

# Two cellphones in one

October 7 2011

---

More and more companies are providing their employees with smartphones. While companies seek the best security available for their data, employees would also like to install apps of their own. Security experts have now developed equipment software with two separate areas: the business area and the personal area. Researchers will unveil this development at the it-sa trade fair held October 11-13 in Nuremberg (Germany).

The company smartphone, the private cellphone, keys for house and car, wallet – the objects we carry around with us every day are becoming more numerous all the time. Which is why many people also use their [business](#) smartphone for personal purposes. It may be convenient, but employees and the IT department have different interests: most employees would prefer unlimited use of their smartphones, installing and using whatever programs they like. But this can also open the door to hackers in search of ways of attacking. As a result, IT departments often try to limit the use of smartphones accordingly. [Security experts](#) at the Fraunhofer Institute for Secure Information Technology SIT and at the Center for Advanced Security Research Darmstadt CASED have now developed a security solution for Android-based smartphones: "BizzTrust for Android". The solution separates private and business applications on the phone itself.

BizzTrust smartphones offer two protected areas for data and apps. They can identify whether content belongs to a business or a private application, store it separately in the appropriate partition and control access to the data during operation. This enhances the security of

business data while still allowing employees to install as many private apps as they wish. Even if attackers manage to infiltrate an unsecured app, they cannot use it to access company data, and the impact of the attack is confined to the private data on the smartphone. "Our development significantly improves the security of today's mobile terminals at no cost to user-friendliness," notes Prof. Dr. Ahmad-Reza Sadeghi, director of Cyber-Physical Systems Security at the SIT/CASED.

A color symbol shown in the display let the user know at all times whether he or she is in the business or "red" area or in the personal, „green" area of the [smartphone](#). Two "clicks" of the touchscreen is all it takes to toggle over to the respective other side.

To implement these two virtual smartphones in a single device, the experts modified the Android operating system so that all data from trustworthy applications is marked as such. The company itself decides which applications are released for business use, and who has access to what areas of company IT. Because these rules may change over time, the business applications are updated or deleted as needed as soon as the user links to the company network. There is another benefit as well: companies can provide their own apps to employees and keep them updated on a regular basis. Security is guaranteed at all times as well: the telephone's software is checked before the telephone can log onto the company's network via a secure VPN link. If a modification is detected critical applications can be blocked.

Researchers will present the BizTrust for Android at the it-sa trade fair. The next step for this technology is to equip smartphones with integrated smartcards that provide additional [security](#) functions. To supplement BizTrust, researchers at SIT are now teaming up with partner companies to develop tools to permit IT administrators to manage smartphones on an everyday basis – the technology would establish a

secure link with the mobile device for wirelessly synchronization and backup of the data stored there – or data deletion if the device is lost or stolen.

Provided by Fraunhofer-Gesellschaft

Citation: Two cellphones in one (2011, October 7) retrieved 21 June 2024 from <https://phys.org/news/2011-10-cellphones.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.