FIGI Security Clinic

Cognitive Continuous Authentication

Jorge Coelho

4-5 December 2019
#financialinclusion

Sponsored by

BILL & MELINDA GATES foundation

Organized by

Committee on Payments and Market Infrastructures
BANK FOR INTERNATIONAL SETTLEMENTS

WORLD BANK GROUP

ITU

Risk-Based Authentication

- FIDO provides password-less, secure authentication
  - It doesn't solve some identity theft issues
- Each authentication attempt should be evaluated based on risk
  - Examples of Risk factors detection:
    - Location
      - Collect the geographical location of the authentication attempt
      - Detect anomalies
    - Device/Browser Fingerprinting (DBFP)
      - Collect the characteristics of the device and browser that are performing the authentication attempt
      - Ex. Browser type, browser version, OS, user-agent, screen resolution
      - Detect anomalies
    - Others (Source IP, Biobehavioral patterns, ...)
  - According to the calculated risk, additional multi-factor authentication steps may or may not be required

Acceptto's Cognitive Continuous Authentication

- Creating a password-less authentication system involves issues that are not solved by FIDO
  - Credential Management (accounts with multiple authenticators, account deletion and recovery, ...)
  - Identity proofing
  - Post-Authorization continuous authentication

- FIDO + Risk Based Authentication + AIML = Acceptto's Cognitive Continuous Authentication
  - Provides a Multi-Factor Authentication system on top of FIDO
  - Access is granted via policies based on sensitivity of transactions and resources
  - AIML engine creates user behavior profiles that ensure additional authentication methods are required if needed
  - Strong user identity proofing (Email, SMS, Device Fingerprint, Corporation Filter, ...)

Acceptto's Cognitive Continuous Authentication