Identity Based Attestation and Open Exchange Protocol (IBOPS)

Scott Streit
scott@scottstreit.com
Chief Scientist
Hoyos Labs
Identity Based Attestation and Open Exchange Protocol (IBOPS)

Presentation Report on new working group on Identity based attestation
https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ibops

Purpose

• Developing a biometrics specification for security systems to support identity assertion, role gathering, multi-level access control, assurance, and auditing capabilities

Overview

■ The IBOPS TC is chartered to produce an end-to-end specification describing the standards necessary to perform server-based enhanced biometric security. This solution will consider enrollment phase, maintenance, storage, and revocation. IBOPS will define how software running on a client device can communicate with an IBOPS-enabled server. The IBOPS specification will provide continuous protection of identity resources in a manner that enables defining of mechanisms that ensure security to a given service level guarantee of security.

■ The IBOPS TC may also develop interoperability profiles for the OASIS Trust Elevation Protocol, FIDO, SAML, OpenID Connect, and OAuth
Why IBOPS?

- We need an inter-operable specification to offer the “what” of communication, authentication and access control for biometric based security
- We need guidance to prevent attacks on systems
- We need a set of best practices for security
- We need an end-to-end approach to security which goes beyond identity
  - up through trusted storage and adjudication
Use Cases

• ATM for Banks allowing secure access to money
• Cars for preferences
• Buildings for entry
• Removal of user names and passwords
• Removal of the need for credit cards
• Biometrics are always with you and only you
• Liveness removes facsimiles of biometrics guaranteeing you are actually a live you.
• Liveness gives us a convenience vs. security choice.
What is IBOPS

• IBOPS comprises the rules governing secure communication of biometrics-based identity assertion between a variety of client devices and the trusted server.
• Provides Identity Assertion, Role Gathering, Multi-Level Access Control, Assurance, and Auditing.
• It creates a uniform standard for the proper use and secure application of biometrics in an Identity Assertion environment, where the goal is Authentication, not authorization
• It defines the roles for secure communication in a biometrics-based identity assertion transactional environment between the devices
• It protects the users privacy: no biometrics must ever leave the mobile device, and all matching must occur in the device
• It defines clear rules for how biometrics and liveness, with levels of convenience, must operate on the mobile device and in the complete identity assertion process, end-to-end
IBOPS Key Rules

• Does not allow user biometric data to be stored in any back end repository
• Requires all data to be fully encrypted, even in an underlying secure transfer layer
• Biometric Match will always happen on device, so as to protect users privacy as well as their data
• Private Key generation will occur in a secure server behind a firewall and not on the device
  • Avoids attacks that could lead to key factories.
• Critical data is to be kept encrypted on device
• Parse out information, distributing it in such a way that only indexes + “minimal” information are found in repository
  • worthless to a hacker
• This paradigm forces hackers to hack a user at a time since there is no one repository of critical data, thus deterring massive breaches of data.
• Secure all access to back end repositories, severs, systems with mobile device based biometric access
Key Rules

- Encrypt all information residing on mobile device with minimum cypher requirements and secured via users biometrics
- IBOPS allows pluggable components to replace existing components functionality accepting integration into current operating environments in a short period of time.
- IBOPS-compliance should use well established standards set by NIST, ITU-T, ISO for accepted levels of image quality and security
- Require Liveness Detection Technology (LDT) to be deployed in conjunction with an Intrusion Detection System (IDS) on the device and back end
  - This will protect against spoofing
- IDS will monitor all systems and data traffic in ALL connected devices and servers in an environment
  - defense against “Replay Attacks” and “Man in the Middle Attacks”
- We are in the middle of the “Hacking Wars” era, we can not ignore any of this any longer
Next Steps

- New work is staring with focus on full collaboration and future standardization at the ITU-T SG 17
- Please join us