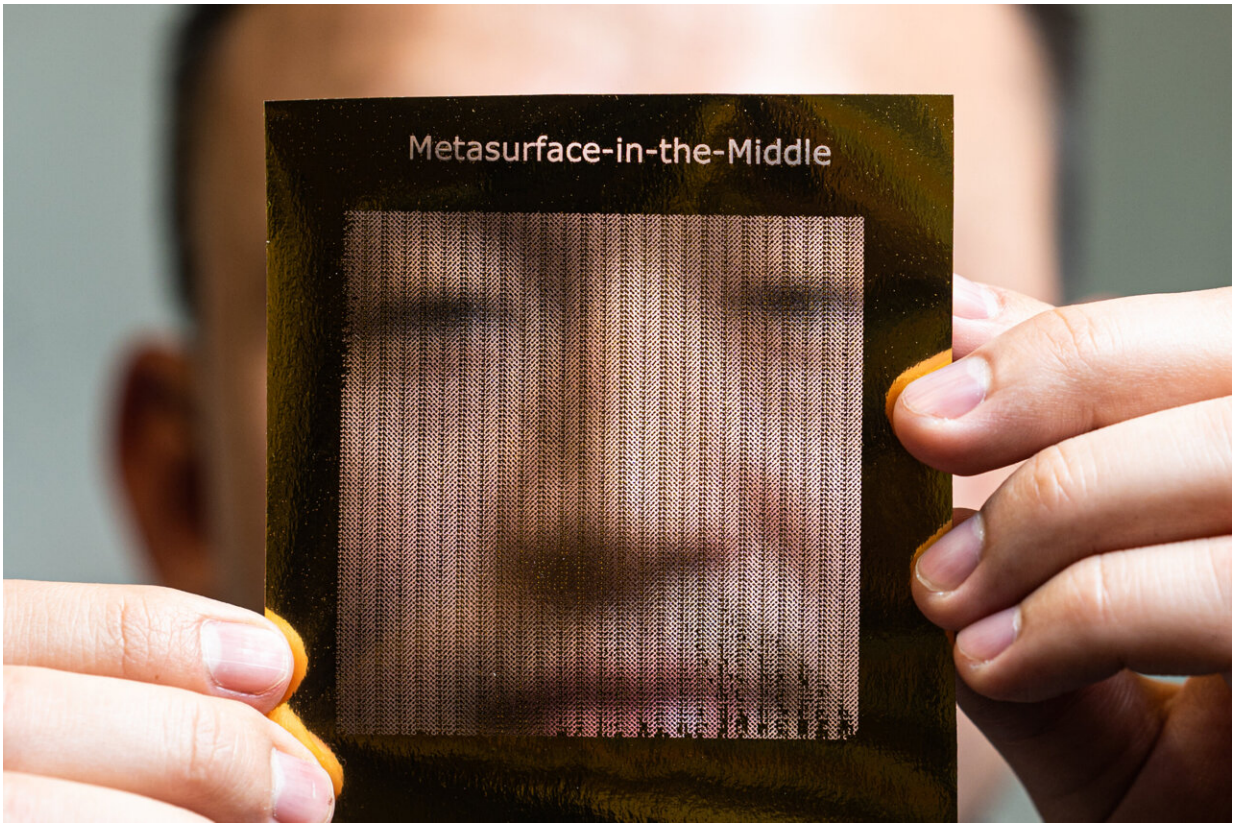
Eavesdroppers can hack 6G frequency with DIY metasurface

May 16 2022



Rice University graduate student Zhambyl Shaikhanov holds a foil sheet he used to create a "metasurface"—a paper sheet covered with a 2D foil pattern—that an eavesdropper could use in a "Metasurface-in-the-Middle" attack to redirect part of a high-frequency "pencil beam" transmission like those planned for 6G wireless networks. Credit: Jeff Fitlow/Rice University

Crafty hackers can make a tool to eavesdrop on some 6G wireless signals in as little as five minutes using office paper, an inkjet printer, a metallic foil transfer and a laminator.

The wireless security hack was discovered by engineering researchers from Rice University and Brown University, who will present their findings and demonstrate the attack this week in San Antonio at ACM WiSec 2022, the Association for Computing Machinery's annual conference on security and privacy in wireless and mobile networks.

"Awareness of a future threat is the first step to counter that threat," said study co-author Edward Knightly, Rice's Sheafor-Lindsay Professor of Electrical and Computer Engineering. "The frequencies that are vulnerable to this attack aren't in use yet, but they are coming and we need to be prepared."

In the study, Knightly, Brown University engineering Professor Daniel Mittleman and colleagues showed an attacker could easily make a sheet of office paper covered with 2D foil symbols—a metasurface—and use it to redirect part of a 150 gigahertz "pencil beam" transmission between two users.

They dubbed the attack "Metasurface-in-the-Middle" as a nod to both the hacker's tool and the way it is wielded. Metasurfaces are thin sheets of material with patterned designs that manipulate light or electromagnetic waves. "Man-in-the-middle" is a computer security industry classification for attacks in which an adversary secretly inserts themself between two parties.

The 150 gigahertz frequency is higher than is used in today's 5G cellular or Wi-Fi networks. But Knightly said wireless carriers are looking to roll out 150 gigahertz and similar frequencies known as terahertz waves or millimeter waves over the next decade.

"Next-generation wireless will use high frequencies and pencil beams to support wide-band applications like virtual reality and autonomous vehicles," said Knightly, who will present the research with co-author Zhambyl Shaikhanov, a graduate student in his lab.

In the study, the researchers use the names Alice and Bob to refer to the two people whose communications are hacked. The eavesdropper is called Eve.

To mount the attack, Eve first designs a metasurface that will diffract a portion of the tight-beam signal to her location. For the demonstration, the researchers designed a pattern with hundreds of rows of split rings. Each looks like the letter C, but they are not identical. The open part of each ring varies in size and orientation.

"Those openings and orientations are very specifically done to get the signal to diffract in the exact direction Eve wants," Shaikhanov said. "After she designs the metasurface, she prints it on a regular laser printer, and then she uses a hot stamping technique that's used in crafting. She places a metal foil on the printed paper, feeds it through a laminator and the heat and pressure create a bond between the metal and the toner."

Mittleman and study co-author Hichem Guerboukha, a postdoctoral research fellow at Brown, showed in a 2021 study that the hot-stamping method could be used to make split-ring metasurfaces with resonances up to 550 GHz.

"We developed this approach in order to lower the barrier for fabrication of metasurfaces, so that researchers could test many different designs quickly and inexpensively," Mittleman said. "Of course, this lowers the barrier for eavesdroppers too."

The researchers said they hope the study will dispel a common misperception in the wireless industry that higher frequencies are inherently secure.

"People have been quoted saying millimeter-wave frequencies are 'covert' and 'highly confidential' and that they 'provide security,'" Shaikhanov said. "The thinking is, 'If you have a super narrow beam, nobody can eavesdrop on the signal because they would have to physically get between the transmitter and the receiver.' What we've shown is that Eve doesn't have to be obtrusive to mount this attack."

The research showed the attack would be difficult for Alice or Bob to detect today. And while the metasurface must be placed between Alice and Bob, "it could be hidden in the environment," Knightly said. "You could conceal it with other sheets of paper, for instance."

Knightly said now that wireless researchers and equipment manufacturers know about the attack, they can further study it, develop detection systems and build those into terahertz networks up front.

"If we had known from day one, when the internet first came out, that there would be denial-of-service attacks and attempts to take down web servers, we would have designed it differently," Knightly said. "If you build first, wait for attacks and then try to repair, that is a much more costly and expensive path than designing securely up front."

"Millimeter-wave frequencies and metasurfaces are new technologies that can each be used to advance communication, but any time we get a new capability for communication we have to ask the question, 'What if the adversary has this technology? What new capabilities will it give them that they didn't have in the past? And how can we realize a secure network against a strong adversary?"

More information: Zhambyl Shaikhanov et al, Metasurface-in-the-Middle Attack, *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (2022). DOI: 10.1145/3507657.3528549

Hichem Guerboukha et al, High-volume rapid prototyping technique for terahertz metallic metasurfaces, *Optics Express* (2021). DOI: 10.1364/OE.422991

Provided by Rice University