

## Fotohandy-PIN: Secure Online Passwords via Camera Mobile Phone

Entering the password resp. the PIN for online accounts (email, bank, enterprise, game server, eBay, Amazon, etc.) is not secure: a trojan virus sitting on the PC of the user can tap the password by a so-called *keylogger* attack: the trojan just checks which keys are hit when the user enters the password. Later the trojan sends the password and the account name to his master.

The new *Fotohandy-PIN* method is presented. It prevents the keylogger attack by involving the user's camera mobile phone (German: *Fotohandy*). During the log-in into an online account the digits 0,...,9 are shown on the display of the camera phone, in some random order. The trojan can not 'see' the order of the digits and therefore is not able to tap the PIN.

### The Fotohandy-PIN Method

The new method is described from the user's point of view. He needs a camera mobile phone on which the Fotohandy-PIN program is installed and is initialized for the account he wants to enter, see next paragraph for the initialization process. The user visits the website of the account server and enters his account name. In reply a 2D-barcode is shown on the screen. The user takes a picture of the barcode with the Fotohandy-PIN program on his camera phone. Immediately the camera phone will show a keypad with the digits 0,...,9 in some random order, see drawing. The user is now able to enter his PIN: he just clicks with the mouse on the empty keypad fields on the computer screen which correspond to his PIN according to the random order shown on the camera phone. This sounds complicated but in fact is not: the handling is intuitive and can easily be learned by everybody.



The Fotohandy-PIN program can be downloaded in the Internet, for example at the *Troja* project site at the University of Tübingen. The one program can handle any number of online accounts. In order to get a secure account at some server, the user visits the server's website and enters his preferred account name. In case the name is available the server replies by sending a 2D-barcode containing the secret key for the account. The server may send the barcode via mail or fax, or may send it – what is less secure – via a document attached to an email or by just showing the barcode on the screen of the user. In any of these cases the user takes a picture of the barcode with the Fotohandy-PIN program on his camera phone. The program recognizes that a key for a new account is transferred and stores the account name and the key on the camera phone. Afterwards a PIN for the account can be defined by the user and is communicated to the account server via an easy online procedure – a trojan will not be able to tap the PIN during that procedure. This finishes the initialization of the new online account.

The barcode shown during the login procedure contains - besides the server name and the account name - an information which is unique for that login session, for example a serial number or the exact date split to the second. All information is openly shown in the barcode - no need to keep it a secret. The security of the Fotohandy-PIN method results from the fact that the random order of the digits shown by the camera phone is computed by a so-called *hash function* which has as inputs both the data contained in the barcode as well as the secret key for that account stored on the camera phone. A trojan sitting on the computer of the user does not know the secret key, he can only recognize mouse clicks into empty fields. Therefore, the trojan is not able to tap the PIN.

In case there is a trojan on the camera phone – what is a rare case until now – the Fotohandy-PIN method is not immediately cracked because that trojan may see the random order of the digits or even the secret key but it can not watch the entering of the PIN. Therefore, in order to tap the PIN a second trojan sitting on the computer of the user is needed which has to cooperate with the one sitting on the camera phone – a difficult, if not unrealistic attack.

The Fotohandy-PIN program may contribute to a problem everybody using the Internet encounters: the growing number of personal online accounts and their respective passwords. Because the Fotohandy-PIN method allows user-defined PINs a few PINs may suffice for dozens of online accounts belonging to the user. Moreover, the Fotohandy-PIN program may show during the login process a user-defined memory aid for the PIN of that online account, for example “old PIN”. The memory aid could go even further: sometimes one forgets not only the password but even the account name. A 2D-barcode shown on the server's website could make the Fotohandy-PIN program showing the account name of the user at that server.

The Fotohandy-PIN method, preventing trojans from tapping the password, can be extended to a method preventing trojans from manipulating online transactions, like money transfers in the case of Online Banking, see the website shown below.

The Fotohandy-PIN was developed at the University of Tübingen, a patent application is pending. An online demonstration was written by students:

<http://www-fs.informatik.uni-tuebingen.de/studdipl/Fotohandy-PIN/>

Some recent press articles are linked on that web page.

As an alternative for users not having a camera phone or, as a fall-back solution in case the user does not carry along his camera phone, the permutation-PIN (pPIN) method is appropriate: a random order of the digits is shown not on the display of the camera phone but on a sheet of paper: <http://www-fs.informatik.uni-tuebingen.de/~borchert/pPIN/>

## Contact

Dr. Bernd Borchert

WSI Informatik, Sand 13, 72076 Tuebingen, Germany

[borchert@informatik.uni-tuebingen.de](mailto:borchert@informatik.uni-tuebingen.de)

phone +49-7071-29-78964, mobile +49-175-4142431

<http://www-fs.informatik.uni-tuebingen.de/~borchert/>