Fraunhofer

SIT

FRAUNHOFER INSTITUTE FOR SECURE INFORMATION TECHNOLOGY

Fraunhofer Institute for Secure Information Technology SIT

Dr. Markus Schneider
Ruben Wolf
Rheinstrasse 75
64295 Darmstadt / Germany

Phone +49 6151 869-337/ -60077
markus.schneider@sit.fraunhofer.de
ruben.wolf@sit.fraunhofer.de
www.imobilesitter.com
www.sit.fraunhofer.de

iMOBILESITTER
CLEVER PASSWORD MANAGEMENT FOR IPHONES

Passwords or PINs are needed for numerous things nowadays, such as EC cards, mailboxes and connections to networks or resources, which are used for private and/or business purposes. But the more we have, the more difficult it becomes for us to remember them without the assistance of tools such as password managers. These must fulfil the highest possible security standards. Fraunhofer SIT has developed the software iMobileSitter, which manages access data on iPhones and protects it against hacker attacks using a particularly clever method. iMobileSitter is available in the App Store.

The software is extremely easy to use: the user simply needs to remember a master password; iMobileSitter takes care of the rest. The software protects all access data on the iPhone with an innovative method, which will really exasperate hackers: it accepts any master password that is entered, thereby opening the storage area and displaying the supposed secrets. Each result that is displayed really looks like it could be the right one. For example, if a four-digit PIN has been saved, a combination between 0000 and 9999 will always be displayed, which means a hacker will be unable to tell whether their attempt was successful. What's more, it doesn't

matter whether the hacker performs the attack directly or uses software to automate the attack. The fact that the attack was unsuccessful will not become apparent until the hacker tries to use an ATM, and the EC card is withheld after three incorrect attempts. The legitimate user, on the other hand, will recognise a typo immediate-

ly: a small symbol on the screen serves as a kind of feedback for the legitimate user. The user recognizes that he has entered the correct master password if the expected symbol is displayed. The attacker does not know the user's symbol; for the attacker the symbol has no semantic value with respect to the correctness or incorrectness of the master password that has been entered.

Shake to encrypt
The software utilizes real random numbers for encryption purposes. And to generate these, the user simply needs to shake the iPhone with a bit of force. A quick shake is therefore generally bad news for password thieves: the chance of determining the access data of this iPhone owner is pretty poor.

Fraunhofer SIT developed iMobileSitter to counteract the growing risk of attacks. Conventional password storage tools can often be cracked quickly with special tools or cloud services. This is even possible when secure encryption methods are used, as the security requirements for password-based encryption are not fulfilled in conventional management tools. This, in turn, enables hackers and digital key-recovery services to access such secrets relatively quickly.

Who would benefit from iMobileSitter?
- Companies that place a great deal of importance on secure password management for their employees
- Private individuals who want to protect their passwords
- For all those who want to do a good deed: gift vouchers can be purchased in the App Store, which can then be used to purchase the software