

Active Authentication Beyond Passwords

Richard Guidorizzi, I2O Program Manager

18 Nov 2011



Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 18 NOV 2011		2. REPORT TYPE		3. DATES COVERED 00-00-2011 to 00-00-2011	
4. TITLE AND SUBTITLE Active Authentication Beyond Passwords				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Defense Advanced Research Projects Agency (DARPA),675 North Randolph Street,Arlington,VA,22203-2114				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES Presented during DARPA Active Authentication Proposer Day - November 18, 2011, Arlington, VA					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 23	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



How Computers Identify Us

Our present:



Our Future?





Active Authentication Program Goal

Computers watch their operators, and manage their level of access based on the accuracy with which they can determine the operator's identity



Source: <http://www.zuschlogin.com>



Source: 2.bp.blogspot.com



Users are the weak link...



Finweb = Jane123
DTS = 123Jane
PKI = JaneA123
DiskCrypt = Jane123A
Gmail = Jane123A



How many passwords do we really use?

DoD IT Asset Type	DARPA Reference System	Non-DoD IT Asset Type	Hacked on	Credentials lost
NIPRnet	Windows DMSS	American Honda Motor Co.	27-Dec-10	4.9m
Laptop Encryption	Guardian Edge	• Bank of America	25-May-11	1.2m
DARPA VPN	Nortel	Carnegie Mellon University	8-Oct-07	19k
PDA	Blackberry/iPhone	Citigroup	27-Jul-10	30m
SIPRnet	Windows DSN	Clarkson University	10-Sep-08	245
JWICS	Windows DJN	• Countrywide Financial Corp.	2-Aug-08	17m
Source Selection	TFIMs, I2O BAA Tool	• Fidelity Investments	24-Sep-07	8.7m
Contract Management	GSA Advantage, SPS	Heartland Payment Systems	20-Jan-09	130m
Contract Invoicing	Wide Area Workflow	IBM	15-May-07	2k
Payroll	MyPay	Johns Hopkins Hospital	22-Oct-10	152k
• Benefits	Benefeds.com	SAIC	7-May-08	630k
HR	hr.dla.mil	Sony	27-Apr-11	12m
• Training	DAU	Stanford University	6-Jun-08	82k
• Collaboration	Defense Connect Online	TD Ameritrade Holding Corp.	14-Sep-07	6.5m
Financial System, Local	Momentum	Texas A&M University	9-Nov-08	13k
Financial System, Agency	DFAS	TJMax Stores	17-Jan-07	100m
• Credit Union	PFCU, NCU, etc.	U.S. Depart. of Veteran Affairs	14-May-07	103m
		U.S. Marine Corp – PSU research	26-Jul-07	208k
		• Visa, MasterCard, and American Express	27-Dec-10	4.9m

Source: www.privacyrights.org/data-breach



MSNBC News Report: Cyber attack on Gannet Targets US Soldiers

Hackers broke into a Gannett Co database containing personal information about subscribers to publications read by U.S. government officials, military leaders and rank-and-file soldiers, the media company said on Tuesday.

Gannett told subscribers via email that it discovered the breach of its Gannett Government Media Corp on June 7. It said it had previously notified subscribers of the breach via a notice on its website.

The attackers accessed subscribers' names, passwords and email addresses, the company said. They also obtained data on the duty status, paygrade and branch of service of some readers who serve in the military.

The information included subscribers to Defense News — one of the world's most widely read publications covering the defense industry — as well as publications aimed at soldiers serving in the U.S. Army, Navy, Air Force and Marine Corps.

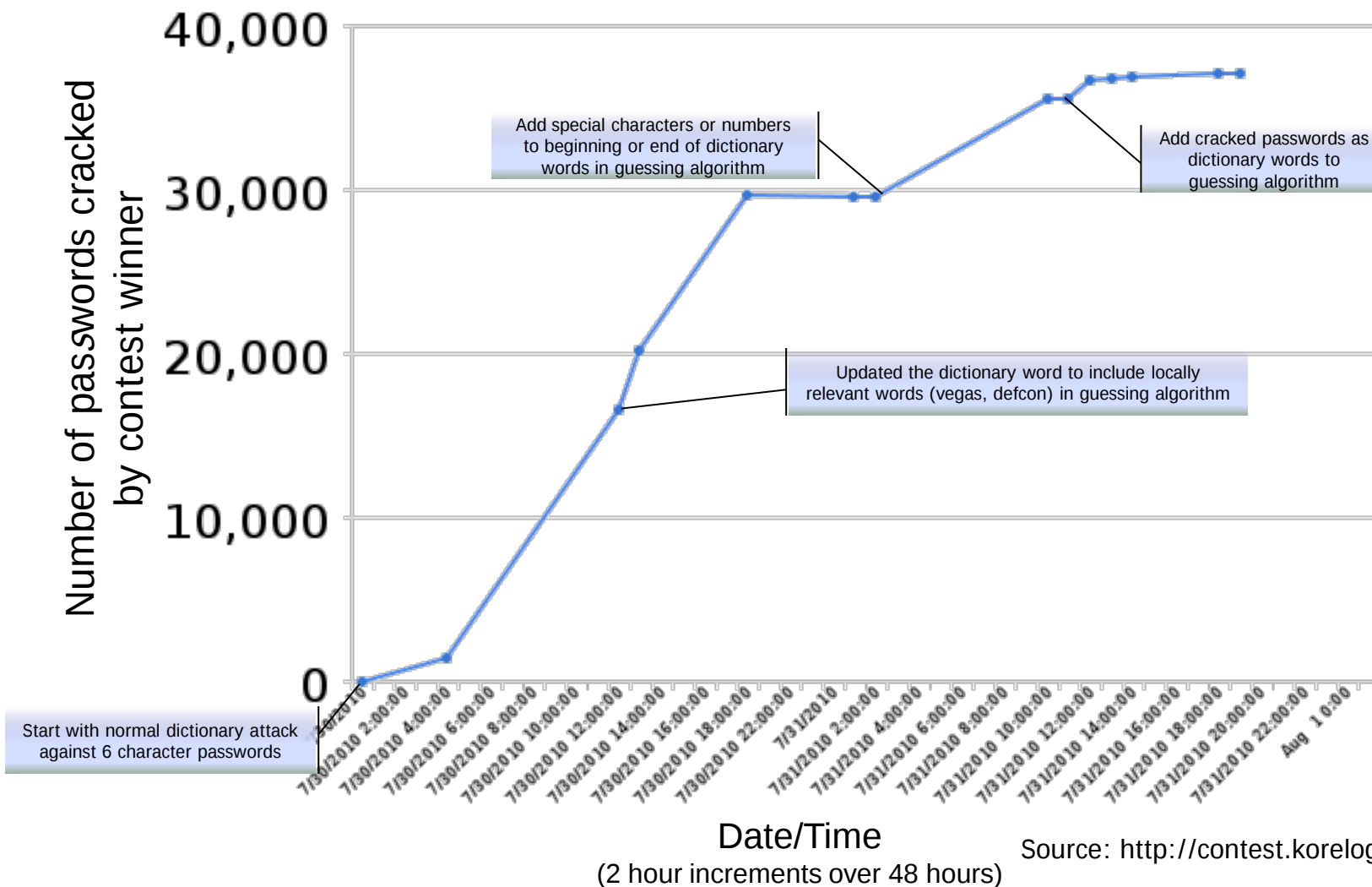
By Jim Finkle
updated 6/28/2011 6:49:26 PM ET

Source: www.msnbc.msn.com



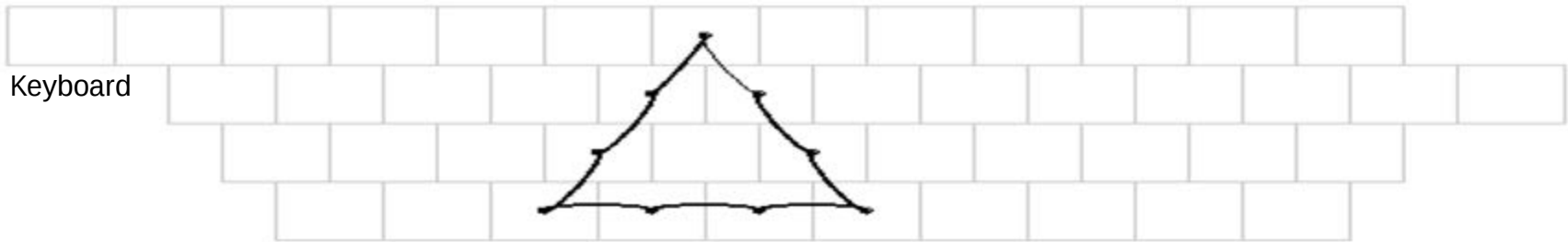
Patterns will always be hackable

Defcon 2010 Contest on Password Hacking of 53,000 passwords

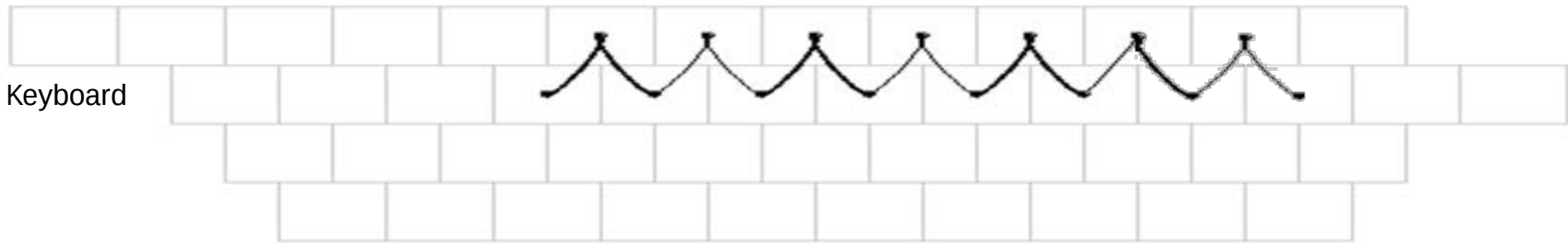




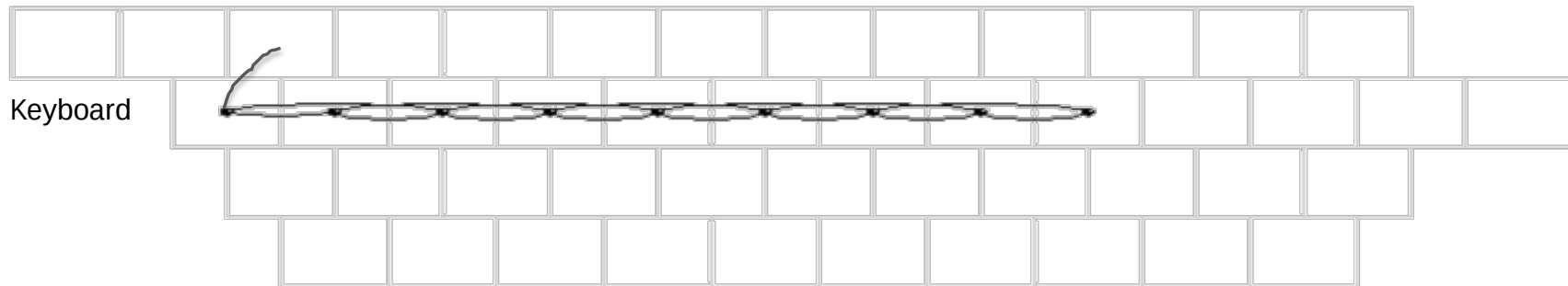
Why will passwords always be a problem?



6tFcVbNh ^ TfCvBn



R%t6Y&u8I(o0P-[



#QWqEwReTrYtUyI

Source: *Visualizing Keyboard Pattern Passwords*, US AF Academy 11 Oct, 2009



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

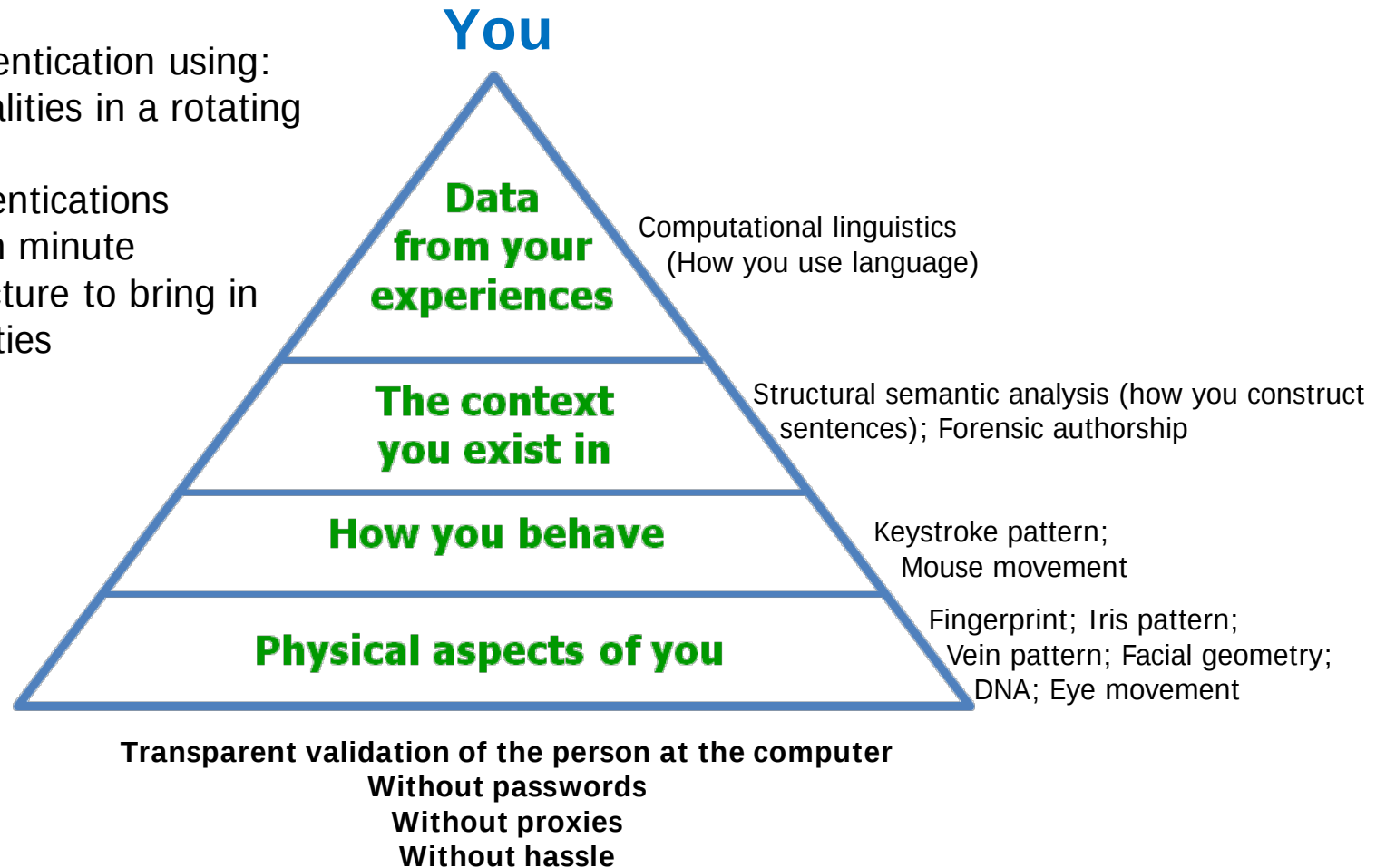


Solution: **Active Authentication**

An open solution that provides **meaningful** and **continual** authentication to DoD's computer systems leveraging that which makes up **you**

Continuous authentication using:

- Multiple modalities in a rotating fashion
- Multiple authentications initiated each minute
- Open architecture to bring in future modalities





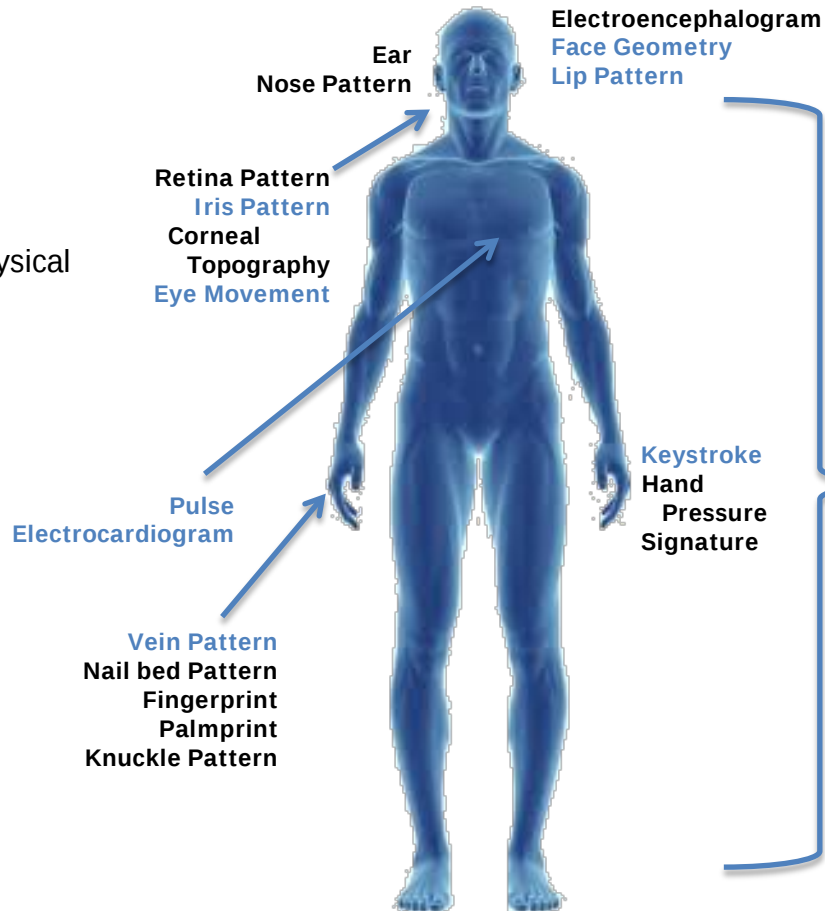
Existing Biometric Modalities

Current Solutions

Physiological Biometrics

Sensors tracking the physical attributes of you

- DNA
- Ear Geometry
- Facial Geometry
- Fingerprint
- Iris Pattern
- Knuckle Pattern
- Lip Pattern
- Nail bed Pattern
- Nose Pattern
- Oto-acoustic Emissions
- Palmprint
- Retina Pattern
- Skin Spectroscopy
- Vein pattern



Behavioral Biometrics

Sensors tracking how you interact with the world

- Eye Movement
- Hand Pressure
- Keystroke pattern
- Signature
- Voice

DNA
Voice
Skin Thermography
Skin Spectroscopy
Odor
Skin Impedance
Muscle Movement

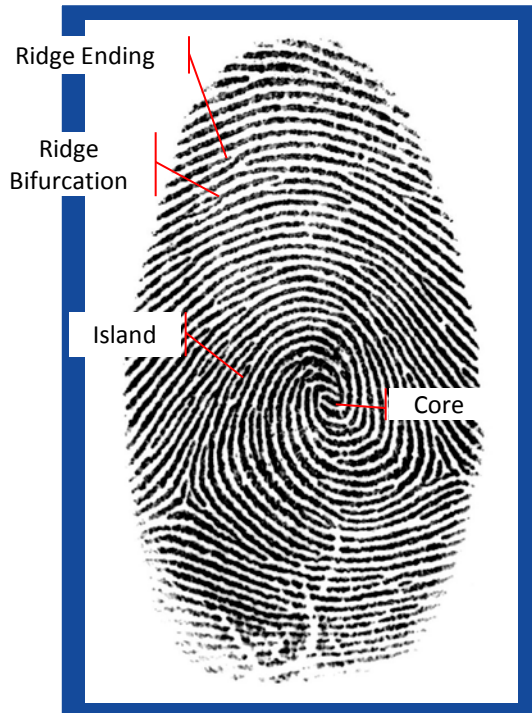
Blue may be suitable for continuous monitoring
Black require interrupting the user



Biometric Identity Modalities

Physical aspects of you

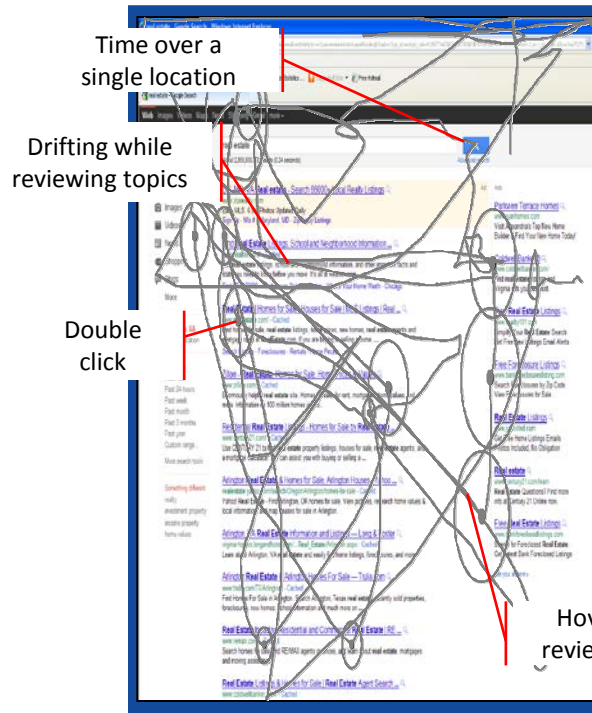
Fingerprint



Source: epdeatonville.org

How you behave

Mouse tracking¹

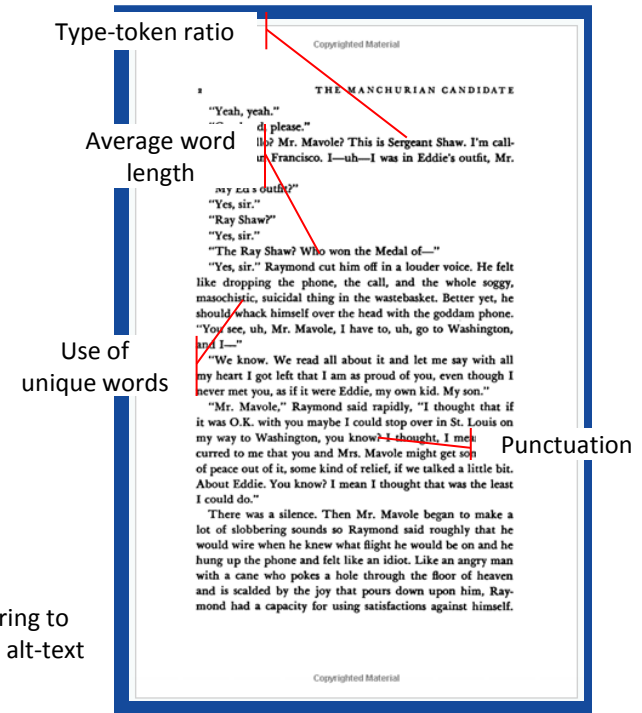


Source: google search for "real estate" with mouse tracking provided by IOGraph

- 1- *What can a mouse cursor tell us more?: correlation of eye/mouse movements on web browsing*, Mon-Chu Chen, John R. Anderson, Myeong-Ho Sohn (all CMU), 31 March 2001

The context you exist in

Forensic authorship²



Source: The Mancurian Candidate, Robert Graves, P2, Amazon Preview

- 2- *Quantifying evidence in forensic authorship analysis*, Dr Tim Grant, Aston University, UK 2007

Existing
Technology

Repurposed
Technology

New
Technology

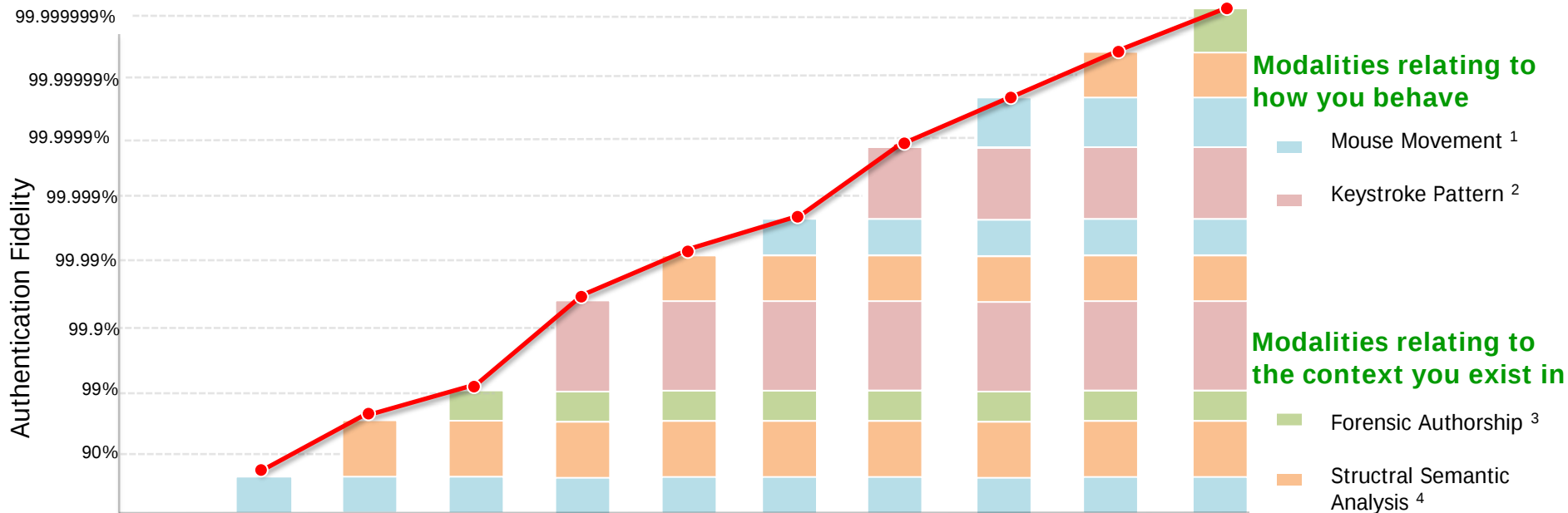


Layering Modalities – how it will work

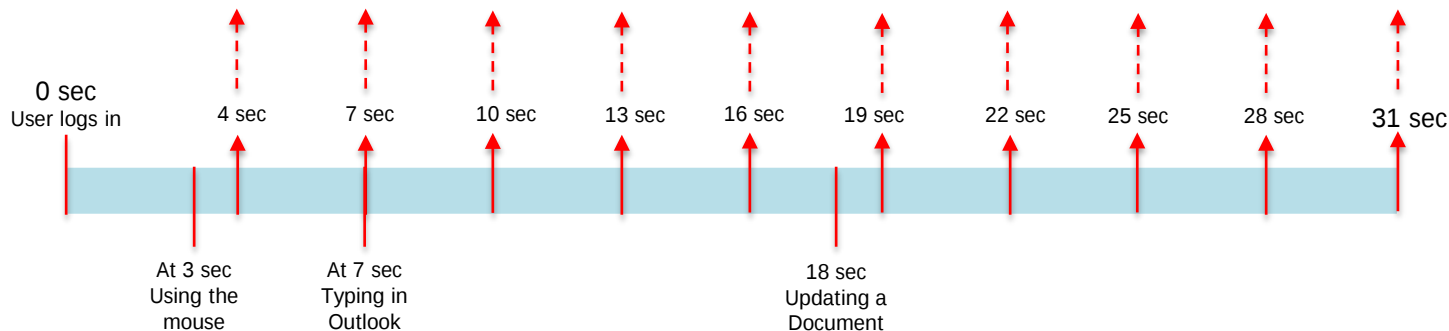
- The Active Authentication Platform replaces the authentication framework within a desktop operating system with a protected framework
 - Ex: winlogon and GINA.DLL for Microsoft Windows
- The user will identify themselves and gain access to the system
- The Active Authentication Platform will then look for user activity, capturing biometric information as it is available
 - Ex:
 - Comparing the mouse when mouse activity occurs
 - Comparing the pattern of typing when the keyboard is used
 - Comparing word usage when documents are created
- As system trust in the identity of the user increases, access to more critical systems is made available
- When system trust is not high enough, the Active Authentication platform initiated a re-check process to validate the identity of the user and takes system admin direction as needed



Active Authentication Scenario



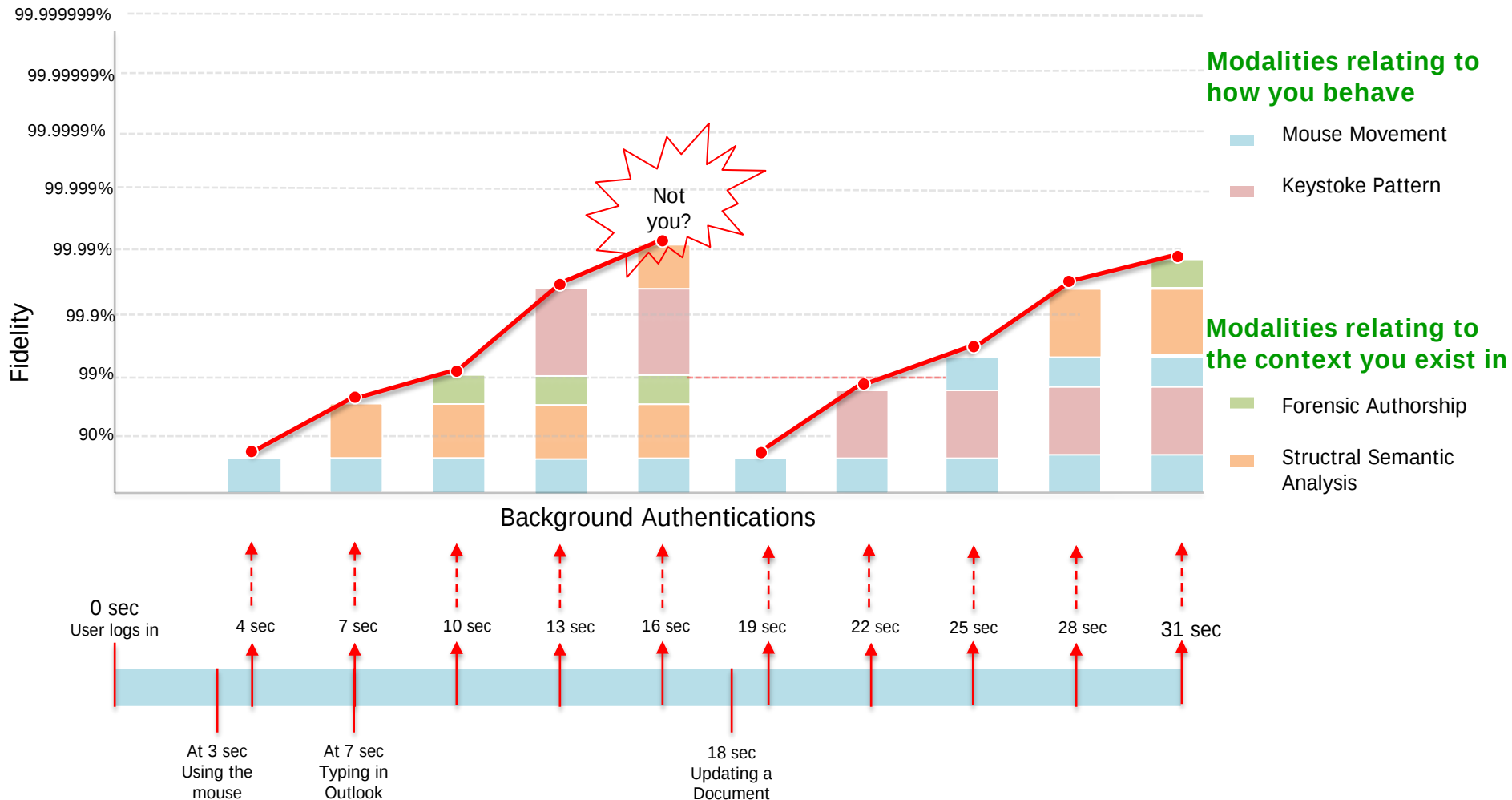
Background Authentications



- 1 - Mouse Movement (Mon-Chu Chen, John R. Anderson, Myeong-Ho Sohn 2001) (73-80% True Positive Rate)
- 2 - Keystroke Pattern (Gunetti et. al., 2005) (94-95% True Positive Rate)
- 3 - Forensic Authorship (Dr Tim Grant, Aston University, UK 2007) (80-93% True Positive Rate)
- 4 - Structural Semantic Analysis (de Vel et. al., 2002) (86-91% True Positive Rate)



Active Authentication Scenario (“not you”)



Automatic system re-test to validate identity to a threshold set by system administrator (example uses 99% over 3 tests)

No user interruption until the system's confidence level is breached (based on local thresholds set)
If it is breached the user is disconnected from all resources (local site chooses actions, logged off or disconnected)



How do we measure success?

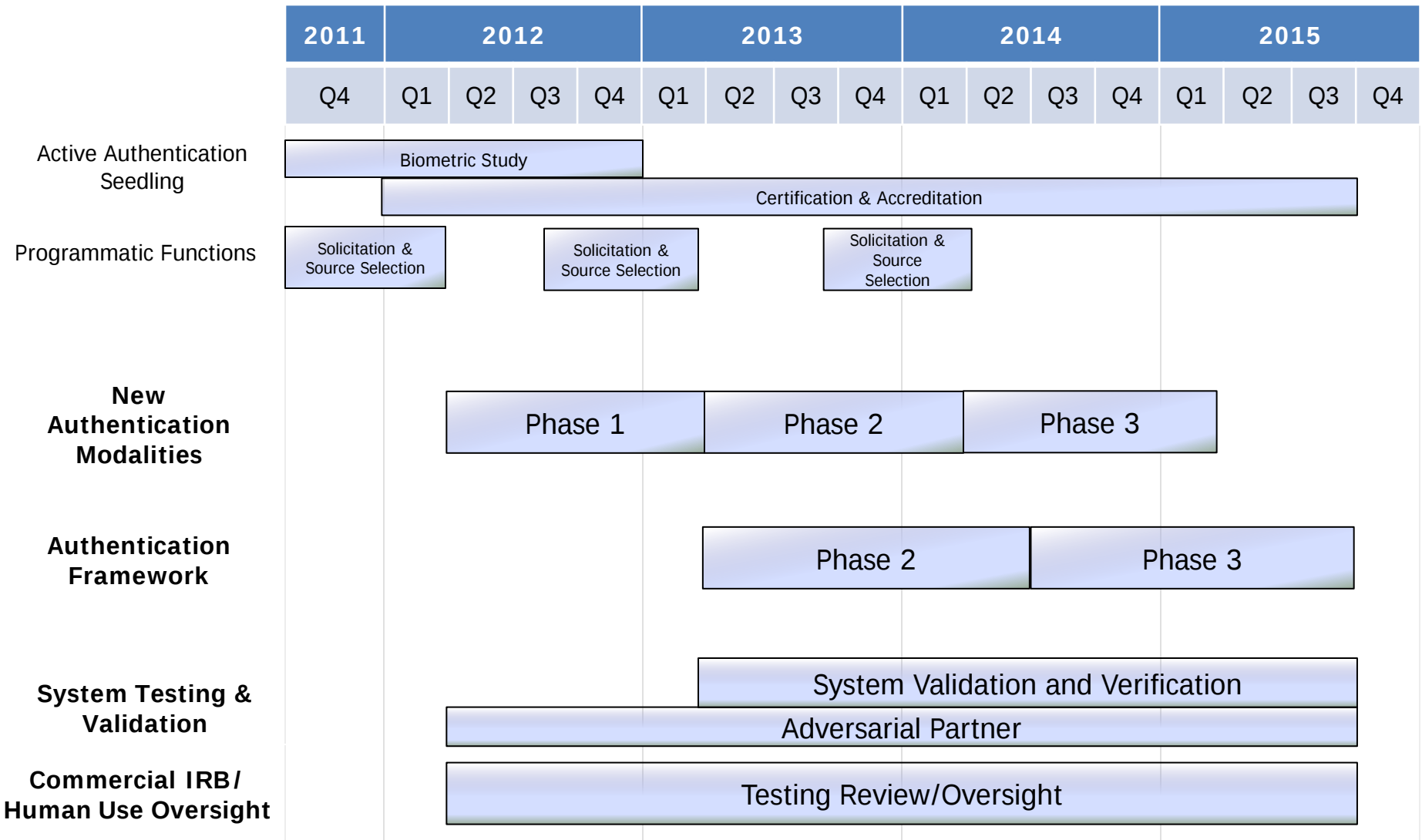
		Phase 1	Phase 2	Phase 3
Introduced new authentication modalities				
	Maximum False Rejections after five (5) scans	1/week	1/month	1/month
	True Positive Rate for each scan	80%	80%	85%
	Usability of modality within the population of DoD personnel	90%	90%	95%

Note: *The Authentication Platform does not start until Year 2, and will be addressed in a later solicitation, below are planned metrics*

			Phase 1	Phase 2
Authentication Platform				
	Able to maintain a minimum True Positive Rate of 99.999% after:		45 sec	30 sec
	Number of integrated modalities		5	10
	Maximum response time to process a single authentication		12 sec	6 sec
	Number of authentications performed per minute (APM)		5	10



Active Authentication Program Plan





Active Authentication Program focus areas

1. Emerging Authentication Modalities:

New methods for verifying a user's identity focusing on software biometrics in an office automation environment

2. Multifactor Authentication Integration:

Integration of the multiple modalities into a single platform for authentication developed in an open architecture to allow introduction of new solutions

***Note:** The multifactor authentication integration focus area does not start until Year 2, and will be addressed in a later solicitation*

3. System Testing & Validation:

Both Independent Verification & Validation of the developed code and active Red Team analysis of the solution to ensure the solutions developed do not increase the current available attack surface



Phase 1 Activities

- The Solicitation is expected to come out in late November/Early December
- The Solicitation is currently expected to be open for 60 business days
- Multiple awards are expected for Technical Area #1
- Technical Area 2 will not be included in the Solicitation for Phase 1
- Multiple awards are not expected Technical Area #3



Technical Area #1

Emerging Authentication Modalities

- New biometric modality studies on software based biometrics that can capture aspects of the “cognitive fingerprint” that will be able to quantitatively their findings with human testing
- Expected to range from 3-6 months in length, but will all complete the end of Phase 1 (Q1 2013)
- Expected cost no more than \$500K per study
- There will be a heavy focus on providing quantitative analysis of the new solutions through testing
- Quantitative analysis will be required for performers in Phase 2



Technical Area #3

System Testing & Validation

- Provide Red Teaming or “Adversarial Partner” Subject Matter Expertise for length of Active Authentication program
- Provide realistic picture of risk introduced with the new modality approaches
- The Level of Effort for this technical area is expected to be low for Phase 1, with a significant increase in Phase 2 and 3
- Both Independent Verification & Validation of the developed code and active Red Team analysis of the solution to ensure the solutions developed do not increase the current available attack surface
- IV&V functions do not start until Phase 2



Potential Future Applications

Tactical Uses



Military personnel in Mission Oriented Protective Posture (MOPP) level 4 have to endure passwords while wearing 2 pairs of gloves



Command and Control



Right before picking up the "Red Phone" is not the time you want to verify your system access!

Medical Safety



Because of time constraints, medical personnel currently have no active verification of proficiency training or authorization

Physical Security



How many times have you forgotten your badge?

Mobile and Commercial



Anywhere passwords are currently being used could be converted to active authentication via biometrics



www.darpa.mil