Doctoral School of Information and Biomedical Technologies
Polish Academy of Sciences (TIB PAN)

SUBJECT:

Sensitive applications user profiling using machine learning methods

SUPERVISOR, ASSISTANT SUPERVISOR:

prof. dr hab. inż. Ewa Niewiadomska-Szynkiewicz, dr inż. Andrzej Sikora
tel. 602 411 914 oraz 22 38 08 275, ewan@nask.pl, andrzej.sikora@nask.pl;
Research and Academic Computer Network – National Research Institute (NASK-PIB), Kolska 12, 01-045 Warszawa

DESCRIPTION:

Widespread access to the global network has led to the emergence of numerous cyber threats, both at the technical and information level. The object of attacks became not only the technical infrastructure but also people. Ensuring cybersecurity is one of the challenges for modern ICT. Hazardous attacks on sensitive applications result in severe consequences, both for the individual citizen and the whole country. Cyberattacks are incredibly varied, take different forms, and, importantly, are subject to constant change. This research project focuses on incidents involving the impersonation of another user and attempts at phishing or fraud. The aim will be to create user profiles based on post-measurement data assuming working with different applications (client applications, websites, etc.) and operating on different devices, i.e. desktop computers and mobile devices. The project involves developing models, methods and tools to enable a systematic approach to detect fraud attempts. An important aspect that distinguishes the proposed solution from those presented in the literature is the comprehensive profile building approach based on the fusion of measurement data collected while using different input-output devices (keyboard, mouse, touch screen, etc.) and available measurement sensors. Machine learning techniques will be used to detect anomalies in the application user's performance and detect attack attempts. Various methods will be considered, ranging from classical solutions to deep artificial neural networks, e.g., siamese and spline. An essential outcome of the project will be the verification of the usability of the computational techniques analyzed, taking into account various criteria defined by the PhD student.

BIBLIOGRAPHY:

1. D. E. Comer, Computer Networks and Internets (6th edition), Pearson Education Limited, 2015.
2. Goodfellow, Y. Bengio, A. Courville, Deep Learning, MIT Press, 2016, http://www.deeplearningbook.org
3. N. A. Mahadi, A Survey of Machine Learning Techniques for Behavioral-Based Biometric User Authentication, IntechOpen, 2018, https://books.google.pl/books?id=kjGozQEACAAJ.
4. K. Revett et al., A Survey of User Authentication Based on Mouse Dynamics, Global E-Security, Communications in Computer and Information Science, vol 12. Springer, 2008, https://doi.org/10.1007.
5. R. Giot, A. Rocha, Siamese Networks for Static Keystroke Dynamics Authentication, proc. 2019 IEEE International Workshop on Information Forensics and Security (WIFS), 2019, pp. 1-6, doi: 10.1109/WIFS47025.2019.9035100.
6. M. Antal, N. Fejér, Mouse Dynamics Based User Recognition Using Deep Learning, Acta Universitatis Sapientiae, Informatica vol. 12 pp. 39-50, 2020.
7. P. Chong, Y. Elovici, A. Binder, User Authentication Based on Mouse Dynamics Using Deep Neural Networks: A Comprehensive Study, IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1086-1101, 2020, doi: 10.1109/TIFS.2019.2930429.