IAWG Meeting Notes 2015-10-01
Kantara Initiative Identity Assurance WG Teleconference

Date and Time

- **Date:** Thursday, 2015-10-01
- **Time:** 12:00 PST | 15:00 EST
- **United States Toll** +1 (805) 309-2350
- **Alternate Toll** +1 (714) 551-9842
- **Skype:** +99051000000481
  - Conference ID: 813-2898
- **International Dial-In Numbers**

Agenda

1. Administration:
   a. Roll Call
   b. Agenda Confirmation
   c. Minutes Approval (since no decisions were taken none at this time)
   d. Action Item Review
   e. Organization Updates - Director's Corner
   f. Staff reports and updates
   g. LC reports and updates
   h. Call for Tweet-worthy items to feed (@KantaraNews or #kantara)
2. Discussion
   a. Presentation from Dean Stamos about Oxford BioChronometrics
   b. Proposal from Secretariat that the IAWG move to classify the RAA and AAS as "ARB policy guidance"

Attendees

**Link to IAWG Roster**

As of 2015-01-22, quorum is 6 of 11

Meeting did not achieve quorum

Voting

- Ken Dagg (C)
- Scott Shorter (S)
- Andrew Hughes (VC)
- Richard Wilsher

Non-Voting

- Angela Rey
- Dean Stamos
- Colin Wallis

Staff

- Joni Brennan

Apologies

- None
Notes & Minutes
Administration

Minutes Approval
(no quorum at previous meeting, no minutes to approve)

Action Item Review

Staff Updates

Joni reports - the organization will be expanding next couple weeks – expect to be joined by Telos from Canada.
Participating in the European workshop for trust and identity, and the GSMA for the Americas in NYC.
Scott mentions that Chi Hickey has signed the group participation agreement, will be joining the IAWG as a voting member.

Director's Corner Link

LC Updates

Participant updates

Discussion

Ken introduces Dean Stamos, the US representative of Oxford Biochronometrics. He speaks to Dean's biography (q.v. http://senahill.com/who-we-are/our-network/)
The company is based in Luxembourg, with the goal of preventing unauthorized access, tell bots from humans and humans from each other. Prevent digital ad fraud, eliminate username/password, reduce the need for MFA.
Dean begins - clearly, "unspoofable" is an impossible the goal is "economically unfeasible". The company is three years old, based on an Oxford thesis on the topic of identifying users across the internet based on their behavioral characteristics. Oxford University incubated, still owns part of the company.
Based on "human recognition technology". There are three stages - three testing levels to determine it. Usually isntantaneous. There's a subset of bots "humanoid bots" that mimic human behavior.
Product called "no more CAPTCHAs" - its moved from being an accessibility product and into being a cybersecurity product. Most attacks, whether brute force, man in the middle, or you name it, are scripted attacks rather than humans clicking on keyboards.
Second tech is advanced form of device recognition - we all know that any device can be cloned. The trick is not just to obtain a hardware signature, but also the characteristics of the system. Gyroscope and accelerometer moving mean that the device is not a server on a rack.
No download of software onto the device, or hardware requirement. Small Javascript on website is enough to monitor though.
The human-identity component, determining that the right human is holding the device. This can change identity proofing and can enhance privacy. The methodology is concerned with your behavior when interacting with a secure session. No names stored, no KBA, no PII is involved with the process. From a bank or Relying Party point of view they get a unique id from OBC instead of a name.
For the final expression - EG&A - the function determines if it's the right device and the right person with the right device. 480 data points
Richard Wilsher asks - when talking about the characteristics of the usage of a handheld device, the characteristics of the use will vary based on a number of factors.
Dean responds - clearly it depends on how you weight things - if driving in a certain radius between work and home, that is a reasonable. Typing characteristics change over time. A fairly important part of the technology is the security component of it - the accelerometer and gyroscopes are huge. After “eDNA” is established, you probably only need 10% of the potential metrics to validate the identity. If there’s biochronometrics server behind a bank’s wall, and that server is what knows what its looking for. A spoofer doesn’t know what to attack. By randomizing the factors being looked at to establish identity.

Establishment of eDNA can take three weeks to three months.

Angela Rey asks about the difficulty of establishing identity of citizens.

Ken refers to the challenge that governments interact with citizens once or twice yearly, and the issue of multiple agencies not being able to identify the same users.

Dean agrees that it would take a long time to establish the eDNA proof in the case of very infrequent interaction. The data sharing component - from Dean’s understanding this means a person’s name. The information gathered is about what is the behavior when interacting with a device.

eDNA - is the equivalent of a 16 million character nondeterministic code. Nondeterministic means of identity proofing is where we’re going.

Angela asks if the approach is compromised if not using the same device or not logging in the same way. Dean responds that it is definitely affected by this. eDNA is a profile on a cell phone, on tablet, etc. that all fall under the main eDNA profile.

Angela mentions that government is considering the potential of public devices, where many people might be able to access it. Is that model applicable with the OBC methodology - Dean responds yes but more difficult.

Dean observes that the lack of industry standard is part of the issue. If 800-63 is the industry standard then that represents archaic view.

Joni appreciates the comments on industry standards, what we are trying to do is help bridge the gap between technology and policy. Help solve the methodology of keeping up with the times, how to review innovative solutions that don’t meet the rigid standard.

Ken - thanks for introducing us to a leading edge and in some case disrupting approach.

AOB

Attachments

Next Meeting

- **Date:** Thursday, 2015-10-08
- **Time:** 12:00 PT | 15:00 ET
- **Time:** 12:00 PDT | 15:00 EDT
- United States Toll +1 (805) 309-2350
- Alternate Toll +1 (714) 551-9842
- **Skype:** +99051000000481
- Conference ID: 613-2898
- Discussion topic will be
  - review of IAF 5415
  - revisit the RAA and AAS
  - comment response to FICAM