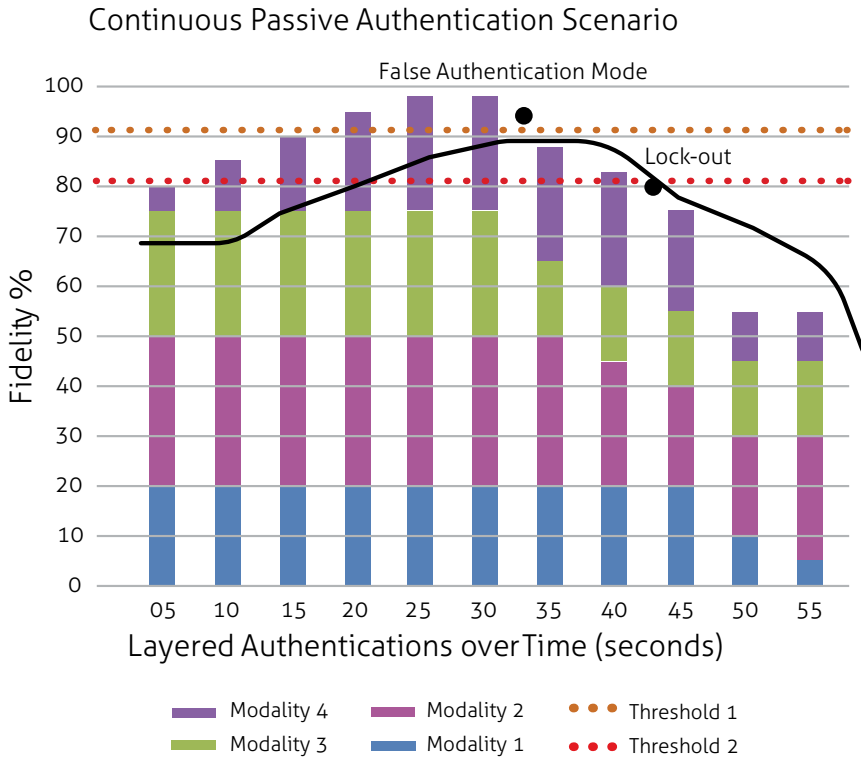
IMPROVING AUTHENTICATION MECHANISMS FOR ENTERPRISE INFORMATION SYSTEMS

The current standard mechanism for user authentication on an information system requires users to do something that is inherently unnatural: create, remember, and manage long, complex passwords. This security mechanism is susceptible to counterfeiting, spoofing, entry error and memory lapses. Moreover, as long as the session remains active, typical systems do not currently incorporate mechanisms to verify that the original, authenticated user is still the user in control of the keyboard and subsequent system applications in use.

The Active Authentication (AA) program under the DARPA Innovation Information Office (I2O) seeks to address these gaps in continuous authentication by developing novel ways of validating user identity at the console. The AA program is aimed at actively leveraging unique behavioral and/or cognitive aspects of the individual user through the use of software-based biometric capture, matching, and authentication technologies.

Novetta is supporting technical research, design, and development of an Active Authentication Platform that continuously collects, fuses, scores, and produces layered fidelity rankings based on multiple aspects of an individual. Novetta is building a secure platform architecture that allows acquisition of raw sensor data and utilization of device sensor frameworks to set tailored collection parameters, thresholds, and event listeners. Novetta performs data collection, fusion platform and unit testing, and integrated system testing.



CONTINUOUS VALIDATION OF BEHAVIORAL AND COGNITIVE MODALITIES BASED ON USER-DEVICE INTERACTIONS

Current Operational and Performance Capabilities:

System software that continuously and transparently authenticates the user through device sensors.

Layered, combinatorial approach of using desktop-based modalities for continuous validation of identity.

Robust authentication solution that depends on multiple aspects of an individual.

Leverages existing built-in sensors through desktop environment without the need for additional hardware.

Even when unlocked, the device will recognize unauthorized use and can either lock or enter "false information" mode.

Future Potential Developments:

Mobile platform development to leverage built-in mobile sensors.

Package application for loading onto mobile platforms.

Features:

Insider threat detection and monitoring. Reduces risk of targeted attack by fusing input from multiple modalities.

Continuous, tiered identity management and authentication that works passively without interrupting normal device usage.

No user interruption until system's confidence level is breached based on thresholds settings.

Configurable remote monitoring and administrative capabilities.