

WhiteSparks

+44 (0) 844 247 4538

whitesparks@whiterockglobal.com

www.whiterockglobal.com

Volume 4, Issue 69: 11 January 2012

Due Diligence on Your Mobile Operator?: Check Its Security Measures

Spy Snaps: [More in the News](#)



Due Diligence on Your Mobile Operator?: Check Its Security Measures

It is no revelation that technology develops fast. It is no surprise either that security measures are always a few steps behind the technology. Computer desktops in corporate environment are great examples, whereby the companies have achieved firm IT security policies and control in the past couple of years. The same, however, cannot be said for mobile phones, which have turned into mini-computers, but are not nearly as well protected as the corporate desktops. For example, it would be a rare sight to spot an Angry Birds App on your work desktop.

A recent study of the mobile operators in Europe, Morocco and Thailand found that many operators provide extremely poor protection from unauthorised surveillance and identity theft for their customers. The research was conducted by one of the world's most prominent security and hacking experts, Karsten Nohl, who runs Security Research Labs in Germany. He presented the results of the study that lasted four months, in December 2011.

For the latest research, Nohl tested 31 mobile operators more than 100 times each, and ranked the quality of their security measures. He used hacking software to make high-speed, educated guesses to decipher the complex algorithmic keys that networks use to encrypt transmissions. Once this key was derived, Nohl said that he was able to intercept voice and data conversations by impersonating another user to listen to their voice mails, make calls or send text messages on their mobile accounts.

While all surveyed mobile operators could easily fix this vulnerability in the GSM system with a simple software patch, only two of them have done so. According to Nohl, T-Mobile in Germany and Swisscom in Switzerland, are already using the enhanced security measure, which involves adding a random digit to the end of each set-up command to thwart decoding. The study further highlighted that the security of Deutsche Telekom's T-Mobile in Germany and Slovakia and Swisscom's Natel in Switzerland is also good. However, according to the research, the security performance of Orange Switzerland, TDC Sunrise in Switzerland and True Move in Thailand was the worst.

The hacking expert claims the test revealed a major vulnerability in most networks that ironically would cost very little, if nothing, to repair. The vulnerability is overlooked as the mobile operators have other priorities, such as building and expanding their networks.

However, for the clients, this negligence means a huge potential loss of both private and business information. Although the technology used for the type of surveillance that Nohl conducted for the research was once possible only by government intelligence agencies, it is now rapidly becoming affordable to a wider range of hackers. Today, much of the GSM digital technology that ensures the privacy of mobile phone calls was developed 20-30 years ago, has become

outdated. Whilst most corporations have a firm grip of their computer security, only a selected few have recognised how to mitigate the vulnerabilities of their smartphones and tablets.

[Read Full Story from Original Source...](#)

DID YOU KNOW?
North Korea changed its secret communication frequencies and encryption codes after the death of its leader Kim Jong-il, to prevent spying by South Korea.

Source: [Oman Tribune](#)



Spy Snaps: **More in the News**

The US Department of Human Services in Oregon announced that the sensitive personal information of 3000 fingerprinted individuals is now compromised after an official laptop was stolen in December 2011. Department officials have already notified some of the people whose identity was affected.

[Read More...](#)

Brightpoint, a global distributor of wireless devices, based in Indianapolis is suing its former top executive for taking trade secrets to his new job at a competitor, Miami-based Brightstar.

[Read More...](#)

WikiLeaks' founder Julian Assange may face espionage charges in the US after prosecutors in the case of Private Bradley Manning, a suspected source of secret military information that the whistle-blower published, revealed evidence of Assange's alleged role in stealing the confidential documents.

[Read More...](#)



© Cope Whiterock Limited 2012 - Critical Information Defence* - SECMI* - ISO9001 Registered Firm - Certification Number GB2000647

WhiteRock - A Bond of Trust