

Streszczenie rozprawy doktorskiej
autor mgr inż. Tomasz Wesołowski

*Biometryczna weryfikacja użytkownika systemu komputerowego
z automatyczną aktualizacją profilu aktywności*

Teza:

Możliwa jest poprawa skuteczności weryfikacji użytkowników systemu komputerowego poprzez wprowadzenie weryfikacji ciągłej wykorzystującej biometryczny profil aktywności, bazujący na obserwacji dynamiki użytkownika klawiatury oraz strategii automatycznej aktualizacji profilu aktywowanej progami decyzyjnymi.

Głównym celem rozprawy było opracowanie autorskiego algorytmu tworzenia biometrycznego profilu użytkownika oraz nowatorskiej metody ciągłej weryfikacji użytkowników opartej na klasyfikatorach, pozwalającej na automatyczną aktualizację profilu behawioralnego. Zadaniem algorytmu jest wyznaczenie biometrycznego profilu uprawnionego użytkownika na podstawie analizy dynamiki pisania na klawiaturze KDA (ang. Keystroke Dynamics Analysis). Profil jest wykorzystywany do weryfikacji użytkownika na podstawie jego bieżącej aktywności i umożliwia weryfikację użytkowników w sposób ciągły. Opracowane algorytmy zostały porównane z innymi technikami weryfikacji bazującymi na analizie dynamiki pisania na klawiaturze. Kolejne etapy realizacji celu głównego obejmują określone w rozprawie **cele szczegółowe**:

1. Akwizycja danych biometrycznych.
2. Opracowanie bazy danych do testów.
3. Opracowanie algorytmu biometrycznego profilowania użytkowników, wykorzystującego zdarzenia związane z użytkowaniem klawiatury.
4. Opracowanie metody weryfikacji użytkowników na podstawie biometrycznego profilu aktywności.
5. Testowanie opracowanych metod na danych rzeczywistych.

W rozprawie przedstawiono autorską metodę weryfikacji użytkowników opartą na klasyfikatorach wspieranych kompetencjami i progami decyzyjnymi, co pozwala na automatyczną aktualizację profilu behawioralnego. Weryfikacja ciągła zwiększa bezpieczeństwo systemu i poprawia skuteczność weryfikacji użytkowników. Szczegółowe rozwiązania proponowanej metody zostały potwierdzone w szerokich badaniach empirycznych. **Tym samym potwierdzona została teza rozprawy.**

W ramach prac zaprojektowano oraz zaimplementowano oprogramowanie do ciągłej rejestracji aktywności użytkownika. Przeprowadzono proces akwizycji danych w rzeczywistych warunkach pracy użytkowników. Na podstawie zarejestrowanych zdarzeń systemowych utworzono własną bazę danych do testów o nazwie *realKDD*.

Pozwoliło to na opracowanie autorskiego algorytmu biometrycznego profilowania użytkowników wykorzystującego KDA oraz opracowanie metody weryfikacji użytkowników na podstawie profilu behawioralnego. W rozprawie zbadano wpływ parametrów profilowania na skuteczność weryfikacji i eksperymentalnie dobrano optymalne wartości parametrów algorytmu profilowania pod kątem maksymalizacji skuteczności.

W rozprawie przedstawiono kilka podejść do weryfikacji użytkowników, w których moduł weryfikacji bazuje na klasyfikatorach użytych pojedynczo, w wersji komitetowej oraz na klasyfikatorach wspieranych kompetencjami. Zaproponowana metoda weryfikacji została rozszerzona o strategię alertów z automatyczną aktualizacją profilu behawioralnego sterowaną progami decyzyjnymi, co poprawiło skuteczność weryfikacji.

Opisane w rozprawie autorskie strategie profilowania i weryfikacji były testowane na danych rzeczywistych i porównane z innymi metodami walidowanymi na tym samym zestawie danych testowych. W przypadku eksperymentów z wykorzystaniem bazy *realKDD* opracowane metody porównano z metodami stosującymi bazę ClarksonII, która charakterystyką była najbardziej zbliżona do bazy *realKDD*. Autorskie algorytmy dodatkowo walidowano używając benchmarkowej bazy Buffalo. Eksperymenty potwierdziły wysoką skuteczność zaproponowanych w rozprawie metod. W badaniach porównawczych, za pomocą testów statystycznych, wykazano wyższość metod autorskich nad innymi, znanymi z literatury.

Tym samym zrealizowane zostały wszystkie cele określone w rozprawie.