Weakness of 2G mobile phone networks revealed

October 21 2016

The encryption scheme used for second generation (2G) mobile phone data can be hacked within seconds by exploiting weaknesses and using common hardware, A*STAR researches show. The ease of the attack shows an urgent need for the 2G Global System for Mobile Communications (GSM) encryption scheme to be updated.

GSM was first deployed 25 years ago and has since become the global standard for mobile communications, used in nearly every country and comprising more than 90 per cent of the global user base.

"GSM uses an encryption scheme called the A5/1 stream cipher to protect data," explains Jiqiang Lu from the A*STAR Institute for Infocomm Research. "A5/1 uses a 64-bit secret key and a complex keystream generator to make it resistant to elementary attacks such as exhaustive key searches and dictionary attacks."

Any encryption scheme can be hacked given sufficient time and data, so security engineers usually try to create an encryption scheme that would demand an unfeasible amount of time to crack. But, as GSM gets older, weaknesses in the A5/1 cipher and advances in technology have rendered GSM communications susceptible to attack.

Straightforward 'brute force' attacks by guessing the secret key from the data stream are still intensively time consuming, and although A5/1 was reported to have been successfully attacked in 2010, the details of the attack were kept secret. By exploiting weaknesses in the A5/1 cipher, Lu and his colleagues have now demonstrated the first real-time attack using a relatively small amount of data.

"We used a rainbow table, which is constructed iteratively offline as a set of chains relating the secret key to the cipher output," says Lu. "When an output is received during an attack, the attacker identifies the relevant chain in the rainbow table and regenerates it, which gives a result that is very like to be the secret key of the cipher."

Using two specific exploits, Lu's team was able to reduce the effective complexity of the key to a level that allowed a rainbow table to be constructed in 55 days using consumer computer hardware, making possible a successful online attack, in most cases within just nine seconds.

"GSM is still widely used in telecommunications, but its A5/1 encryption system is now very insecure," says Lu. "Our results show that GSM's 64-bit key encryption is no longer sufficient and should be upgraded to a stronger scheme as a matter of urgency."

More information: Time–Memory Trade-Off Attack on the GSM A5/1 Stream Cipher Using Commodity GPGPU. *Applied Cryptography and Network Security*. DOI: 10.1007/978-3-319-28166-7_17

Provided by Agency for Science, Technology and Research (A*STAR), Singapore

Citation: Weakness of 2G mobile phone networks revealed (2016, October 21) retrieved 26 April 2024 from https://phys.org/news/2016-10-weakness-2g-mobile-networks-revealed.html