Activation-match: Transforming resource access with independent, multi-modal biometric methods organically interested in superior security and user experience

Introduction

Passwords are outdated and undermine security and user experience. Our problems don't stem from user password selection or poor cyber hygiene; the issue is the unproductive nature of passwords. Users juggle dozens of complex and increasingly uniquely constrained passwords, highlighting the need for a better method of secure resource access and identity authentication. Our vision is simple: minimal user effort, maximum security (zero trust). We're reimagining resource access and identity authentication to recognize users as humans with physical and digital modals of life.

Solution: Activation-match

Activation-match is an algorithm of next-generation resource access and identity authentication strategies built on two independent biometric processes: one local (e.g., fingerprint or palmprint) and one cloud-based (e.g., retina, sclera, and iris combination). This design is simultaneous and frictionless for users, mathematically superior to current standards of resource access, and more privacy-preserving than traditional logins or single-biometric methods, given our novel distributed data architecture that leverages randomization of code chains and indexing of information chains.

Key features

- Multi-modal combinations of biometrics: Uses two or more independent biometric processes simultaneously to enhance security and user experience.
- Local and cloud-based distributed system: Combines local verification (activator biometric) with cloud-based identification (matcher biometric) methods to ensure robust, resilient security system.
- Privacy-preserving data architecture: Keeps all personally identifiable information (PII) off the cloud, storing it locally and protecting it through the activation-match process.
    - Code chain changes randomization and deployment of XML-based code (non-predefined code)

Applications

Activation-match can replace passwords, passcodes, PINs, physical credit and debit card transactions, access and QR codes, CAPTCHAs, public transit cards, gift and store cards, and keys. It offers seamless resource access for both physical and digital realms.

Advantages over existing solutions

- **Enhanced security**: Requires spoofing multiple unrelated biometric traits.
- **Eliminates passwords**: Removes phishing targets and user frustration.
- **User-centric workflow**: Guides towards effortless resource access, leveraging the uniqueness of the user as the credential.

Security architecture

The activation-match method introduces a novel security architecture that distributes data and trust between the user's device (local data store) and the cloud, while keeping all PII in the local encrypted store. By splitting the biometric factors, we ensure that no single biometric can defeat the system.

Device-side security

The fingerprint, palmprint, or other method used as local activator is stored and verified on the user's device within a secure local store. Modern smartphones and laptops have secure co-processors or subsystems (like Apple's Secure Enclave) that can store biometric templates and perform matches in an isolated environment. While many companies and solutions deploy this device-side security as an absolute solution currently, we view this solution as having information-bias and thus define it solely as a sufficient *verification* method (we define *authentication* as *verification* and *identification*, with the latter being the more rigorous process).

Server-side security

The retina, sclera, and iris scans that are independently and unbiasedly matched against their respective global template libraries – a process that combinedly serves as our cloud-based matcher solution. It's a process entirely absent of PII.

Conclusion

Activation-match offers a seamless, secure, and user-centric solution for resource access and identity authentication. By leveraging multi-modal biometrics and distributed data architecture, we can significantly enhance security and user experience across sectors.