Cellcrypt Launches Encrypted Voice for Android Smartphones

Cellcrypt, the leading provider of encrypted voice calling on mobile phones, today announced that it has launched Cellcrypt Mobile for Android, a version of its encrypted voice calling application that runs on Android devices operating over Wi-Fi, GSM and CDMA wireless networks.

Cellcrypt Mobile provides encrypted voice calling for off-the-shelf cell phones using government-certified security in an easy-to-use downloadable application that makes highly secure calling as easy as making or placing a normal phone call. It is a software-only solution that uses the IP data channel of cellular (2G, 3G, 4G), Wi-Fi and satellite networks and can be deployed to personnel anywhere in the world in as little as 10 minutes.

Cellcrypt Mobile is in use by governments and corporations globally, uses cryptography certified to U.S. government National Institute of Standards and Technology FIPS 140-2 security standards and has been awarded the CESG Claims Tested Mark (CCTM) from the U.K. government’s information assurance authority.

The interception threat level increased during 2010 as hackers developed, demonstrated and published details of low-cost air-interface interception equipment that uses open source software freely downloadable from the internet and a generic off-the-shelf radio transceiver costing less than $2,000. Another group of hackers demonstrated interception in December 2010 using four modified cell phones as transceivers each costing $15 (interception was filmed in London by the BBC in April 2011 http://www.bbc.co.uk/news/technology-13013577). At least one top-tier European University has added practical lessons in GSM interception to its curriculum.

"Cellular voice interception is different from other types of data breach,” said Nigel Stanley, Practice Leader, Security at Bloor Research, “if you lose a laptop, USB stick or disk drive it can be fairly obvious that the data has gone missing. But with voice, a successful interception can leave no physical trace so there is little chance of realizing your data has actually been intercepted resulting in disastrous consequences. If you can compromise a cell phone then you are more or less assured that you can collect the most relevant, current and damaging data possible about a user, their business or their private life. By supporting Android devices, Cellcrypt is providing enhanced security for one of the world’s most popular mobile platforms.”

At the same time as the threat level is increasing, the use of cell phones for discussing sensitive and confidential information has also increased, even among government employees, due to the ease of use, ubiquity and interoperability of

mobile phones. This leads to an increased need for government-grade end-to-end protection that provides assurance that call security is controlled along all points of the call path between caller and recipient and risks are adequately mitigated in compliance with internal security policies.

“We are seeing a growing tension between organizational security requirements and personal convenience requirements with people often discussing sensitive issues on mobile phones to get their jobs done faster or because they have no other practical choice.” said Richard Greco, CEO of Cellcrypt, continuing, “With Cellcrypt’s support of Android we are meeting the usability demands of a fast-growing user base whilst continuing to help organizations meet their operational security requirements.”

Cellcrypt Mobile for Android is available immediately on devices supporting Android 2.3 and is interoperable with Cellcrypt running on other devices such as Nokia and BlackBerry smartphones.

For more information please visit: www.cellcrypt.com.