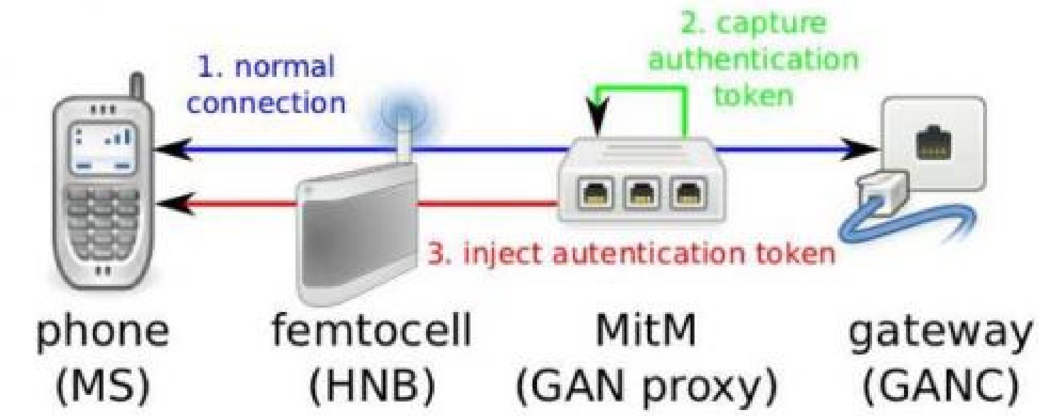
3G protocols come up short in privacy, say researchers

October 11 2012, by Nancy Owano



Experimental Attack Setup. Credit: Nico Golde et al.

(Phys.org)—Researchers from the UK and Germany have found that 3G telephony systems pose a security weakness that results in threats to user privacy. The weakness makes it possible for stalkers to trace and identify subscribers. Their paper, "New Privacy Issues in Mobile Telephony: Fix and Verification," says that 3G systems come up short in preventing unauthorized parties from tracking the physical location of users "We have shown that the protocols are vulnerable to new privacy threats and that these threats lead to attacks that can be mounted in practice at low cost."

The authors, Myrto Arapinis, Loretta Mancini, Eike Ritter, Mark Ryan of University of Birmingham, and Nico Golde, Kevin Redon, Ravishankar Borgaonkar of Ttechnische Universität Berlin and Deutsche Telekom Laboratories, note a security timeline to 3G:

When 3G protocols were first introduced in 1999, the possibility of an active attack was remote, partly because of the high cost of the equipment that would have been required and the lack of open source implementations of the protocol stack. The possibility is no longer remote. They said that cheap base stations can be produced by programming USRP (Universal Software Radio Peripheral) boards. "These lower the cost of producing radio devices thanks to software emulation of specialized functions once executed by expensive hardware."

The researchers said that devices' physical locations could be identified at any time with relative ease, as the attacker does not need to know any keys, or to get involved with "fancy cryptography." Instead, the weaknesses involve errors in the protocol logic.

Encroachments on user privacy could range from personal stalking to worker harassment to other kinds of spy operations, to commercial profiling.

The team tested phones on four networks and found they showed vulnerabilities. They tested networks of major operators T-Mobile, O2, SFR, and Vodafone. They showed that these were vulnerable to the researchers' attacks. The authors propose fixes in the paper that use public key cryptography.

"We used formal methods to show that the exposed privacy vulnerabilities could have been detected at design time. We developed and verified lightweight solutions to avoid the privacy vulnerabilities."

They noted that additional costs of using public-key cryptography are small.

"The solutions we propose show that privacy friendly measures could be adopted by the next generation of mobile telephony standards."

Citation: 3G protocols come up short in privacy, say researchers (2012, October 11) retrieved 20 March 2024 from https://phys.org/news/2012-10-3g-protocols-short-privacy.html