Contribution ID: **485** Type: **Sectional talk**

Hybrid Continuous Authentication System Based on Risk Analysis and Keystroke Biometrics

Thursday 10 July 2025 15:45 (15 minutes)

User authentication is one of the core components of any secure distributed computing system. Traditional methods typically rely on static, one-time verification steps (e.g., password entry at login), which leaves active sessions vulnerable to takeovers. In response to this challenge, the concept of continuous authentication (CA) has gained traction –an approach where user identity is verified repeatedly throughout the session using behavioural or contextual signals. This paradigm aligns closely with the zero-trust security model, which operates on the principle of "never trust, always verify."

This work presents the architectural design of a hybrid continuous authentication system suitable for deployment in distributed computing platforms. It integrates machine learning-enhanced risk-based authentication (MLE-RBA) with keystroke dynamics analysis. MLE-RBA evaluates contextual factors such as device type, IP address, and access time to estimate the likelihood that a session is legitimate. Keystroke dynamics, in turn, provide a behavioural biometric based on how the user types, allowing the system to monitor for deviations from the legitimate user's typing profile during the session.

The proposed system architecture combines these two methods in a risk fusion engine that periodically assesses both contextual and behavioural data to determine whether further authentication is required. This design is well-suited for distributed environments, where contextual signals may vary widely across nodes, and where keystroke-based biometrics can provide a consistent, user-centered verification layer. The approach improves resilience against credential theft and mid-session hijacking while minimizing user disruption.

While this paper focuses on architectural design, earlier experiments with MLE-RBA indicate that machine learning methods significantly improve anomaly detection over classical RBA approaches. The combination with keystroke biometrics is expected to further strengthen real-time detection of intrusions without imposing constant friction on the user.

This hybrid model lays the groundwork for secure, user-friendly authentication in distributed environments, and constitutes a promising direction for practical zero-trust authentication.

Keywords: continuous authentication, risk-based access, keystroke biometrics, anomaly detection, zero trust

Authors: MATIUSHIN, Iurii (Saint Petersburg State University); KORKHOV, Vladimir (St. Petersburg State University)

Presenters: MATIUSHIN, Iurii (Saint Petersburg State University); KORKHOV, Vladimir (St. Petersburg State University)

Session Classification: Methods and Technologies for Experimental Data Processing