DARPA's Active Authentication Phase 2 Proposers' Day

Mr. Richard Guidorizzi
Program Manager
DARPA, I2O

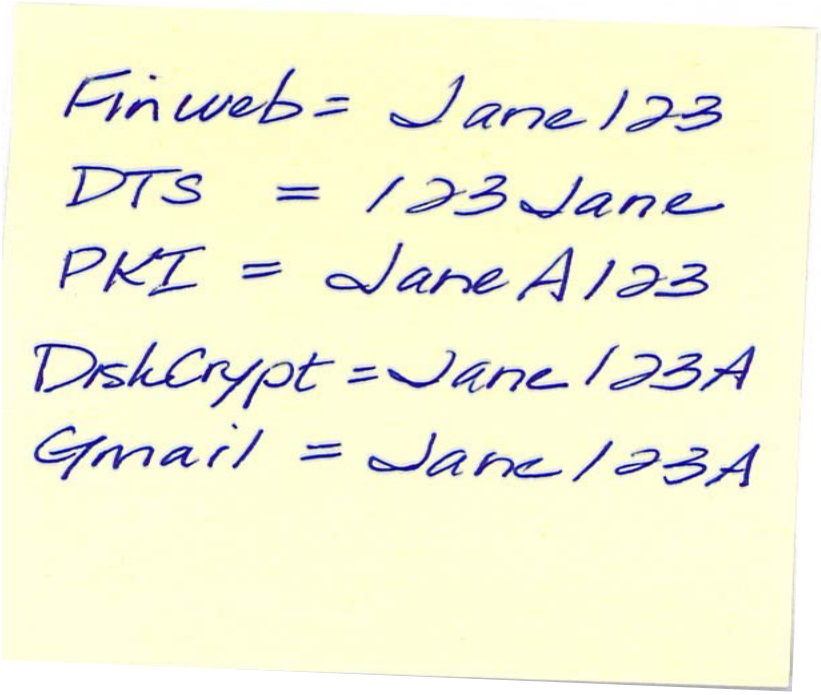
Program Overview

February 8, 2013

The Active Authentication Phase 2 BAA posted at www.fbo.gov will take precedence over the information provided herein.

Approved for Public Release, Distribution Unlimited

Active Authentication Program Background



Passwords will never work as a truly secure identification solution because they:

- Provide no information about the person at the keyboard, they are simply data;
- Are intended as a proxy for person at the keyboard and proxies can be faked.

How do we move from proxies for you to the actual you?

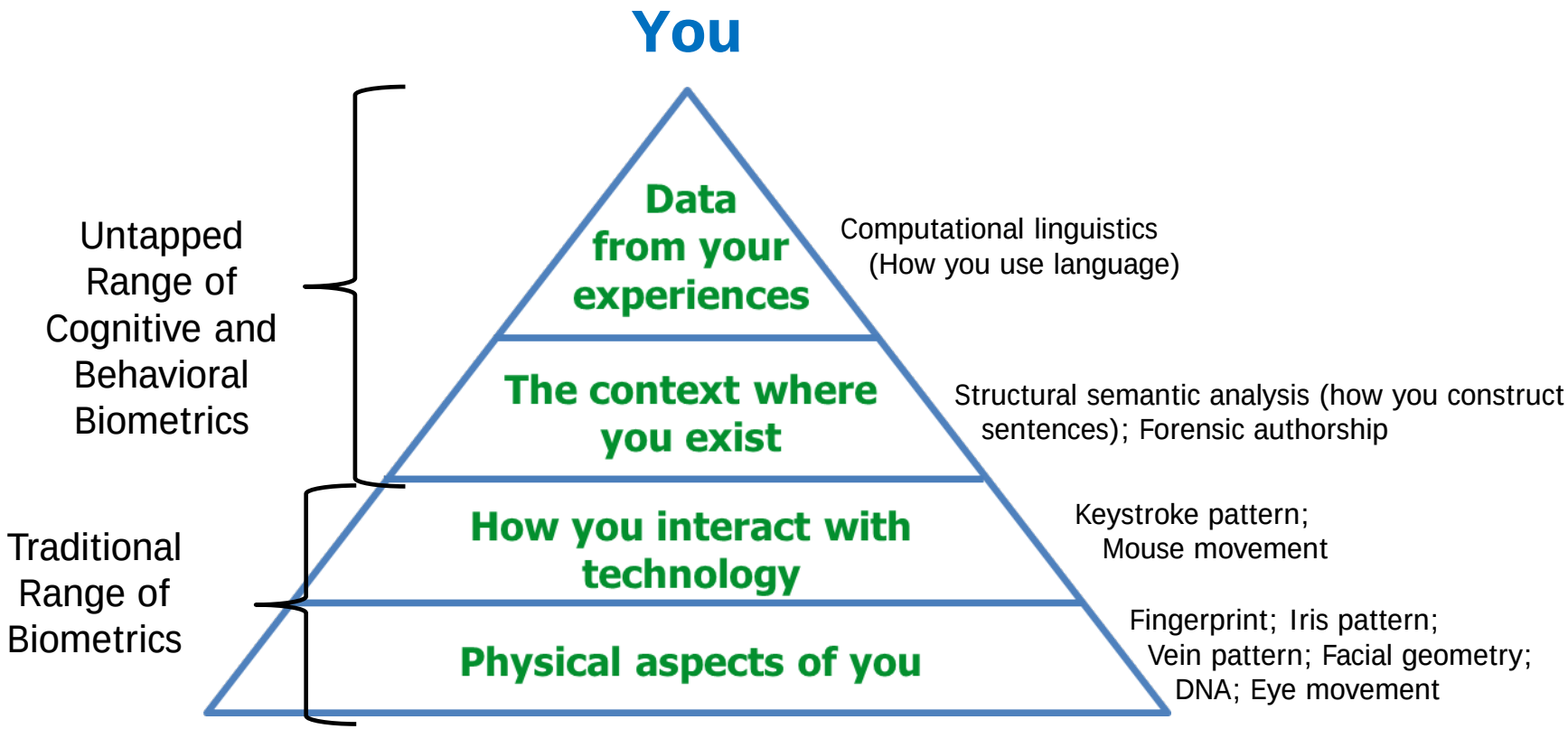
By using biometrics that don't require the user to do anything different, and that collect the biometric information without deployment of sensors.

We can turn available data from normal computer use into biometric features, and then use that information for the validation of identity without interrupting the user doing work.

Approved for Public Release, Distribution Unlimited

The Active Authentication Program

A continuous authentication solution that takes the data available on a DoD IT device and makes an informed decision on the identity of the user of the device.



Leverage cognitive and behavioral biometrics that allow the validation of identity simply by the user acting normally, i.e., not requiring interruption of the user.

Active Authentication Program Goals

- Expanding research in the area of the computational behavioral traits that can be observed through how a computer user interacts with the world without requiring them to do anything different from their normal work functions.

- Developing an application ("Biometric Platform") that can integrate all biometrics available on a single device to allow for the most accurate validation of the identity of the individual using the device, whether the biometrics collected are behavioral, cognitive, or physical. In this respect, the application is trying to identify you by looking at all available aspects of you, not just a single sensor connected to the device.

Approved for Public Release, Distribution Unlimited

Active Authentication Program Plan

The overall Active Authentication program was developed with three planned phases.

Phase 1 (addressed in a previous solicitation):

- Focused on expanding research on software-based biometrics that did not interrupt a computer's user and proving, with tests on human subjects, that these new biometrics were effective in identifying an individual using a standard DoD desktop.

Approved for Public Release, Distribution Unlimited

Active Authentication Program Phase 1 Research

Neuro-Cognitive Patterns – Naval Postgraduate School	
	Developing digital "cognitive fingerprints" from various biometric sources; potentially developing a framework for identification of other behavioral biometrics. Also able to provide behavioral forensics of the user to ascertain shifts in thought process, social programming, belief structure, etc.
User Search Patterns – Allure Security Technology, Inc.	
	Using the user's patterns for searching for information on the computer, verified by high volumes of decoy document touches placed in the file system.
Keystroke and Mouse Dynamics – BehavioSec	
	Enhancing keystroke & mouse behavioral biometrics with large scale user trials including research into the areas of continuous trust models & application usage patterns.
User Behavior Patterns As Seen From the Operating System – Coveros	
	Using traditional computer-based IDS algorithms on user behavior (as seen in OS interactions) to determine when someone other than the authorized user is accessing the system.
Stylometry – Drexel University	
	Using traditional stylometric methods to validate a user based on what they are typing. Also researching how to detect adversaries who attempt to impersonate users through mimicking typing methods.
Stylometry focused on Cognitive Processing Time – Iowa State University	
	Using stylometric methods to validate the user based on natural pauses in the way they type.
Stylometry focused on Cognitive Rhythms – NYIT	
	Using text productivity, pause, and revision behaviors to validate users based on how they type (includes content/language).
Covert Games – Southwest Research Institute	
	Determine the user's pattern of behavior by introducing patterned system aberrations that the user intuitively learns, i.e. hidden games in the computer interface.
Screen Interface – University of Maryland	
	Using spatio-temporal screen fingerprints to identify the user for authentication.
Behavioral Web Analytics – Naval Research Labs (NRL funded)	
	Identification of the user from Web browsing activities to include semantic (what kind of webpages are visited) and syntactic session features.

Active Authentication Program Plan – Phases 2 & 3

Phase 2 (addressed in this solicitation):

- Continue research on biometric modalities that will not interrupt a desktop user's normal operations and can be validated by empirical testing, and will add a third criterion that the modalities can be integrated into the Desktop Biometric Platform.
- Explore new pilot biometric modalities that can work in a mobile environment (e.g., smartphone, tablet). The focus for this aspect will be on researching biometrics that do not require the installation of additional hardware sensors and can be captured through the technology already in use in a mobile environment, looking for aspects of the cognitive fingerprint.

Phase 3 (addressed in a future solicitation):

- Develop additional Pilot Biometric Modalities for desktops and, depending on the success of Phase 2 research, those for mobile environments;
- Develop Biometric Platform(s) for mobile environments;
- Transition the desktop application (Biometric Modalities + Biometric Platform) to an operational partner.

Approved for Public Release, Distribution Unlimited

Active Authentication Program Plan – Technical Areas

The key aspects of the program are addressed by the following Technical Areas (TAs):

TA1: Pilot Biometric Modalities

- TA1a – Desktop *(solicited under this BAA and possible Phase 3 solicitation)*
- TA1b – Mobile *(solicited under this BAA and possible Phase 3 solicitation);*

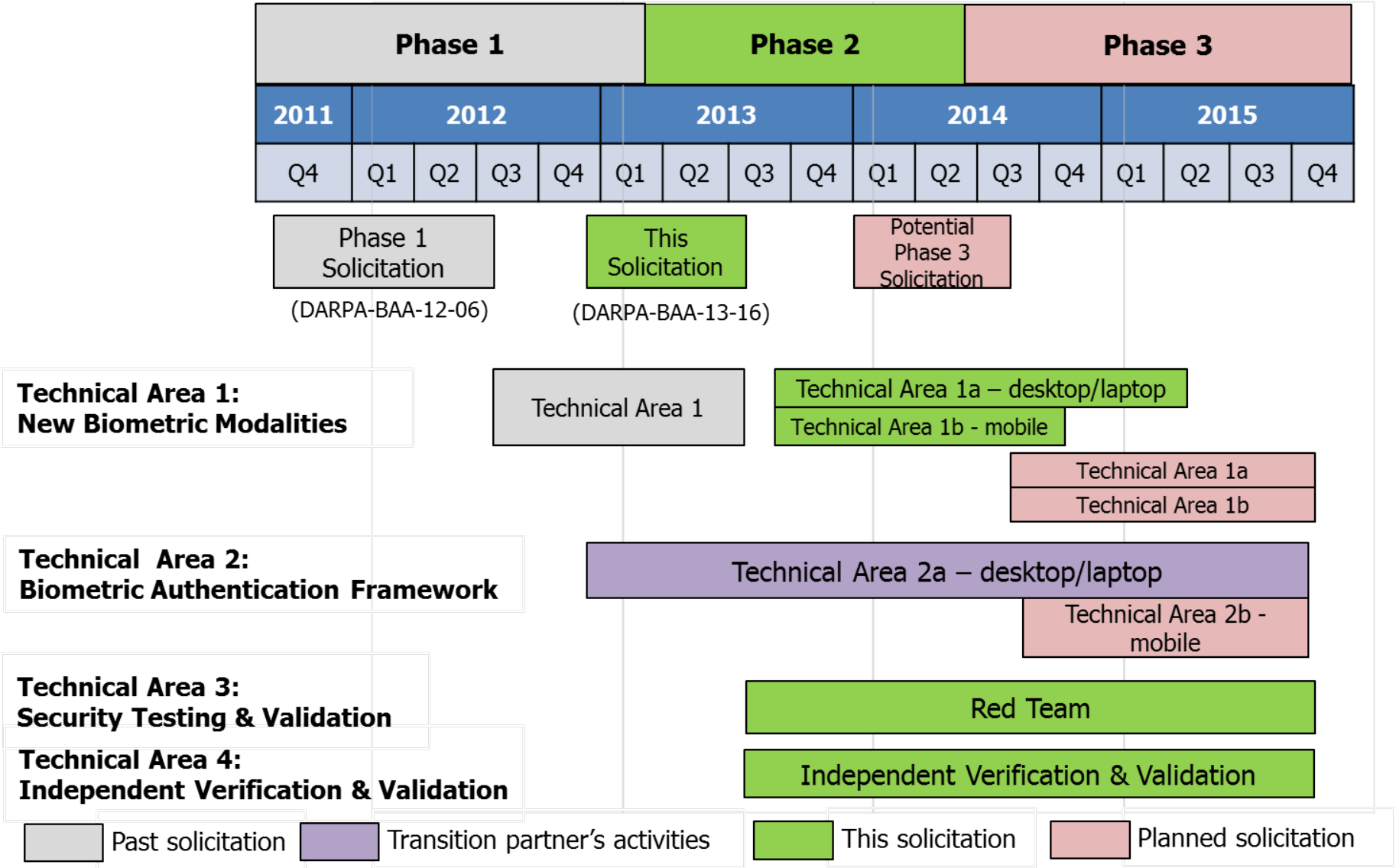
TA2: Biometric Platform

- TA2a – Desktop *(performed by transition partner - not solicited under this BAA)*
- TA2b – Mobile *(possible Phase 3 solicitation only - not solicited under this BAA);*

TA3: Security Testing and Validation - Red Team *(solicited under this BAA); and*

TA4: Independent Validation and Verification *(solicited under this BAA).*

Active Authentication Planned Program Schedule



Approved for Public Release, Distribution Unlimited

How will the desktop application validate identity?

The application takes data from available biometric features on the computer to validate the person at the keyboard.
It uses the features available to develop a secure "key" that can be passed to the server and validate the user's identity.

Claimed identity

Desktop Biometric Platform

Validates Level of trust in Identity

Biometric Data

Validated access

Keys are validated on the server using the same algorithms and features for the claimed identity

Key exchange provides access

Only the key is passed over the wire

Keys are established using any available biometric modalities, that are pulled in when available, adding context as an additional validation.
In other words, when the keyboard is being used, keyboard behavioral modalities become available to the client application; when it is not, they are invalid (to catch "replay attacks" trying to spoof the application).

Active Authentication Phase 2 Solicitation Notes

- Single awards are expected for Technical Areas 1a, 3 and 4. Multiple awards are expected for Technical Area 1b.

- Technical Area 2a is being performed by DARPA's transition partner and is not open for proposals under this solicitation. Technical Area 2b is not open for proposals under this solicitation.

- Proposers may submit against any or all of TAs 1a, 1b, 3 and 4; however, separate proposals must be submitted for each technical area, with the exception of TA1a and TA1b. Proposers who plan to submit to both TA1a and TA1b may combine both areas into one proposal; however, each biometric modality must be proposed as a separate task in the Statement of Work and Cost Volume. By the same token, proposals for only TA1a or TA1b may include multiple modalities in one proposal however, each modality must be proposed as a separate task in the Statement of Work and Cost Volume.

- Proposers should note that they cannot receive awards in either TA3 or TA4 if they receive an award in TA1a or TA1b due to conflict of interest concerns.

Approved for Public Release, Distribution Unlimited

Technical Area #1a
Pilot Biometric Modalities - Desktop

- Pilot biometric modalities will focus on behavioral-based biometrics that validate the identity of an individual without interrupting their normal work process.
- Proposals are expected to include a one year base and a one year option.
- Total funding for this Technical Area is expected to be approximately $1.8M.
- DARPA anticipates a breakdown of the work/funding to be: 57% in FY 2013; 43% in FY 2014.
- DARPA expects the solution to be demonstrated quarterly, with an integrated demonstration annually with the Desktop Biometric Platform.
- After contract award, the TA2a developers will work with the TA1a performer to establish standards (APIs) for application communication.

Technical Area #1b
Pilot Biometric Modalities - Mobile

- Pilot biometric modalities will focus on behavioral-based biometrics that validate the identity of an individual without interrupting their normal work process.

- Proposals are expected to include a one year base (or less, if appropriate).

- Total funding for this Technical Area is expected to be approximately $3.4M over 12 months (no more than $500K per performer).

- DARPA expects the solution to be demonstrated quarterly.

- DARPA is not specifying a particular hardware device. No solutions for a particular hardware device will be given preferential treatment over solutions proposed for other hardware devices. In this solicitation, DARPA seeks to advance research with regard to new biometric authentication solutions for mobile devices, and a solution that works for any mobile device currently on the market will be considered.

Technical Area #3
Security Testing and Validation (ST&V) - Red Team

- Provide Red Teaming or “Adversarial Partner” Subject Matter Expertise for Phases 2 and 3 of the program, providing a realistic picture of potential risk introduced with the new modality approaches during development. This also includes the development of the Desktop Biometric Platform and, potentially in Phase 3, Mobile Biometric Platform(s).

- Proposals are expected to include a one year base, a one year option, and a final six month option.

- Total funding for this Technical Area is expected to be approximately $1.2M over 30 months. The anticipated breakdown of the work/funding is: 21% in FY 2013; 63% in FY 2014; 16% in FY 2015.

- Red Team analysis is being included for all modalities developed under the Active Authentication program to ensure they do not increase the current available attack surface for DoD end users.

Technical Area #4
Independent Validation and Verification (IV&V)

- Provide Independent Verification and Validation of the developed code for the Biometric Platforms (Desktop and, potentially, Mobile) and the Pilot Biometric Modalities for Phases 2 and 3 of the Active Authentication program, ensuring the modalities function as planned.

- Proposals are expected to include a one year base, a one year option, and a final six month option.

- Total funding for this Technical Area is expected to be approximately $2.5M over 30 months.

- DARPA anticipates a breakdown of the work/funding to be: 40% in FY 2013; 40% in FY 2014; and 20% in FY2015.

- Independent Verification and Validation analysis is being included for all modalities developed under the Active Authentication program to ensure the overall integrated solutions can be deployed for DoD transition partners.

www.darpa.mil