Changing SIM card number for more secure mobile phone

November 23 2016

A continuously changing SIM card number ensures that your mobile phone can no longer be traced and tapped and enables it to check whether it is in contact with an authentic radio tower. Computer scientist Fabian van den Broek came up with this solution to solve the largest security flaw found in mobile phones today, and he is currently in contact with the GSM Association to discuss the possibility of incorporating the innovation into international standards. Van den Broek will be publicly defending his PhD thesis at Radboud University on 14 December.

Whenever your [mobile phone](#) connects to a network, the SIM card will authenticate itself to that network. This does not work the other way round unfortunately; your mobile phone does not receive proof of authentication from the radio tower. As a result, all communications transmitted from your mobile phone can be traced and tapped; a serious security flaw for systems that are connected to the network, such as transaction codes of banks and identification services like DigiD which are sent via text message.

Changing IMSI

Fabian van den Broek, digital security researcher at Radboud University, analysed the protocols and encryption techniques of the connection between a mobile phone and radio tower. He also scrutinised the security protocol of the software that deals with mobile phone communications.

According to Van den Broek, the biggest [security flaw](#) can be easily solved by having the SIM card number change automatically. This fifteen-digit number, the International Mobile Subscriber Identity (IMSI), is your identity within the mobile network. Van den Broek: "If your IMSI changes regularly, an illegal non-authentic radio tower will not be able to process the data because your identity within the mobile network is not permanent, as is the case now. This will prevent users from being traced." The solution also allows mobile phones to check whether they are in contact with an authentic radio tower.

"It would be easy for your own provider to hide the information that changes the IMSI-number inside the information that is already sent to your mobile phone, without there being consequences for you as a user," as Van den Broek puts it. His team is currently having discussions with the GSM Association (GSMA) about incorporating the proposed solution into international standards.

Safe and usable

After completing his PhD, Fabian van den Broek will continue his work of solving security flaws, where end users who are not computer scientists are central to him. "Computer scientists often come up with great solutions for security flaws, but don't always take adequate account of the end user," Van den Broek explains. "Those who try to take advantage of users often understand them better than we do, that's why they are so successful." Together with his colleagues from the Digital Security group of Radboud University, Van den Broek is working on a new and safe identification system for personal data that does have sufficient usability: IRMA, I Reveal My Attributes. This application saves all sorts of user data – personal data such as age, bank account number and memberships – and will only release data when necessary.