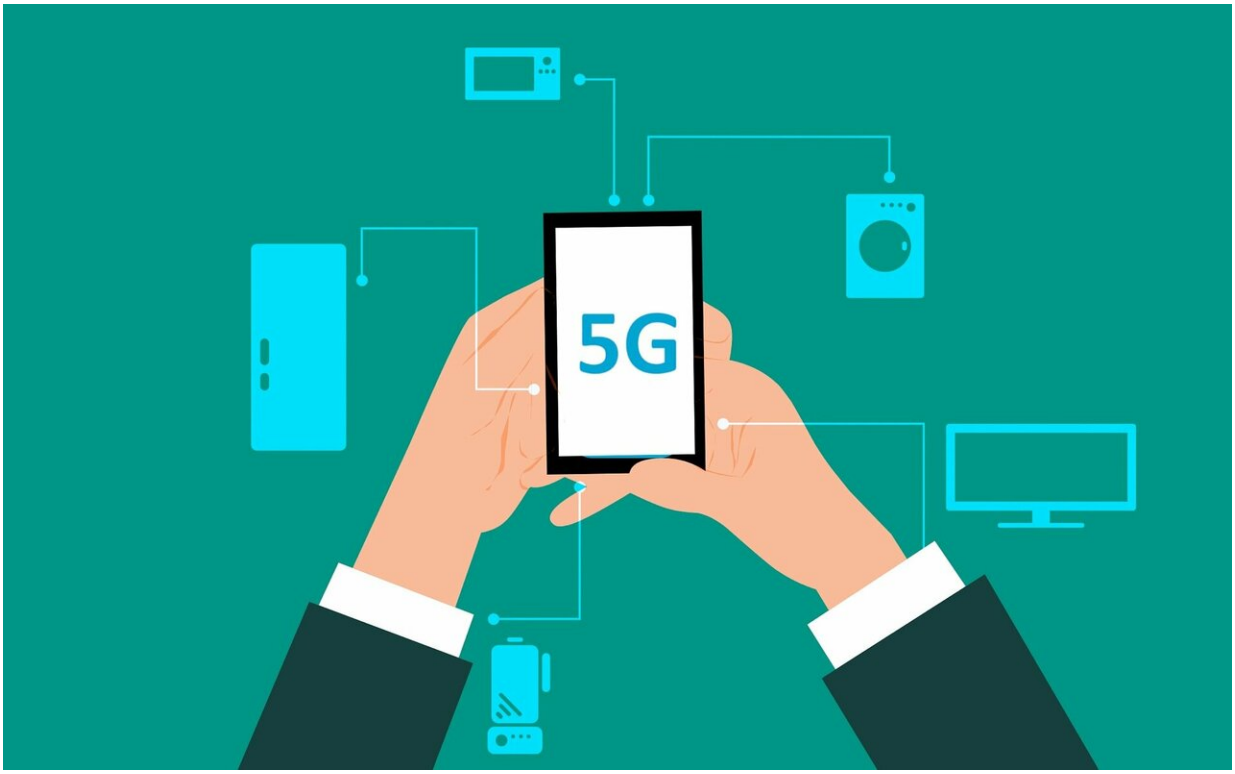
Security problems found in 5G protocol

November 14 2019, by Bob Yirka



Credit: CC0 Public Domain

A combined team of researchers from the University of Iowa and Purdue University has found nearly a dozen security breaches in the 5G protocol. They have written a paper describing both their findings and a security breaching tool they developed called 5GReasoner, and have uploaded it to the Documentcloud server.

5G is the next generation protocol for servicing smartphones—some customers are already using it. It has been developed to provide users faster and more secure service. Unfortunately, it may not be as secure as users have been hoping. The researchers with this effort have found vulnerabilities that leave users at risk of being tracked, along with several other issues.

The work by the researchers involved building the software tool 5GReasoner, which they used to test the new protocol, finding 11 vulnerabilities. Using 5GReasoner, the researchers set up a radio base station that could be used to attack phones in the nearby vicinity. They report that they were able to obtain network IDs for local phones, which in turn allowed them to discover paging occasions—and that allowed them to see the current location of a phone, which could be used to track the person using it. They report also that they were able to broadcast phony emergency alerts to phones in a given area, and in some cases, were able to track phone activity. Also, they found they could run denial-of-service systems to prevent phones from accessing their designated networks—a scheme that could result in downgraded service, or worse, no service at all.

The researchers note that some of the vulnerabilities could be used for surveillance attack by hackers or law enforcement personnel. They further report that all of the vulnerabilities they found could be exploited by anyone with a basic knowledge of either 4G or 5G networks—and that it could be done with low-cost software.

The researchers have reported their findings to the GSM Association (GMSA), which is responsible for approving international phone protocols. In response, the GMSA released a note describing the vulnerabilities as nil, or of low impact. They did not mention if the vulnerabilities would be fixed.

More information: 5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol, www.documentcloud.org/document … 4575-5GReasoner.html