New 5G Research; “the interfaces that carriers have set up to manage Internet-of-things data are riddled with security vulnerabilities”

Description

Experts have been warning about significant cybersecurity vulnerabilities with 5G and Internet of Things (IoT) technologies FOR YEARS (see 1, 2, 3, 4, 5). New research provides more reasons to avoid using these technologies.

From Ars Technica:

One of 5G’s biggest features is a security minefield

There are vulnerabilities in 5G platforms carriers offer to wrangle embedded device data.

Lily Hay Newman, wired.com

True 5G wireless data, with its ultrafast speeds and enhanced security protections, has been slow to roll out around the world. As the mobile technology proliferates—combining expanded speed and bandwidth with low-latency connections—one of its most touted features is starting to come in to focus. But the upgrade comes with its own raft of potential security exposures.

A massive new population of 5G-capable devices, from smart-city sensors to agriculture robots and beyond, are gaining the ability to connect to the Internet in places where Wi-Fi isn’t practical or available. Individuals may even elect to trade their fiber-optic Internet connection for a home 5G receiver. But the interfaces that carriers have set up to manage Internet-of-things data are riddled with security vulnerabilities, according to research presented this week at the Black Hat security conference in Las Vegas. And those vulnerabilities could dog the industry long-term.

After years of examining potential security and privacy issues in mobile-data radio frequency standards, Technical University of Berlin researcher Altaf Shaik says he was curious to investigate the application programming interfaces (APIs) that carriers are offering to make IoT data accessible to developers. These are the conduits that applications can use to pull, say, real-time bus-tracking data or

information about stock in a warehouse. Such APIs are ubiquitous in web services, but Shaik points out that they haven't been widely used in core telecommunications offerings. Looking at the 5G IoT APIs of 10 mobile carriers around the world, Shaik and his colleague Shinjo Park found common but serious API vulnerabilities in all of them, and some could be exploited to gain authorized access to data or even direct access to IoT devices on the network.

"There's a big knowledge gap. This is the beginning of a new type of attack in telecom," Shaik told WIRED ahead of his presentation. "There's a whole platform where you get access to the APIs, there's documentation, everything, and it's called something like 'IoT service platform.' Every operator in every country is going to be selling them if they're not already, and there are virtual operators and subcontracts, too, so there will be a ton of companies offering this kind of platform."

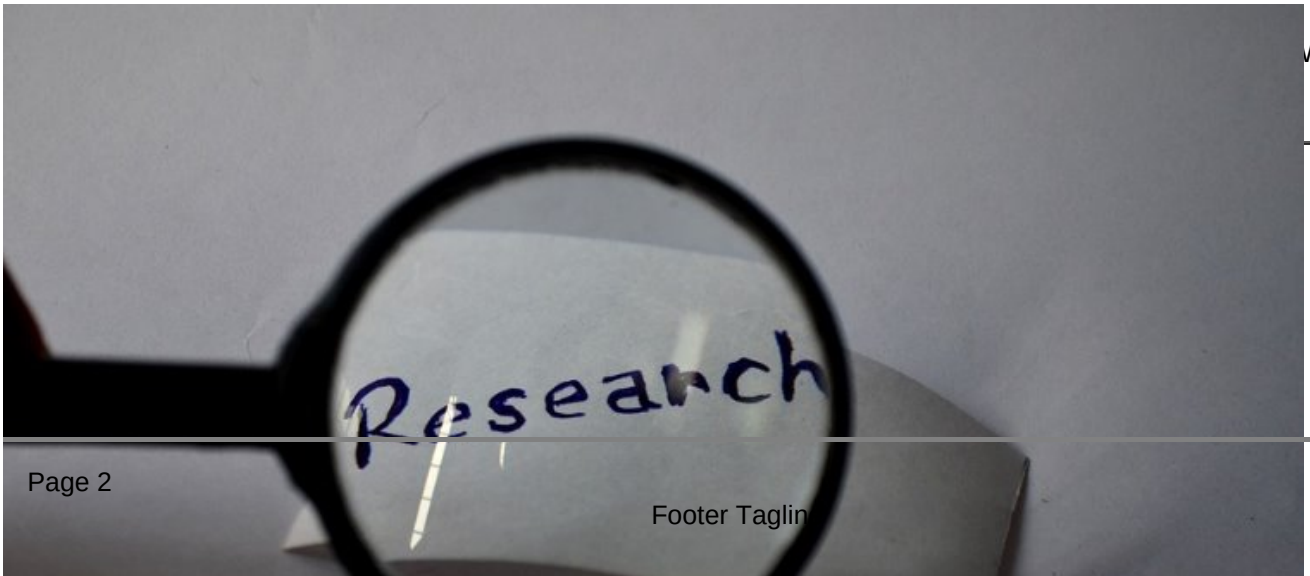
The designs of IoT service platforms aren't specified in the 5G standard and are up to each carrier and company to create and deploy. That means there's widespread variation in their quality and implementation. In addition to 5G, upgraded 4G networks can also support some IoT expansion, widening the number of carriers that may offer IoT service platforms and the APIs that feed them.

The researchers bought IoT plans on the ten carriers they analyzed and got special data-only SIM cards for their networks of IoT devices. This way, they had the same access to the platforms as any other customer in the ecosystem. They found that basic flaws in how the APIs were set up, like weak authentication or missing access controls, could reveal SIM card identifiers, SIM card secret keys, the identity of who purchased which SIM card, and their billing information. And in some cases, the researchers could even access large streams of other users' data or even identify and access their IoT devices by sending or replaying commands that they shouldn't have been able to control.

The researchers went through disclosure processes with the 10 carriers they tested and said that the majority of vulnerabilities they found so far are being fixed. Shaik notes that the quality of security protections on the IoT service platforms varied widely, with some appearing more mature while others were "still sticking to the same old bad security policies and principles." He adds that the group isn't publicly naming the carriers they looked at in this work because of concerns about how widespread the issues might be. Seven of the carriers are based in Europe, two are in the US, and one is in Asia.

"We found vulnerabilities that could be exploited to access other devices even though they don't belong to us, just by being on the platform," Shaik says. "Or we could talk to other IoT devices and send messages, extract information. It's a big issue."

Shaik emphasizes that he and his colleagues didn't hack any other customers or do anything improper once they discovered the different flaws. But he points out that none of the carriers detected the researchers' probing, which in itself indicates a lack of monitoring and safeguards, he says.



there have been additional issues reported about the use of 5G technology by aviation groups, government agencies, and telecom companies (see 1, 2, 3, 4, 5, 6). Research and warnings about health risks from exposure – including to pilots – continue to be reported as well.

Opposition to 5G is worldwide and this has limited, slowed, and/or stopped deployment in some locations (see 1, 2, 3, 4). Since 2017 doctors and scientists have asked for moratoriums on Earth and in space (see 1, 2) *and* the majority of scientists oppose deployment. Since 2018 there have been reports of people and animals experiencing symptoms and illnesses after it was activated (see 1, 2, 3, 4, 5). In 2019, telecom executives gave congressional testimony that they had NO independent scientific evidence that 5G is even safe! Some researchers have also suggested that 5G activation may be contributing to COVID-19 infections as well as hundreds of thousands if not millions of bird deaths. Of course, there are health and environmental risks associated with 4G and other sources of wireless Wi-Fi radiation (see 1, 2) and electromagnetic fields (aka "Electrosmog") too. Regardless, 5G and IoT proponents continue to downplay or simply ignore ALL risks associated with these technologies as well as promote its not-entirely-without-risk successor, 6G.

By B.N. Frank

Category

1. Freedom-Free speech-Resitance & H-rights
2. Health-Wellness-Healing-Nutrition & Fitness
3. Main
4. Science-Tech-AI-Medical & Gen. Research

Date Created
08/14/2022