NEWS RELEASE

SecureCom™ Mobile Fixes Cellphone Privacy Sabotage

Vancouver, B.C., February 26, 2015 – SecureCom™ Mobile ("SecureCom™", "the Company") announces in a news article broken by The Intercept last week, that US and UK governments compromised the largest SIM card manufacturer, stealing encryption keys used to protect the privacy of cellular communications. [3] According to The Intercept, American and British spies hacked into the internal computer network of the world's largest manufacturer of Subscriber Identity Modules ("SIM cards"), stealing encryption keys used to protect the privacy of cellphone communications across the globe, according to top-secret documents provided to The Intercept by National Security Agency whistleblower Edward Snowden.

The hack was perpetrated by a joint unit consisting of operatives from the NSA and its British counterpart Government Communications Headquarters, or GCHQ. The breach, detailed in a secret 2010 GCHQ document, gave the surveillance agencies the potential to secretly monitor a large portion of the world's cellular communications, including both voice and data.

Cell phone encryption provides privacy when properly employed. Cell phone encryption has been sabotaged in several ways:

(1.) Cellphone privacy features were deliberately designed to be weak. Strong encryption is required to protect private communication. The Global System For Mobile Communication ("GSM") standard specifically mandated a weakened encryption algorithm to enable eavesdropping.[1] When GSM was relatively new in 1990, only determined and well-funded organizations could execute a successful attack. A decade later advances in cryptography and computer technology had reduced the cost of a successful attack so much that an individual could afford the purchase the necessary tools. Today, anyone with a computer, a $30 radio, and time to follow a free step-by-step tutorial can break it.[2]

(2.) SIM card encryption is not protecting the communication between two parties. Regardless of encryption strength, in order for cellphone encryption to be effective, it must be used in the correct place. The correct place is in between those who are supposed to have access to the private communication. Instead of placing the encryption in the correct place between the users, cellphone encryption is placed on the phone's SIM card between the user and their wireless network provider, so that wireless network providers are able to eavesdrop.

(3.) Cell phone encryption keys are in the hands of outsiders or have been stolen. All encryption utilizes secret keys. It's crucial that only those who are allowed to view the communication possess the secret keys. For GSM cellphone privacy to work as advertised, secret keys must reside only on the customer's mobile phone and in the infrastructure of the wireless service provider. Instead, it is a third party SIM card manufacturer who creates the secret keys; SIM cards are sold to the wireless service provider, which means that right from the start someone who isn't supposed to have access to private communication has the means to eavesdrop on it. The attack by US and British spies to steal SIM card encryption keys has broadened illicit access to your cell phone's SIM card based encryption.

These three weaknesses, broken encryption (1.), improperly placed encryption (2.), and possession of encryption keys by third parties (3.) , constitute backdoor breaches in cellphone privacy.

SecureCom Mobile users are protected from security weaknesses outlined above:

- SecureCom Mobile products only use strong encryption algorithms.
- SecureCom encryption is placed between the end users, preventing us, your wireless service provider, and other third parties from reading or listening in on your conversations.

Canada: 1500 – 888 Dunsmuir Street, Vancouver, B.C., V6C 3K4
Europe: Second Floor, 11 Pilgrim Street, London, United Kingdom EC4V 6RN
Telephone Number: Vancouver: (778) 945-1368 London: +44 20 7887 6314
Fax Number: Vancouver: (604) 608-9009 London: +44 20 7887 6001
E-mail: info@securecommobile.com

- SecureCom secret encryption keys are manufactured on your own device, and that's where they stay. We don't get copies, your wireless service provider doesn't get copies, and your wireless service providers' SIM card manufacturer certainly doesn't get copies either.

By ensuring keys are properly distributed instead of entrusted to entities with no legitimate purpose in having them, SecureCom prevents wireless providers, their partners and suppliers, and government agencies from eavesdropping on you, and also prevent all of them from allowing others to do the same, whether through malice or incompetence.

[1] http://en.wikipedia.org/wiki/A5/1#Security
[2] http://domonkos.tomcsanyi.net/?p=418
[3] https://firstlook.org/theintercept/2015/02/19/great-sim-heist/

About SecureCom™ Mobile Inc.

SecureCom™ Mobile™ develops and markets consumer software encryption communications products for mobile phones, tablets, and computer-based platforms. Its technology enables people to communicate, in complete privacy, with ease, using voice, text and data messaging. The Company employs cryptographically strong algorithms and protocols to shield communication from surveillance and analysis. Its encryption scheme cannot be circumvented by mobile carriers or other parties, thereby ensuring total privacy. SecureCom™ Mobile products are developed for the Android and Blackberry platforms, and are expected to soon be available for the entire slate of popular OS platforms.

SecureCom™ Mobile Inc. trades on the Canadian Securities Exchange under the symbol SCE and Frankfurt Stock Exchange under S6U, WKN#: A12CAR.

See http://www.securecommobile.com (English) or http://www.securecommobile.de (German)

For further information please contact: Peter Wilson, Director, +1.778.945.1368
E-mail: info@securecommobile.com

Forward-Looking Information: This press release may include forward-looking information within the meaning of Canadian securities legislation, concerning the business of SecureCom™. Forward-looking information is based on certain key expectations and assumptions made by the management of SecureCom™, including future plans for the research and development of digital products. Although SecureCom™ believes that the expectations and assumptions on which such forward-looking information is based are reasonable, undue reliance should not be placed on the forward-looking information because SecureCom™ can give no assurance that they will prove to be correct. Forward-looking statements contained in this press release are made as of the date of this press release. SecureCom™ disclaims any intent or obligation to update publicly any forward-looking information, whether as a result of new information, future events or results or otherwise, other than as required by applicable securities laws.

Forward-looking statements are often identified by terms such as "will", "may", "should", "anticipate", "expects" and similar expressions. All statements other than statements of historical fact, included in this release are forward-looking statements that involve risks and uncertainties. There can be no assurance that such statements will prove to be accurate and actual results and future events could differ materially from those anticipated in such statements. Important factors that could cause actual results to differ materially from the Company's expectations include the failure to satisfy the conditions of the Canadian Securities Exchange and other risks detailed from time to time in the filings made by the Company with securities regulations.

The reader is cautioned that assumptions used in the preparation of any forward-looking information may prove to be incorrect. Events or circumstances may cause actual results to differ materially from those predicted, as a result of numerous known and unknown risks, uncertainties, and other factors, many of which are beyond the control of the Company. The reader is cautioned not to place undue reliance on any forward-looking information. Forward-looking statements contained in this news release are expressly qualified by this cautionary statement.