Biometrics: Big Data, Analytics, & Biometric-Enabled Intelligence — For Defense, Intelligence, Homeland Security and Law Enforcement —

This Conference brought to you by:

www.ttcus.com

LinkedIn/Groups: Technology Training Corporation

@Techtrain
DARPA’s Active Authentication

Mr. Richard Guidorizzi
Program Manager
DARPA, I2O

Moving Beyond Passwords

Program Overview Briefing

Dec 12, 2013

Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)
Users are the weak link...

Finweb = Jane123
DTS = 123Jane
PKI = JaneA123
DiskCrypt = Jane123A
Gmail = Jane123A
The Active Authentication Program

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

- **You**
  - Untapped Range of Behavioral Biometrics
  - Data from your experiences
    - Computational linguistics (How you use language)
  - The context you exist in
    - Structural semantic analysis (how you construct sentences); Forensic authorship
  - How you behave
    - Keystroke pattern; Mouse movement
  - Physical aspects of you
    - Fingerprint; Iris pattern; Vein pattern; Facial geometry; DNA; Eye movement

Non-cooperative behavioral biometrics allow the validation of identity simply by the user acting normally, not requiring interruption of the user.
The Active Authentication Program Plan

- **Iowa State**: Stylometry focused on thought processing time
- **Drexel**: Stylometry augmented by author classification and verification
- **NY IT**: Stylometry how a user types - ignoring the words
- **NPS**: Behavioral manifestations of human thought processes
- **BehavioSec**: Keystroke, mouse, in context
- **NRL**: Identification of users through Web browsing behavior
- **UMD**: Information processing from computer screens
- **Coveros**: User Behavior Patterns as seen from the Operating System
- **Allure Security**: User search behavior characteristics
- **SWRI**: Use covert games disguised as computer anomalies

AA Application
Validates Level of trust in Identity

Claimed identity

Biometric Data
Validated access

12/18/2013

Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)
What are the performers working on

### Phase 1 Results

<table>
<thead>
<tr>
<th>Performer</th>
<th>TP</th>
<th>FAR</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allure Security</td>
<td>95.0%</td>
<td>1.0%</td>
<td>5m</td>
</tr>
<tr>
<td>Iowa State U (KRR)</td>
<td>92.7%</td>
<td>5.5%</td>
<td>29sec</td>
</tr>
<tr>
<td>NYIT</td>
<td>92.0%</td>
<td>4.0%</td>
<td>1min</td>
</tr>
<tr>
<td>Drexel U</td>
<td>92.0%</td>
<td>5.0%</td>
<td>50sec</td>
</tr>
<tr>
<td>University of MD</td>
<td>82.8%</td>
<td>20.0%</td>
<td>83sec</td>
</tr>
<tr>
<td>NRL</td>
<td>82.0%</td>
<td>6.0%</td>
<td>4hrs</td>
</tr>
<tr>
<td>Coveros</td>
<td>80.0%</td>
<td>10.0%</td>
<td>30sec</td>
</tr>
<tr>
<td>SWRI</td>
<td>75.0%</td>
<td>25.0%</td>
<td>8min</td>
</tr>
<tr>
<td>Alenka Brown</td>
<td>10.1%</td>
<td>10.0%</td>
<td>1min</td>
</tr>
</tbody>
</table>

TP = True Positive Rate
FAR = False Accept Rate
Time = time before decision

---

TPR FAR Time

- **How you think**
  - Look for information
  - Interactions with applications
  - Word choice/use
  - Time to think when writing

- **How you use your device**
  - How you move your phone when using it
  - How you compose language (written and spoken)
  - How device is used
  - How you swipe/type

- **Physical aspects of you visible to the device**
  - Passive Fingerprint Detection
  - Passive Facial Recognition
  - Passive Heartbeat Detection

---

12/18/2013

Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)
Active Authentication Performers (five examples)
**Phase 1 Summary**

**Neuro-cognitive patterns - Naval Post Graduate 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.
PERFORMER OVERVIEW AND STATUS

**BIOMETRIC:** User search behavior characteristics, how a user searches their own files and directories for information they seek. Decoy files are used to detect adversarial information gathering activities.

**Key Objectives**
- Establish statistics-based biometrics for user search behavior modeling
  - Capture host features related to: file, window, process, and network manipulation.
  - Develop learning statistical model the evolves over time and tracks change in user behavior.
  - Quantify the characteristics of unique user behavior as a measurement of these features and design new statistical models that encapsulate these measurements.
  - Develop metrics for behavioral models that measure the similarity between one model and another, including metrics for measuring behavior change and behavioral variability of the same user.
- **Decoy document** implants for intrusion trip-wiring, and data leakage tracking:
  - Automatically generated, based on previously studied measurements of standard user documents.
  - Automatically implanted in user’s file system
  - Decoys are believable, enticing, non-interfering, stealthy
  - Abnormal user behavior and unusual decoy touches indicates a masquerader with very high accuracy

**Status**
- Host sensor for monitoring user behavior and implanting decoy files completed and deployed in an ongoing user study.
- Completed detailed analysis of a prior user study, that generated a dataset, RUU, and identified superior audit features for accurate user modeling.

**Team Members**

**Principal Investigator:** Salvatore J Stolfo, Allure Security, New York, NY
- Malek Ben Salem (Co-PI), Accenture, Arlington, VA
- Yingbo Song (Researcher), Allure Security, New York, NY
- Shlomo Hershkop (Researcher), Allure Security, New York, NY

© Allure Security in association with Accenture

User Search Behavior Biometric
For Active Authentication

User Commands

Authenticating User
Learning User Search Behavior
User Actions

Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)
PERFORMER OVERVIEW AND STATUS

BIOMETRIC: Keystroke and mouse dynamics in the context of each other and application use.

- Behavioral biometrical features that is considered in the approach.
- Keystroke patterns are collected by the way users type at the keyboard.
- Mouse dynamics which are acquired by analyzing the inputs a user performs by a pointing device.
- Both keystrokes and mouse usage are tied to what application that is currently in use.
- Application usage - the time an application opened, when it was closed what applications are open in parallel, how they are opened and closed, number of open views, memory consumption, CPU consumption etc.

Key Objectives

- Reports
  - Common metrics for continuous authentication
  - Common data format
  - Application behaviometrics
  - Continuous trust
- Current work
  - Run simulations: 1:1 (against self) 1:n (simulated ‘passive attacks’ against others using their natural behavior) to calculate the performance.

Status

- All Reports completed and filed.
- Initial (using subset) analysis of passive attackers completed with positive results. Keyboard detection in less than 6 keystrokes, mouse under 3 minutes for ‘passive attacker’
- Final analysis of large data set underway with presentation expected at RSA security show in June & BCC in September

Team Members

Principal Investigator: Dr Neil Costigan, Sweden
- Peder Nordstrom (Engineering)
- Tony Libell (Engineering)
- Johan Lindholm (Engineering)
- Linus Nilsson (Engineering)
- Ingo Deutschmann (Engineering)
- Olov Renberg (Program manager)
PERFORMER OVERVIEW AND STATUS

**BIOMETRIC:** User behavior as seen from the perspective of the operating system - analyzes system calls/event sequences to identify anomalous computer behavior that may be caused by unauthorized access.

- Analyze system call/event sequences to identify anomalous computer behavior that may be caused by unauthorized access.
- Use learning algorithms to distinguish normal and abnormal user behavior based upon these sequences.
- Examine mechanisms for combining learning algorithm results to reduce false accepts and false rejects within the system.

**Key Objectives**

- Determine the most effective system call based anomaly detection mechanism through empirical analysis.
- Incorporate time and other characteristics of system calls into our algorithm to reduce false rejects and false accepts.
- Prototype our approach to demonstrate feasibility and field test on real users.

**Status**

- Combining sensors have resulted in overall false reject and false accept rates below 10% across all learning algorithm thresholds with rates approaching 3-5% for particular threshold values.
- Prototype developed and deployed internally for alpha testing, external fielding testing to be performed in late April 2013.

**Team Members**

**Principal Investigator:** Mr. Jeffery Payne, Fairfax, VA

- Dr. Mark Fenner, Research Scientist
- Mr. Jonathan Kauffman, Research Associate
- Mr. Max Saperstone, Senior Consultant

Images © Microsoft ClipArt

© Coveros, Inc.
PERFORMER OVERVIEW AND STATUS

**BIOMETRIC:** Stylometry (how people use language when they write) augmented by author classification and verification.

**Key Objectives**

- **Adapt stylometric techniques** for the authentication problem to validate the identity of writers by analyzing the style of their writing.
- Integrate this technology with other known techniques in order to identify the context and circumstances under which this technology would be most useful.
- Gather a large data set of text produced by routine computer use for development and testing of the modality.
- Integrate known Human-Computer Interaction (HCI) modalities with a fusion algorithm and test.
- Harden our approach against active adversaries that might circumvent it or spoof users. (In progress)
- Investigated authorship attribution using higher level linguistic sensors based on Myers-Briggs Personality Type, Handedness, and Gender. These sensors use character bigrams and common words for features, and centroid-based 1-nearest-neighbor leave-one-out validation for classification.

**Status**

- New techniques developed and adapted for High Level Modalities
  - Results show: Dominant Hand-99.2%, Judging/Perception-80.1%, Extrovert/Introvert-78.4%, Gender-76.6%, Thinking/Feeling-76.5%, Sensing/Intuition-73.0%
- Fusion algorithm developed. Preliminary analysis suggests using the fusion system to look at how other modalities can address weaknesses in any specific modality.
  - Performance - FAR: < 10%, FRR: < 5%; Timing - Time to make first decision: < 1 minute, Decision Rate: 1.72 per second
- Adversarial approach developed
  - adversarial algorithm to detect stylometric attacks rejects 85% of imitation attacks
- Integration work remains

---

**Team Members**

**Principal Investigator:** Rachel Greenstadt, Philadelphia, PA
- Moshe Kam, Drexel University Philadelphia, PA (Co-PI)
- Drexel Students: Ariel Stolerman, Alex Fridman, Sayandeep Acharya
- Juola and Associates: Patrick Juola, Patrick Brennan, John Noecker, Michael Ryan

© Drexel University in association with Juola & Associates
PERFORMER OVERVIEW AND STATUS

**Biometric**: Stylometry, focused on how thought processing impacts keystroke dynamics. Users changes in typing rhythms induced by cognitive factors, especially when it is manifested as natural pauses in typing.

**Key objectives**

Developing a biometrics-based authentication system with four modules:

- **Sensor module**: acquires the biometric data from a user via a web-based tool
- **Feature extraction module**: processes the acquired biometric data and extracts a feature set to represent it (with cognitive fingerprints)
- **Matching module**: compares the features with the stored profiles using a classifier to generate matching scores
- **Decision module**: uses the matching scores (from multiple classifiers) to verify a user’s identity (authentication)

**Status**

- Large scale experiment at ISU (Nov. ~ Dec. 2012): Email invitations to 36,000 candidates (faculty, staff and students). 1,977 participants finished two 30-minute segments (900 words each). 983 participants (out of 1977) finished additional 33-minute segment (1,200 words)
- Two off-line verification systems are developed: Different in basic machine learning technique; SVM (off-the-shelf library) and KRR (in house developed tool); Similar in: feature selection, classifiers, cross-validation techniques, and fusion method
- **Experiment Results**
  - 983 individual profiles (trained files) were built, each tested by 1,977 users (900 words each user)
  - SVM-based (FAR 5.5%, FRR 0.7%, training time 15m/user, testing time 0.6s/user, size of trained file 20MB/user)
  - KRR-based (FAR 5.5%, FRR 1.77%, training time 29s/user, testing time 3.5ms/user, size of trained file 1MB/user)
- A prototype system was demonstrated at PI meeting on April 8, 2013

**Team Members**

**Principal Investigator**: Jien Morris Chang, Iowa State University
- Chris Chu, Ahmed Kamal, Stephen Gilbert, Iowa State University
- Sun-Yuan Kung, Princeton University
Identification through behavioral manifestations human thought processes. Focuses on identifying signal characteristics from individual neuropsychometric indicators (NPI) (e.g. voice features, ocular movements, heart rate, gait, speech patterns, etc.).

• Using an expert systems development approach, produce proof-of-concept for constructing an automated neuro-cognitive classification system that can be used in building an active authentication tool for continuously recognizing individual users via their unique cognitive fingerprints.

• Effort involves matching signal characteristics from individual neuro psychometric indicators (NPI) (e.g. voice features, ocular movements, heart rate, gait, speech patterns, etc.) to human test subject neuro-cognitive modalities identified by the SME.

Key Objectives

• Develop a methodology for translating SME’s psychometric classification process into an automated system for simultaneously using multiple NPIs to continuously authenticate system users.

  ✓ Work focused on extracting voice signal features (tone, tempo, frequency, intensity) from test subject samples and determining signal ranges for each of 3 primary neuro-cognitive modalities (Visual, Auditory, and Kinesthetic) identified by the SME.

Status

✓ Results were inconclusive due to limited availability of test subject data. (Completed in Fall 2012. )

✓ Additional research required to expand the voice signal sample set and provide a statistically relevant proof-of-concept level determination of methodology viability.

Team Members

Principal Investigator: Dr. James Scrofani, PI for NPS
  • Dr. Alenka Brown, SME/PI for ORNL
  • Col Ronald Dodge, PI for USMA
PERFORMER OVERVIEW AND STATUS

**BIOMETRIC:** Identification of users through Web browsing behavior. Develop the theoretical foundations and supporting algorithms for the detection, tracking and prediction of Web browsing behavior using information available from the address line of the browser.

- The biometric is the activity patterns that can be captured in the browser including the timing of clicks, the nature of pages visited, the length of a session, the revisit rate, etc.

**Key Objectives**

- Identify, extract and analyze features of Web behavior collected in a user study.
- Investigate structured prediction methods to authenticate users based on their Web browsing behavior and analyze a large clickstream dataset obtained from comScore.
- Develop a genre palette to categorize webpages for authentication and identification purposes.

**Status**

- Browser extensions for tracking and monitoring user Web behavior completed and deployed in an ongoing user study.
- Completed detailed analysis of initial user study dataset and identified key features of Web browsing behavior.
- Completed initial authentication approach using ensemble of one-class SVMs and random subspace method with best FRR: 18%; and best FAR: 7%.

**Team Members**

**Principal Investigator:** Myriam Abramson, Code 5584
- David W. Aha, Code 5514
- Steve Russell, Code 5584
PERFORMER OVERVIEW AND STATUS

**BIOMETRIC:** Stylometry, focused on capturing information on how a user types, harnessing a combination of cognitive rhythms making it language independent.

Cognitive rhythms of a user constitute:

- **Pausality** behaviors - pause time before the beginning of a new sentence, pause time followed by a text revision, and pause duration between two discourse markers
- **Text revision** behaviors - number of revisions in sentence of length \(L\) characters
- **Linguistic** behaviors - number of verbs in a paragraph containing \(N\) words and number of function words
- **Keystroke** dynamics - key hold and interval latencies

The behaviors are captured when the user plans, composes, types, and revises text on a desktop computer.

**Key Objectives** *(User Population of 480 Users)*

- Find the baseline equal error rate of keystroke features under fusion-based continuous authentication model
- Find the equal error rate of continuous user authentication with cognitive rhythm features under fusion-based authentication model
- Find false reject and impostor pass rate confidence intervals achieved with cognitive rhythms at 95 percent significance level under, a) zero-effort impostor attempts and b) algorithmic forgery attempts.

**Status**

- Achieved 2.9 percent equal error rate with atomic- and sentence-level cognitive rhythms.
- Results on algorithmic forgery attacks with atomic cognitive rhythms published in IEEE Transactions in Information Forensics and Security journal.
- Ongoing work on evaluating paragraph-level cognitive rhythms, privacy-preserving continuous authentication, and adversarial template update.

---

**Team Members**

**Principal Investigator:** Kiran S. Balagani, Old Westbury, New York

- Vir V. Phoha, Co-PI, Louisiana Tech University
- Andrew Rosenberg, Co-PI, Queens College, The City University of New York
- NYIT students: Patrick Koch, Sathya Govindarajan, and Ming Xu
- LTU students: Zibo Wang, Abdul Serwadda, and Shafaeat Hossain
- CUNY students: Adam Goodkind and David Guy Brizan
**PERFORMER OVERVIEW AND STATUS**

**BIOMETRIC:** Uses covert games disguised as computer anomalies to verify unique user features through the user’s responses to changes in the GUI (the covert games).

**Key Objectives**

- Applies game theory principles by allowing users to develop unique strategy paths for playing the imperceptible games disguised as Windows alert messages.
- Game applies a matrix based on Prisoner’s Dilemma (studied in classic game theory).
- Users’ response to the window prompts computer’s next move.
- Ending game allows users to return to their primary task.

**Status**

- Completed testing and evaluation with 95 participants:
  - Game remained covert to all.
  - Some users persevere by responding only one way, regardless of effect on productivity.
  - Using mechanisms for forcing dynamic behavior from perseverators (i.e., different type of game window).
  - Many users unconsciously develop an individual strategy.
- Unique game response paths and styles (cognitive fingerprints) have emerged as invariant user attributes.
- Final evaluation with 40 participants yielded following results:
  - Covert game theory-of-mind model to classify unique response styles.
  - Receiver Operating Characteristic (ROC) accuracy of 0.888, hit rate up to 0.875, and false alarm rate of 0.36 while maintaining a 0.83 hit rate under particular criterion values.

**Team Members**

**Principal Investigator:** Jenifer Wheeler
- Denise Varner, Technical Lead
- Sentier Strategic Resources, Austin, TX

© Southwest Research Institute
PERFORMER OVERVIEW AND STATUS

**BIOMETRIC:** Uses how an individual processes information on their computer screen - focuses only on how the information is displayed on the screen. Leverages computer vision algorithms to find spatio-temporal screen fingerprint.

- The proposed technology exploits the synergy between recent advances in pixel-level screen analysis and vision-based biometrics
- Pioneer attempt to combine vision-based biometrics and pixel-level screen analysis in a complementary manner for the purpose of active authentication

**Key Objectives**
- Extract textural and motion features from the screen fingerprint for authentication
  - Taking a screen recording of the computer being used by the operator and by extracting discriminative visual features from this recording
  - Qualities captured in screen-fingerprints include cognitive abilities, motor limitations, subjective preferences, and work patterns
- Characterize the discriminative power present in the screen fingerprint for detecting an intruder from an authorized user.
- Design rules for detecting anomalies in screen fingerprints that may correspond to access by an unauthorized user.
- Design dimensionality reduction methods and classifiers for user authentication.

**Status**
- Collected datasets under different scenarios (browsing a document, resizing a document, typing, dragging the cursor, etc)
  - Initial results show that screen fingerprints contain discriminative information to authenticate users
  - More experiments with different features and classifiers are being conducted and validated using different metrics such as Receiver Operating Characteristics (ROC), Cumulative match Curve (CMC) and confusion matrix

**Team Members**

**Principal Investigator:** Prof. Rama Chellappa
- Prof. Larry Davis (Co-PI)
- Prof. Tom Yeh (Co-PI)
- Dr. Vishal M. Patel (Co-PI)
- Mohammed E. Salem (RA)
- Yangmuzi Zhang (RA)
Overview of Phase 2 Funded Projects
What are we working on in the Active Authentication Program?

Solutions using desktops

<table>
<thead>
<tr>
<th><strong>User Search Patterns</strong> - Allure Security Technology, Inc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using the user’s patterns of application use and searching for information on the computer, verified by decoys placed on the file system to detect masqueraders.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Stylometry focused on Cognitive Processing Time</strong> - Iowa State University</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using stylometric methods to validate the user based on natural pauses in the way they type.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Stylometry focused on keystroke dynamics, cogni-linguistic features, and demographic classification</strong> - Louisiana Tech University</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop a collection of keystroke-based algorithms that analyze free-text input to capture unique aspects of -- how a user types, how the user composes text and uses language, and the demographic classifications to which the user belongs.</td>
</tr>
</tbody>
</table>
What are we working on in the Active Authentication Program?

<table>
<thead>
<tr>
<th>Solutions using mobile devices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Search Patterns - Allure Security Technology, Inc</strong></td>
</tr>
<tr>
<td>Using the user’s patterns of application use and searching for information on the computer, verified by decoys placed on Android devices, and incorporating additional modalities, (eg. voice, image) to detect masqueraders.</td>
</tr>
<tr>
<td><strong>Fast Pattern Recognition Applied to Kinematic Gestures and Finger Images authentication - AMI Research</strong></td>
</tr>
<tr>
<td>Utilize Fast Pattern Recognition (FPR) and online signature recognition algorithms to process touchscreen gestures and finger images (including partial images) captured in the normal process of use of the mobile device.</td>
</tr>
<tr>
<td><strong>Mobile perpetual authentication - BAE Systems</strong></td>
</tr>
<tr>
<td>The Active Authentication on-the-Go program will compute robust gait biometrics using motion data collected by inertial sensors embedded in a mobile device for continuous identity validation whenever the user is on the move.</td>
</tr>
<tr>
<td><strong>Type and swipe authentication - BehavioSec</strong></td>
</tr>
<tr>
<td>Using the user’s touches, gestures, and finger pressure with input from the accelerometer, GPS positioning, application data, and timing of events.</td>
</tr>
<tr>
<td><strong>Stylometry integrated with eye tracking - Drexel University</strong></td>
</tr>
<tr>
<td>Make use of stylometric methods to validate a user based on what they are typing, but driving the focus beyond current research to microtext, also using eye tracking for additional classification.</td>
</tr>
<tr>
<td><strong>Gestures and use of virtual keyboards - Iowa State University</strong></td>
</tr>
<tr>
<td>Study of touch gestures including the timing between the end of each scrolling and the beginning of next action; and the use of virtual keyboard including the typing error patterns and typing pressure and area of typing each virtual key.</td>
</tr>
<tr>
<td><strong>Heartbeat - JPL</strong></td>
</tr>
<tr>
<td>Authentication of mobile device users by microwave detection of heartbeats using signals emitted from the mobile device.</td>
</tr>
<tr>
<td><strong>Power, touch, and movement authentication - Kryptowire</strong></td>
</tr>
<tr>
<td>Assess the capabilities of individual biometric modalities namely power, gyroscope, and touchscreen for multi-user mobile use case scenarios.</td>
</tr>
</tbody>
</table>

Distribution Statement “A” (Approved for Public Release, Distribution Unlimited)
<table>
<thead>
<tr>
<th>Method Description</th>
<th>Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>What are we working on in the Active Authentication Program?</td>
<td>DARPA</td>
</tr>
<tr>
<td><strong>Human voice authentication</strong> – Li Creative Tech</td>
<td>Make use of human voice for authentication using text dependent verification for point authentication and text independent verification for continuous authentication.</td>
</tr>
<tr>
<td><strong>Context aware kinetic authentication</strong> – Louisiana Tech</td>
<td>Integrates information extracted from users’ body movements, typing patterns, and touch gestures, to actively authenticate mobile phone users.</td>
</tr>
<tr>
<td><strong>Covert Games</strong> – Southwest Research Institute</td>
<td>Determine the user’s pattern of behavior by introducing patterned system aberrations that the user intuitively learns based on game theory principles, i.e. hidden games in the mobile device’s interface.</td>
</tr>
<tr>
<td><strong>Motion</strong> – SRI International</td>
<td>Developing a Joint Physiological and Behavioral (JPB) authentication mechanism by extracting and matching fine-grained anthropometric and behavioral signatures from the motion induced on the mobile device via accelerometers, gyroscopes, magnetometers, and proximity sensors.</td>
</tr>
<tr>
<td><strong>Visual fingerprint</strong> – University of Maryland</td>
<td>“Visual fingerprint” through visual images of the operator acquired through three visual streams including the front camera, the back camera, and the screen recorder respectively.</td>
</tr>
<tr>
<td><strong>Hand movement</strong> – New York Institute of Technology</td>
<td>Spatial-temporal hand micro-movements and oscillations (hand movement, device orientation, and grasping patterns) during two modes of user interaction with the touch screen: (1) touch-burst and (2) cognitive-pause.</td>
</tr>
<tr>
<td><strong>Human voice</strong> – SRI International</td>
<td>Continuous authentication through natural speech and language activity performed by the user (spoken and written inputs) on mobile devices.</td>
</tr>
</tbody>
</table>