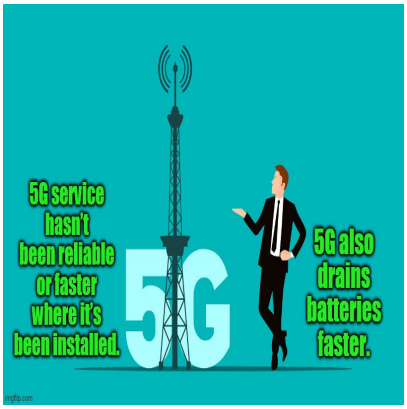

Another 5G Service Woe: “You’re potentially susceptible to tracking, eavesdropping, and so-called “downgrade attacks”

Description

By B.N. Frank

Even if you aren’t opposed to 5G deployment due to concerns about reduced property value (see 1, 2, 3, 4), public safety (see 1, 2, 3, 4, 5, 6, 7, 8, 9), health (see 1, 2, 3, 4, 5, 6, 7, 8, 9, 10), cybersecurity (see 1, 2), privacy (see 1, 2), economic, and/or environmental risks (see 1, 2, 3, 4, 5) – consumer reports have indicated that 4G service is still better and safer than 5G (see 1, 2, 3, 4, 5). In fact, now experts are warning that 5G phones are more susceptible to unwanted surveillance.

From Wired:

A 5G Shortcut Leaves Phones Exposed to Stingray Surveillance

You may not have the full story about what network you’re on—and how well you’re protected.

In North America and many other parts of the world, high-speed 5G mobile data networks dangled just out of reach for years. But as 5G coverage becomes ubiquitous, the rollout comes with an important caveat. Even if your phone says it’s connected to the next-generation wireless standard, you may not actually be getting all of the features 5G promises—including defense against so-called stingray surveillance devices.

To get 5G out to the masses quickly, most carriers around the world deployed it in something called “non-standalone mode” or “non-standalone architecture.” The approach essentially uses existing 4G network infrastructure as a jumping off point to put out 5G data speeds before the separate, “standalone” 5G core is built. It’s like starting your cake-decorating business out of your cousin’s ice cream shop while you renovate a new storefront three blocks away.

You may see where this is going. As long as your 5G connection is in non-standalone mode, a lot of what you’re getting is still actually 4G, complete with security and privacy weaknesses that *actual* 5G

aims to address.

“It’s a false sense of security,” says Ravishankar Borgaonkar, a research scientist at the Norwegian tech analysis firm SINTEF Digital and associate professor at University of Stavanger. “Currently a lot of the 5G deployed all over the world doesn’t actually have the protection mechanisms designed in 5G. You’re getting the high speed connection, but the security level you have is still 4G.

In practice, that means one of 5G’s top-billed privacy benefits—the ability to stymie stingray surveillance—does not yet apply for most people. Also known as “IMSI catchers” for the “international mobile subscriber identity” number assigned to every cell phone, stingrays act like legitimate cell towers and trick devices into connecting. From there, the tools use IMSI numbers or other identifiers to track the device, and even listen in on phone calls. Stingrays are a popular choice among US law enforcement; they were a reportedly common presence at many of last summer’s anti-police brutality protests. To prevent that sort of monitoring, 5G is built to encrypt IMSI numbers.

Borgaonkar and fellow researcher Altaf Shaik, a senior research scientist at TU Berlin, found that major carriers in Norway and Germany are still putting out 5G in non-standalone mode, which means that those connections are still susceptible to stingrays. The two presented at the Black Hat security conference in Las Vegas last week.

In the United States, T-Mobile is the farthest along in rolling out its standalone network. The company was the first to begin mass-deployment in August 2020. Verizon and AT&T have taken longer to transition and are still working on switching to high speed 5G in general. Verizon told WIRED that it is on track for “full commercialization” of 5G standalone mode by the end of 2021. AT&T says that it began “limited SA deployments” late last year, and that it will scale up “when the ecosystem is ready.”

A February study by the mobile network analytics firm OpenSignal found that at the beginning of 2021 US mobile users spent about 27 percent of their time on non-standalone mode 5G and less than six percent of their time on standalone mode connections.

While the distinctions between the types of 5G matter a great deal, there’s no easy way to tell whether you’re on a standalone network just by looking at your phone. Android users can download apps that analyze a device’s network connection and can flag non-standalone mode, but that’s an onerous extra step. And those tools are less common on iOS because of Apple’s app restrictions.

The security benefits you miss while on a non-standalone 5G network extend beyond stingrays. You’re potentially susceptible to tracking, eavesdropping, and so-called “downgrade attacks” that push target devices onto older, more vulnerable data networks like 3G. And none of this gets communicated to mobile data users, despite enhanced security features being a key 5G selling point.

Read full article

Opposition to 5G is worldwide. Cities and entire countries have taken action to ban, delay, halt, and limit installation AS WELL AS issue moratoriums. Since 2017, doctors and scientists have been asking for moratoriums on Earth and in space (see 1, 2). Since 2018 there have been reports of people and animals experiencing symptoms and illnesses after it was installed (see 1. 2, 3, 4). The majority of scientists oppose deployment.

Date Created
08/23/2021