'Master key' to Android phones uncovered

4 July 2013 http://www.bbc.co.uk/news/technology-23179522

If exploited, the bug would give attackers access to almost any Android phone

A "master key" that could give cyber-thieves unfettered access to almost any Android phone has been discovered by security research firm BlueBox.

The bug could be exploited to let an attacker do what they want to a phone including stealing data, eavesdropping or using it to send junk messages.

The loophole has been present in every version of the Android operating system released since 2009.

Google said it currently had no comment to make on BlueBox's discovery.

Writing on the BlueBox blog, Jeff Forristal, said the implications of the discovery were "huge".

The bug emerges because of the way Android handles cryptographic verification of the programs installed on the phone.

Android uses the cryptographic signature as a way to check that an app or program is legitimate and to ensure it has not been tampered with. Mr Forristal and his colleagues have found a method of tricking the way Android checks these signatures so malicious changes to apps go unnoticed.

Any app or program written to exploit the bug would enjoy the same access to a phone that the legitimate version of that application enjoyed.

"It can essentially take over the normal functioning of the phone and control any function thereof," wrote Mr Forristal. BlueBox reported finding the bug to Google in February. Mr Forristal is planning to reveal more information about the problem at the Black Hat hacker conference being held in August this year.

The danger from the loophole remains theoretical because, as yet, there is no evidence that it is being exploited by cyber-thieves.

One other hurdle is that in order to catch out Android users, malicious hackers would have to get their booby-trapped version of a legitimate application on to the Google Play store, said security expert Dan Wallach in an interview with Ars Technica.