GCN

INDUSTRY INSIGHT

Next-generation identity assurance for mobile environments

By Sarbari Gupta

May 23, 2019

Traditional authentication models are limited to one-, two- or three-factor authentication with remote verification services siloed from one another. Each verification service, which stores user authentication reference data, requires transmission of live authentication data from the user over shared networks.

The Hyper-Authentication (HyperAuth) framework improves user privacy protection and enhances user experience by providing rapid local authentication. It eliminates the need for unique passwords for each application and gives users access to services once considered too sensitive for mobile platforms.

HyperAuth does so by leveraging the unique capabilities and features of smart mobile platforms (e.g., sensors and contextual information) to implement multifactor and context-aware local (on-device) authentication verification services using authentication reference data (e.g., biometric templates) stored securely on the device. It transforms the mobile platform into a self-contained, privacy-protecting authentication machine that supports various authentication and contextual factors.

Key features and benefits of HyperAuth include:

A standard framework for transaction-based risk decisions.

Secure on-device storage of authentication reference data.

Local identity authentication verification services.

Context- and environment-based authentication risk assessment.

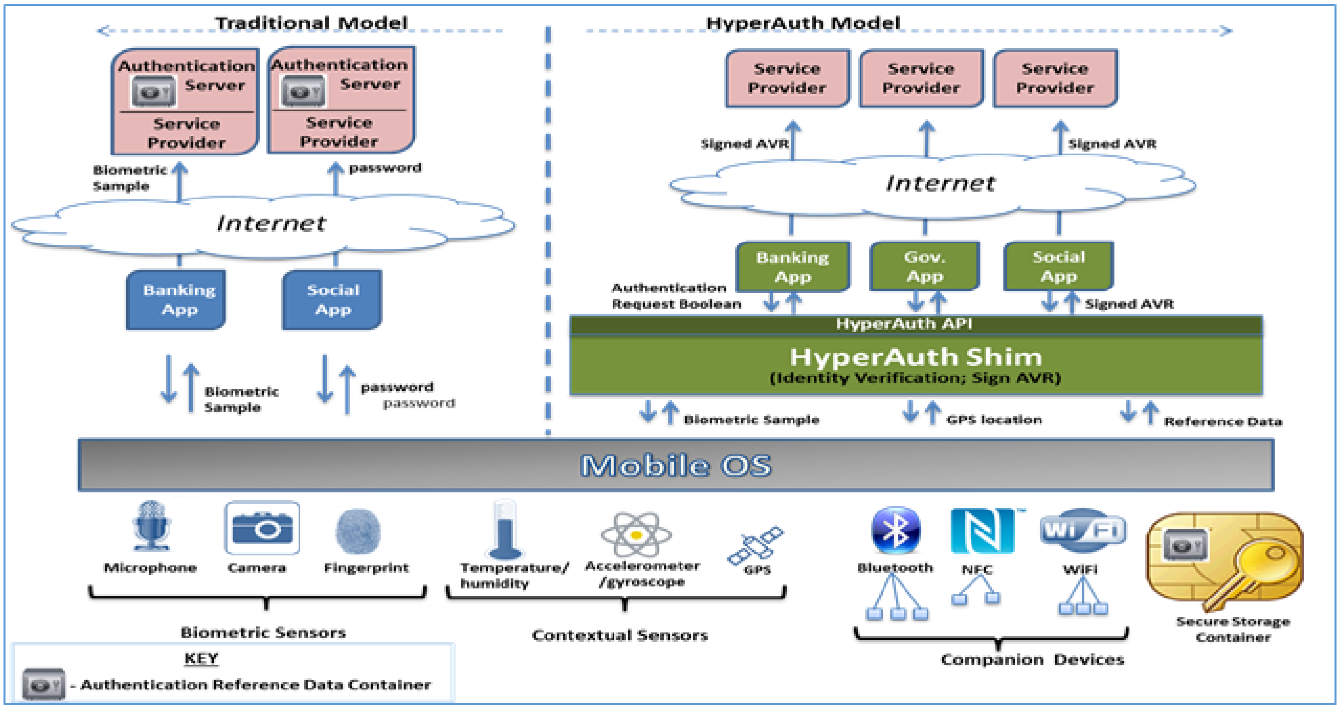
Multiple authentication assurance levels that allow diverse policies for different applications.

Logical boundaries for authentication assurance.

Foundation for continuous user authentication.

Traditional computing platforms employ the well-established three-factor approach: something you know (e.g., password), something you have (e.g., token or cryptographic key) and something you are (e.g., biometric). Many consider biometric authentication over public networks to be inappropriate because live biometric samples are transmitted over an untrusted network. Also, each remote service provider acts as an authentication service, establishing an identity and authentication token for access. Users thus must establish and use an authentication token unique to every service. Figure 1 (left half) illustrates the traditional model.

Figure 1



Mobile computing platforms offer a range of reliable data from biometric and context-related sensors that can be used to authenticate the device user and balance risk against the type of service being provided. These platforms also offer application sandboxing, reliable network time, cryptographic capabilities and secure storage containers that can be leveraged to implement innovative authentication models that outpace the three-factor approach. Mobile devices thus make local identity verification practical and secure in mobile platforms with the right architecture.

The HyperAuth framework leverages device capabilities and features to improve privacy protection of user data and user experience. Figure 1 (right half) illustrates the HyperAuth model and its components including:

An authentication assurance model incorporating multiple authentication factors (biometrics, PIN/password, cryptographic keys, etc.) and contextual factors (GPS location, time since last use, paired companion devices, etc.) to derive an authentication assurance score.

A security model allowing authentication verification activities to be performed on the local mobile platform and delivery of authentication verification results to mobile apps.

An application programming interface allowing mobile applications to request authentication services from an authentication module local to the mobile platform via a standardized set of calls.

To demonstrate framework feasibility, a lightweight prototype of the HyperAuth Shim was developed (using Android API calls to implement authentication using various on-board sensors and authentication reference data held in the secure container) and a set of HyperAuth mobile applications that request authentication services at different levels of authentication assurance. The HyperAuth Shim module (see Figure 1) uses the Android resources and API to

Secure live samples from biometric sensors.

Obtain contextual data from sensors/data sources.

Request reference biometric and contextual data from the secure storage container.

Perform authentication verification by comparing live data (biometric and contextual) against reference data.

The HyperAuth API allows mobile applications to query the authentication services available on the mobile device, request a set of authentication services as Boolean or vector and obtain a signed authentication verification result (AVR) that serves as an authentication status token.

In practice, the HyperAuth concept would operate as follows:

A user takes the mobile device to a HyperAuth identity provider to initialize the HyperAuth Shim and the local secure storage container with the user's biometric reference data, cryptographic keys and selected contextual reference data. The IdP conducts the traditional identity proofing activities prior to initializing the HyperAuth Shim, which possesses a unique asymmetric key-pair and signing certificate issued by the IdP. The user then personalizes the HyperAuth Shim with additional biometric reference data or contextual data.

When the user goes to a bank, for example, to create a mobile-accessible account, the bank's one-time password pairs the account to the mobile application. The user downloads the mobile application and connects to the account using the one-time password, and authenticates with a combination of authentication factors using the HyperAuth Shim.

When the user initiates a mobile banking transaction, the app asks the HyperAuth Shim to authenticate the user. The Shim authenticates the user and delivers a signed AVR to the mobile banking application. When the signed AVR is transmitted to the remote banking server as a token of authentication success (or failure), the banking server validates the AVR signature and delivers the requested banking service.

In summary, HyperAuth offers a unique authentication model wherein authentication verification can be performed local to the mobile platform, resulting in better performance, increased privacy and improved user experience.

About the Author

Sarbari Gupta is a cofounder, president and CEO of Electrosoft Services.