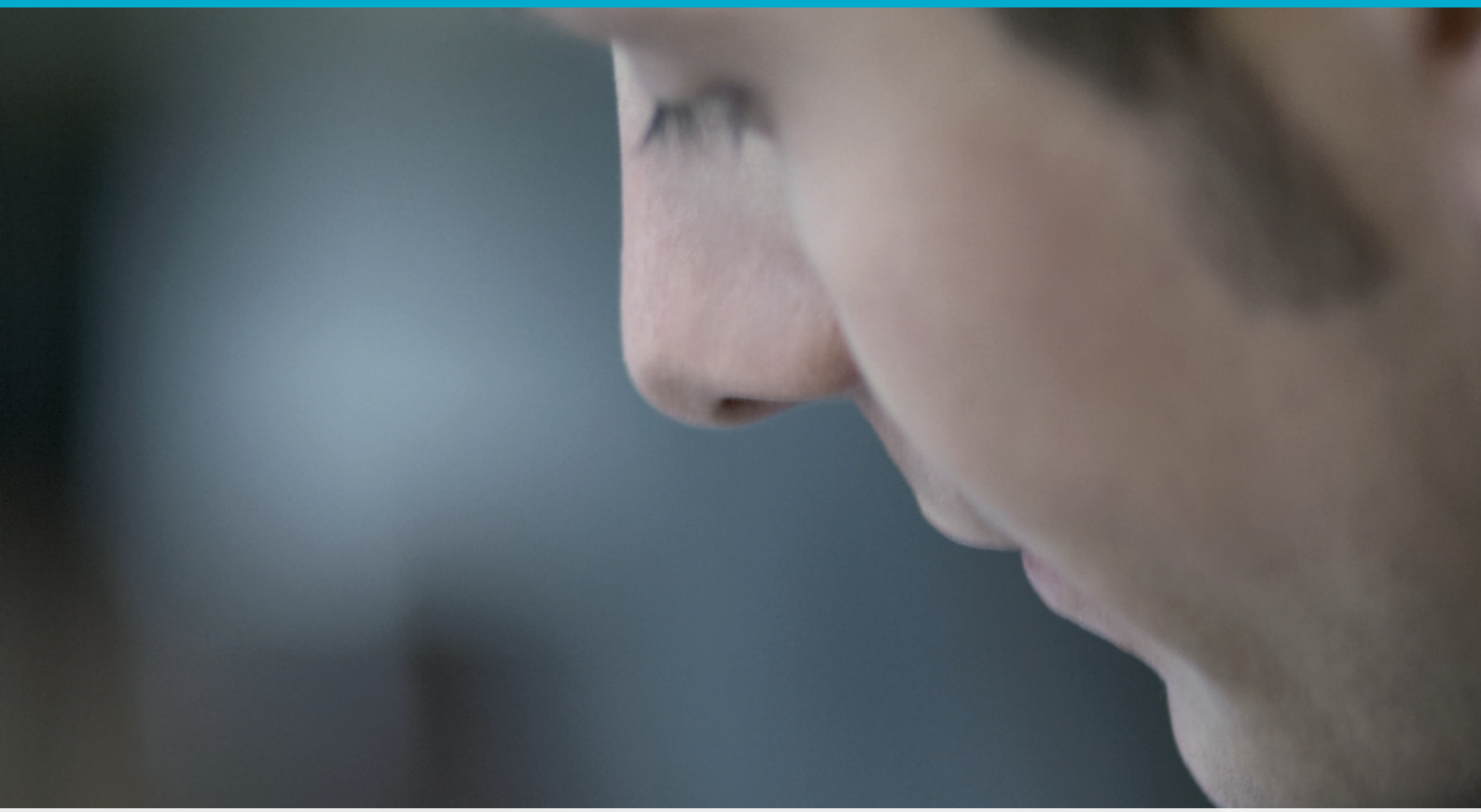
Fraunhofer
SIT

FRAUNHOFER INSTITUTE FOR SECURE INFORMATION TECHNOLOGY

MOBILESITTER

SECURE PASSWORD MANAGEMENT FOR SMARTPHONES



MobileSitter

MOBILESITTER

From e-mail communication through e-commerce or Web 2.0 to bank transactions – life today would be unthinkable without passwords, PINs, and TANs. Yet the more access codes we are required to remember, the more difficult it becomes. Password managers generally make things simpler for users, though many of these supposedly secure tools are actually easy prey for intruders – even if they are based on strong encryption algorithms. Fraunhofer SIT's MobileSitter is different: it protects passwords, PINs, and TAN lists using an innovative technique that offers far greater security than other password manager. While users value the client-friendly interface of this mobile solution, hackers despair because MobileSitter effectively frustrates typical password attacks.

MobileSitter users only have to memorize a single password – the master password. The software takes care of the rest. Once the master password is entered correctly, it decrypts and displays all stored passwords, PINs, and TANs. It can be installed on many smartphones, giving you access to your passwords whenever and wherever you need them. MobileSitter is ideally suited for both private users and companies – also as a promotional gift.

Weaknesses of conventional products

Despite their use of accepted encryption algorithms, many password managers are compromised by gaping security holes. Developers tend to overlook one vital fact: algorithms like AES (Advanced Encryption Standard) that are widely considered to be secure are, in reality, only truly safe if all possible key combinations are equally probable. The key space of AES, in other words the set of all possible cryptographic keys, comprises a total of 2^{128} ($\approx 3.4*10^{38}$) elements, for instance. If, say, a master password consists of a maximum of 12 digits, the number of possibilities that can be entered on the keypad is only $4.8*10^{23}$ – equivalent to just $1.4*10^{-13}$ percent ($\approx 0.00000000000014\,\%$) of the AES key space. An attacker hoping to get hold of encrypted secret information therefore only has to try out a relatively small number of cryptographic keys. Under the right conditions, this step could be accomplished in a very short time, given the computing capacities available today. In practice, the situation for a potential hacker is likely to be far more favourable, because out of all the conceivable master password combinations some have a higher probability than others. According to an ElcomSoft study, around forty percent of all passwords utilized by businesses can be found in a dictionary.[I] Attackers therefore program their hacking software to start by trying every word in a dictionary (dictionary attack).

Methods of attack

Modern invaders planning to carry out a dictionary or brute force attack (in which they try out all relevant possibilities) employ hacking software that is more or less freely available and intuitive to use.[II] Anyone who is unwilling to get their

hands dirty can resort to one of the digital online cryptography portals that offer password cracking as a service.[III] In addition, new technologies like cloud computing allow people to purchase enormous amounts of computing capacity, which will make password cracking even simpler, faster, and cheaper in the future.[IV] Even now, attackers can already test billions of combinations in next to no time. In many cases, this happens without the data's proper owner being even remotely aware and without giving other protection mechanisms a chance to become effective. Although some manufacturers endeavor to artificially increase the computational overhead for encryption and decryption as a way to limit the number of attempts per minute in the event of a dictionary or brute force attack, such countermeasures are inappropriate for mobile devices with limited CPU capacity – such as smartphones – because they impose serious restrictions on the usability of the hardware.

The trick

With a conventional password manager, an attacker can tell whether or not a decryption attempt is successful. With Fraunhofer SIT's MobileSitter this is no longer possible; there are no clues in the decryption result that reveal whether an intruder's aim has been achieved. MobileSitter accepts all inputs regardless of the attempted master password; it decrypts the stored information on the basis of this password, irrespective of whether or not it is correct. The decryption result that appears on the terminal device is generated according to the master password entered. Every password, PIN, or TAN that is decrypted and displayed looks as if it could be correct. If an attacker decrypts a PIN assigned to a debit card, for instance, the decryption result that is returned will always be a four-digit number combination, in accordance to the requested format. The intruder – either the hacker themselves or the hacking software – has no means of assessing whether the master password entered was actually correct. Every attempt to decrypt the codes appears to be successful. Thus, dictionary or brute force attacks are effectively frustrated. To determine whether a decryption result is correct, the hacker has no choice but to log into the relevant access or account or type in the PINs and TANs. After a defined number of failed attempts, e.g. three in the case of a debit card, addintional security mechanisms of the application will take effect. The rightful user, however, realizes immediately if the master password entered is correct or if it was simply mistyped: MobileSitter displays an easily recognizable, graphical symbol depending on the master password entered. The proper user, who memorized the proper symbol, will thus have an immediate confirmation of the correctness of his input. On the other hand, this image is of no help to the attacker, who neither knows the symbol for a correct password nor has any way of finding it out.

Technology / system requirements

MobileSitter was developed on the basis of Java ME. This allows it to be installed on and used with different mobile phones, regardless of the operating system. The MIDP 2.0 and CDLC 1.1 standards, which are supported by the majority of mobile devices, were used to realize MobileSitter for mobile phones. Software variants for iPhone and Android phones are under development

The master password is entered in MobileSitter.

I. *ElcomSoft: Password Security Survey 2009. www.elcomsoft.com/surveys.html*
II. *Heise Online: ElcomSoft now also cracks passwords with word lists. www.heise.de/newsticker/meldung/ElcomSoft-knackt-Passwoerter-nun-auch-mit-Wortlisten-832342.html; Heise online. Password cracker for iPhone backups. www.heise.de/security/meldung/Passwortknacker-fuer-iPhone-Backups-922983.html;*
III. *Heise online. Password cracker as a payment service. www.heise.de/newsticker/meldung/Passwort-Cracker-als-Bezahldienst-147107.html;*
IV. *Heise online. How to crack codes cheaply in the cloud. www.heise.de/newsticker/meldung/Preiswert-Schluessel-knacken-in-der-Cloud-848574.html; iX. Cloud service cracks WLAN passwords. www.heise.de/ix/meldung/Cloud-Dienst-knackt-WLAN-Passwoerter-879888.html*

A patented procedure specifically developed for MobileSitter is used to encrypt the secret code combinations (passwords, PINs, or TANs). This procedure is based on globally accepted standards such as AES-128, PKCS#5, and ISO/IEC 9797-1.

Applications

With MobileSitter, any type of code combination can be managed on a mobile phone, for example passwords, PINs, or even complete TAN lists. Users thus always have access to their secret codes and can use them wherever they need them – on a computer, at home or in the office, to settle the bill in a restaurant or when shopping in a supermarket or on the Internet. MobileSitter users only have to memorize one password – the master password. All other codes are safely stored.

MobileSitter is an attractive solution for both business and private use. In a commercial context, it provides particular benefits to the following parties:

- ++ Companies that would like to offer their employees a secure management solution for their secrets. These companies can significantly improve their security at a critical weak point.
- ++ Manufacturers of mobile terminals who would like to integrate MobileSitter into their products (product refinement or enhancement).
- ++ Providers of mobile communication services who would like to integrate MobileSitter into their products (service enhancement).
- ++ IT providers who would like to act as distributors for Fraunhofer SIT and market MobileSitter to their customers.
- ++ Companies that would like to offer MobileSitter to their customers or business associates as a promotional gift branded with their own logo. The recipients of this extremely expedient and secure tool will be reminded of who gave it to them every time they use it. The logistical procedure for distributing MobileSitter in this way is very simple (free download with a voucher code).

Ongoing development

MobileSitter was developed as part of a Fraunhofer SIT research project and is continuously optimized. The Institute is currently working on software variants for specific plattforms e.g. iPhone and Android

Fraunhofer Institute for Secure Information Technology SIT

Contact:
Dr. Markus Schneider, Ruben Wolf
Rheinstrasse 75
64295 Darmstadt, Germany

Phone +49 6151 869-337/-60177
Fax +49 6151 869-224
markus.schneider@sit.fraunhofer.de
ruben.wolf@sit.fraunhofer.de

www.mobilesitter.de