Researchers discover vulnerabilities that allow mobile phone users to be tracked by friends and enemies

Posted on Thursday 11th October 2012

New privacy threats have been discovered by University of Birmingham researchers which allow the physical presence of mobile phones operating on 3G networks to be tracked by third parties. This research will be presented at the ACM conference on Computer and Communications Security in Raleigh, North Carolina on Tuesday 16th October 2012.

The research team from Birmingham, who collaborated with the Technical University of Berlin, will explain how these vulnerabilities could be exploited to enable ordinary people to find the location of phones and other 3G-capable devices. Attackers could track 3G user movements across countries and even within office buildings, without knowing phone identities. The flaws affect the latest 3G networks, not just the older generation GSM networks.

The team have also proposed solutions to the issue, and are cooperating with standards organisations and network operators to promote the adoption of privacy-respecting solutions in future mobile networks.

During the study the researchers discovered two flaws on the 3G standard which is implemented on all mobile phones today. One attack, the IMSI paging attack, forces mobile devices to disclose the temporary identity (TMSI) in response to a static identity (IMSI) paging request. This can reveal the presence of devices in a monitored area by correlating the IMSI and TMSI. Another attack involves the Authentication and Key Agreement (AKA) protocol of the phone. By distinguishing two different error replies from a phone, an attacker can send a message that allows him/her to determine if a certain phone is nearby or not.

The vulnerabilities were demonstrated using an off-the-shelf femtocell unit that had been modified with new software created by the Berlin group. The attacks were made by intercepting, altering and injecting 3G Layer-3 messages into communication between the base station and mobile phones in both directions. The research team tested the vulnerabilities on network providers including T-Mobile, Vodafone and O2, and the French SFR.

Mark Ryan, Professor in Computer Security at the University of Birmingham, who led the study, said: *'The attacks could be used to track staff movements within a building. It could be used by stalkers who want to follow individuals, or spouses that want to track their partner's movements.*

'To exploit the vulnerability, the employer would need to capture wireless data from the phone as it interacted with a normal base station. This could happen in a different area than the monitored one. Then the employer would position their femtocell near the entrance of the building. Movements inside the building could be tracked as well by placing additional devices to cover different areas of the building,' said Dr Myrto Arapinis from the University of Birmingham's School of Computer Science.

The team have come up with a way to fix the problem. *'Our paper details modifications of the 3G protocols that we have proposed in order to overcome these vulnerabilities'*, Loretta Mancini from Birmingham, said. The researchers propose fixes for the vulnerabilities by employing new methods that stop an attacker being able to link different occasions when the phone is being used. Their proposed solution uses public-key cryptography, a particular type of encryption that mobile operators have been reluctant to use because it is difficult to deploy. The researchers have found that this kind of encryption needs to be deployed within their networks to thwart a privacy attack. The researchers took care to devise solutions that minimise the use of public-key cryptography in order to reduce deployment difficulties.

'The solutions we propose show that privacy friendly measures could be adopted by the next generation of mobile telephony standards while keeping low the computational and economical cost of implementing them', says Dr Eike Ritter, also part of the Birmingham team. *'We are endeavouring to work with the 3G standards organisations to achieve that.'*

This work is part of a more general effort by the Birmingham research team to identify privacy concerns and to promote privacy-friendly technologies. *'Since we use wireless technology for all aspects of our lives, from transport tickets like London's Oyster card to wireless payment cards and door-entry fobs, there is a risk of being tracked by third parties like neighbours, family and colleagues',* said Ryan.

'Online services like those of Facebook and Google also monitor users' behaviour', said Arapinis, *'and we are proposing ways in which that monitoring could be limited.'*

Ends

For further information
Kate Chapple, Press Officer, University of Birmingham, tel 0121 414 2772 or 07789 921164.