

icsl informs:

## Mobile phone eavesdropping for everyone– starting at 35 Euro



Translation of an article found in Austria's most serious daily paper: „Die Presse“

**Oct 9th 2011**

<http://diepresse.com/home/techscience/mobil/707210/HandyAbhoeren-fuer-jedermann-ab-35-Euro>

**Oct. 10th 2011**

„Die Presse“ printed edition, page 10

## Mobile phone eavesdropping for everyone– starting at 35 Euro

09.11.2011 | 16:42 | Von Andreas Wetz (Die Presse)

***From monitoring your wife up to espionage: Experts expose serious security holes which can be exploited by everybody with a little skill and money.***



Bild: (c) Reuters (DANISH SIDDIQUI)

[Vienna] At the time when former finance minister Karl-Heinz Grasser, lobbyist Walter Meischberger and real estate agent Ernst Karl Plech had their – meanwhile legendary – telephone conversation, they imagined themselves being safe. Using non-registered prepaid cards and relying on GSM's encryption should get the job done, they thought. In fact, it did not. The police were waiting around the corner and listening in with a special device worth 500,000 Euro.

That was back in February 2010. Today, a year and a half later, that sort of thing can be done by interested laymen and probably it will soon be possible for virtually everyone. This is the message emanated by a conference on Security in Communications and Information Technology in Vienna. Organized and hosted by the “Abwehramt”, the domestic intelligence service of the Austrian Armed Forces. High-ranking business leaders, police and the military officers shared their knowledge about new developments and threats.

### **Software turns mobile phone into a wiretapping device**

Key fact: The rapid proliferation of smartphones is turning into a threat to the state, economy and every citizen. As an official of Austria's Federal Agency for State Protection and Counter Terrorism (“BVT”) puts it: “Who gains access to someone else's smartphone, takes over his life”. These devices “know” everything about their owner because they are always close to them and store motion profiles, e-mails, text messages, communication patterns, appointments, acquaintances, photos, videos and a whole lot more.

Several dubious developers - often from the Far East – offer entire espionage suites at discount prices, 24-hour support via e-mail included. For 59.95 USD (44 €), one can obtain a software called “Cell Spy”. It is installed on the phone via data cable or, even better, clandestinely via WLAN. It is irrelevant whether the operating system is iPhone OS, Android or Blackberry OS. It grants remote access to contact lists, text message memory and the phone call function. In a test conducted by “Die Presse”, the most alarming feature worked faultlessly right away: Upon establishing a call to



Translation of an article found in Austria's most serious daily paper: „Die Presse“

the infected phone, the latter is turned into a mobile bugging device. Without the other person having to answer the call and without any reaction on their display, you can set up a connection and activate the microphone. This enables you to eavesdrop on your wife from the other end of the world. Or on someone else.

“The main application area of these methods is undoubtedly industrial espionage”, says Marco Di Filippo from “Compass”, a Swiss security services provider consulting on how to identify such attacks. This statement is confirmed by a study of the “BVT” and the Austrian college “FH Campus Wien”. Its authors estimate that **nearly one in three companies has already fallen victim to an “unintended disclosure of information”**. Di Filippo: “Eavesdropping on mobile phones has the potential to become a national pastime.”

### DIY eavesdropping equipment

This is no big deal for the committed layman. In these circles, an old Motorola phone has achieved an almost legendary reputation. A used C123 model can be purchased for 10 €. Invest additional 25 € in a compatible data cable, download the free software “OsmocomBB” from the internet and you get to tap in on all surrounding mobile phones currently running on the same transmission tower. The software’s only “drawback” is its inability to target specific phone numbers.

There are other methods. The free software “OpenBTS” allows the attacker to operate his own GSM transmitter, which is set up near the target’s residence. Exactly as the police did with Karl-Heinz Grasser. The necessary do-it-yourself hardware kit costs between 150 and 900 €, depending on the quality. All you need is a decent knowledge of English in order to understand the instruction manuals and a little skill with the soldering iron.

The application of these methods is punishable by law. However, the reports of “BVT” and military intelligence services show that their use is on the advance. According to a member of the military, “the problem is that mobile phones have become indispensable to everyday life”. Currently, the only protection is the the dial-in via UMTS network, since its encryption is still considered safe. Their disadvantage: **These networks are often overloaded in cities and not available at all in remote regions.**

(“Die Presse”, printed edition of Oct. 10th 2011)