First publ. in: Financial cryptography and data security : 14th International Conference, FC 2010, Tenerife, Canary Islands, Spain, January 25 - 28, 2010 / Radu Sion (ed.). Berlin : Springer, 2010, p. 429
The original publication is available at www.springerlink.com

hPIN/hTAN: Low-Cost e-Banking Secure against Untrusted Computers

Shujun Li[1], Ahmad-Reza Sadeghi[2] and Roland Schmitz[3]

[1] University of Konstanz, Germany
[2] Ruhr-University of Bochum, Germany
[3] Stuttgart Media University, Germany

Abstract. We propose hPIN/hTAN, a low-cost token-based e-banking protection scheme when the adversary has *full* control over the user's computer. Compared with existing hardware-based solutions, hPIN/hTAN depends on neither second trusted channel, nor secure keypad, nor computationally expensive encryption module.

Due to the rapid progress of the Internet, e-banking has become more and more popular all over the world and security is considered as one of the most serious issues of e-banking. The earliest and simplest defense protecting e-banking systems is user authentication based on static PINs. Since static PINs are prone to identity theft, two-factor user authentication such as PIN/TAN has been widely adopted to make e-banking more secure. However, PIN/TAN cannot resist man-in-the-middle (MitM) attack, whose aim is to manipulate transactions. In the strongest form of MitM attacks, the user's computer is under the *full* control of the adversary, who can observe and tamper with all the communications between the user and the e-banking server. The wide spread of malware over the Internet renders such advanced MitM attacks possible in reality.

In this poster, we propose hPIN/hTAN, the first (to the best of our knowledge) hardware-based solution against MitC attacks that depends on neither second trusted channel nor secure keyboard nor computationally expensive encryption (such as PKC). Instead, hPIN/hTAN bases its security only on proper use of a cryptographic hash function and active involvement of human attention.

The hPIN/hTAN includes two specific protocols – hPIN and hTAN, which protect the login process and online transactions, respectively. The involved parties include a human user, a trusted USB-token issued by the bank to the user, an untrusted terminal computer, and the e-banking server. The USB-token is equipped with a trusted display and shares a secret with the server.

The core of the hPIN protocol is a random code shown on the trusted display of the USB-token, which makes it possible for the user to input a transformed PIN on the untrusted computer without leaking the PIN. After the user authenticates herself to the USB-token, the hPIN protocol continues to achieve mutual authentication between the USB-token and the server. In the hTAN protocol, the user verifies the transaction data *simultaneously* while typing them on the keyboard of the untrusted computer. Then the USB-token and the server perform a transaction verification process based on the shared secret.

Konstanzer Online-Publikations-System (KOPS)
URN: http://nbn-resolving.de/urn:nbn:de:bsz:352-opus-126765
URL: http://kops.ub.uni-konstanz.de/volltexte/2010/ 12676