Turkish Journal

of

Electrical Engineering &
Computer Sciences

Keywords
Authors

elektrik@tubitak.gov.tr

Scientific Journals Home Page

Turkish Journal of Electrical Engineering & Computer Sciences

Improving the Security and Flexibility of One-Time Passwords by Signature Chains

Kemal BIÇAKCI, Nazife BAYKAL
Middle East Technical University, Informatics Institute,
İnönü Bulvarı, 06531, Ankara-TURKEY
bicakci,baykal@ii.metu.edu.tr

Abstract: While the classical attack of ``monitor the network and intercept the password'' can be avoided by advanced protocols like SSH, one-time passwords are still considered a viable alternative or a supplement for software authentication since they are the only ones that safeguard against attacks on insecure client machines. In this paper by using public-key techniques we present a method called signature chain alternative to Lamport's hash chain to improve security and flexibility of one-time passwords. Our proposition improves the security because first, like other public-key authentication protocols, the server and the user do not share a secret, thereby eliminating attacks on the server side. Second, from any incorrectly revealed one-time password, unspent passwords cannot be calculated if a signature chain is preferred. Having an infinite length, the chain in our proposition is more flexible and facilitates using the protocol without the complexity of restarting. On the other hand, the disadvantage of signature chain is the longer verification time with respect to hash chain based approaches.

Key Words: authentication, hash chain, signature chain, public-key authentication protocol, one-time password, network security

---

Turk. J. Elec. Eng. & Comp. Sci., **11**, (2003), 223-236.
Full text: pdf
Other articles published in the same issue: Turk. J. Elec. Eng. & Comp. Sci.,vol.11,iss.3.