Activity-based Verification Continuous User Verification after Successful Login

Researchers

Yisrael Mirsky
ymirsky1@gmail.com

Prof. Yuval Elovici
elovici@inter.net.il

Prof. Lior Rokach
liorrk@bgu.ac.il

Dr. Robert Moskovitch
robertmo@bgu.ac.il

Publications

Feher, C., Elovici, Y., Moskovitch, R., Rokach, L., & Schclar, A. (2012). "User identity verification via mouse dynamics," *Information Sciences*, 201, 19-36.

Shimshon, T., Moskovitch, R., Rokach, L., & Elovici, Y. (2010), "Continuous verification using keystroke dynamics," IEEE International Conference on Computational Intelligence and Security (CIS), 411-41.

Schclar, A., Rokach, L., Abramson, A., & Elovici, Y. (2012). "User Authentication Based on Representative Users," IEEE Transactions on SMC, 42(6), 1669-1678.

Description

Authentication vulnerability - The Internet and internal company applications currently require interacting with a multitude of identities and passwords since services such as e-mail or eBanking use a mandatory login. Administering and maintaining this increasingly confusing multitude of access data, PINs, and TAN lists, however, is considered a bewildering and complex task, which leads users to often neglect security in favor of convenience.

Due to the misuse of user data, great financial damage is caused worldwide, both for the users and for the providers of products and services. Corresponding authorization credentials can get lost in any number of ways: through voluntary transmission, physical theft, or digital attacks such as phishing, sniffing, or Trojans. Another vulnerability of today's authentication mechanisms in Internet applications is the fact that users' identities are verified only at the start of every session.

Behavioral-based characteristics - Solutions that focus on behavioral-based characteristics for authentication are developed in the Activity-Based Verification project. When interacting with the computer, every person generates individual activity patterns that can be saved as biometric signatures. Machine learning technologies can be used to recognize and analyze biometric characteristics. The underlying verification program must initially be trained for the respective user behavior. After logging in to a system, continuous verification will then be made on the basis of these specific biometric characteristics as to whether the logged in user remains the user of the system during the course of a session. For this, the system can use current typing behavior, mouse movements, or the operation of applications for comparison with the previously generated signatures. In the process, this ensures that authorized users are not disallowed and unauthorized users are not accepted.

Simpler and better security - Compared to physiological biometric characteristics (such as fingerprints, iris, etc.), behavioral-based biometric characteristics have the great advantage of being easily monitored without special hardware or modified user behavior. For example, password reset could be designed in a more user-friendly manner with activity-based verification. Instead of the current procedure, with which a temporary password is issued during registration with a service, the user would be prompted to transcribe a randomly selected word list. The biometric characteristics during the use of the keyboard would be evaluated and used for authentication.

Activity-based verification could also be used to replace transaction numbers (TANs) or hardware tokens that are currently required for online banking.