A backdoor in mobile phone encryption from the '90s still exists

June 16 2021

Although the insecure algorithms are still implemented in modern mobile phones, the researchers do not expect them to pose a significant threat to users. Credit: RUB, Marquard

The encryption algorithm GEA-1 was implemented in mobile phones in

the 1990s to encrypt data connections. Since then, it has been kept secret. Now, a research team from Ruhr-Universität Bochum (RUB), together with colleagues from France and Norway, has analyzed the algorithm and has come to the following conclusion: GEA-1 is so easy to break that it must be a deliberately weak encryption that was built in as a backdoor. Although the vulnerability is still present in many modern mobile phones, it no longer poses any significant threat to users, according to the researchers.

Backdoors not useful according to researchers

"Even though intelligence services and ministers of the interior understandably want such backdoors to exist, they are not at all useful," says Professor Gregor Leander, Head of the Workgroup for Symmetric Cryptography. "After all, they are not the only ones who can exploit these vulnerabilities, any other attackers can exploit them as well. Our research shows: once a backdoor is implemented, it is very difficult to remove it." Accordingly, GEA-1 should have disappeared from mobile phones as early as 2013; at least that's what the mobile phone standards say. However, the research team found the algorithm in the current Android and iOS smartphones.

For the study, a team led by Dr. Christof Beierle, Dr. David Rupprecht, Lukas Stennes and Professor Gregor Leander from RUB collaborated with colleagues from Université de Rennes and Université Paris-Saclay as well as the French research institute Center Inria de Paris and the Norwegian research institute Simula UiB in Bergen. The team will present its findings at the Eurocrypt conference in October 2021. The paper has been available online since 16 June 2021.

The project was embedded in the Bochum Cluster of Excellence CASA—short for Cyber Security in the Age of Large-Scale Adversaries –, which aims at enabling sustainable IT security against large-scale

attackers, most importantly national states.

Lottery win more likely than weak code being a coincidence

The IT security experts received the GEA-1 and GEA-2 algorithms from a source who wishes to remain anonymous and verified their authenticity in the first step. The ciphers had been used to encrypt data traffic over the 2G network, for example when sending emails or visiting websites. The researchers analyzed how exactly the algorithms work. They showed that GEA-1 generates encryption keys that are subdivided into three parts, two of which are almost identical. Due to their architecture, these keys are relatively easy to guess.

According to the Bochum-based team, the properties that render the cipher so insecure can't have happened by accident. "According to our experimental analysis, having six correct numbers in the German lottery twice in a row is about as likely as having these properties of the key occur by chance," as Christof Beierle illustrates.

GEA-2 algorithm likewise weak—but unintentionally so

The IT experts also scrutinized the GEA-2 algorithm. It is hardly more secure than GEA-1. "GEA-2 was probably an attempt to set up a more secure successor to GEA-1," assumes Gregor Leander. "GEA-2 was hardly better, though. But at least this algorithm doesn't seem to be intentionally insecure."

The encryptions that GEA-1 and GEA-2 produce are so weak that they could be used to decrypt and read live encrypted data sent over 2G. Today, most data traffic is sent over the 4G network, also called LTE.

Moreover, the data is now protected with additional transport encryption. Therefore, the researchers assume that the old vulnerabilities that still exist no longer pose a serious threat to users.

Manufacturers don't adhere to standards

Originally, GEA-1 must not be implemented in mobile devices since 2013. "The fact that it is still happening shows that manufacturers are not following the standard properly," explains David Rupprecht. Through the mobile phone association GSMA, the Bochum-based group contacted the manufacturers before publishing their data to give them the opportunity to remove GEA-1 through software updates. In addition, they contacted ETSI, the organisation responsible for telecommunications standards, to also remove GEA-2 from phones. In the future, – so ETSI's decision—smartphones should not support GEA-2 anymore.

More information: Christof Beierle et al, Cryptanalysis of the GPRS Encryption Algorithms GEA-1 and GEA-2, *Advances in Cryptology – EUROCRYPT 2021* (2021). DOI: 10.1007/978-3-030-77886-6_6

Provided by Ruhr-Universitaet-Bochum