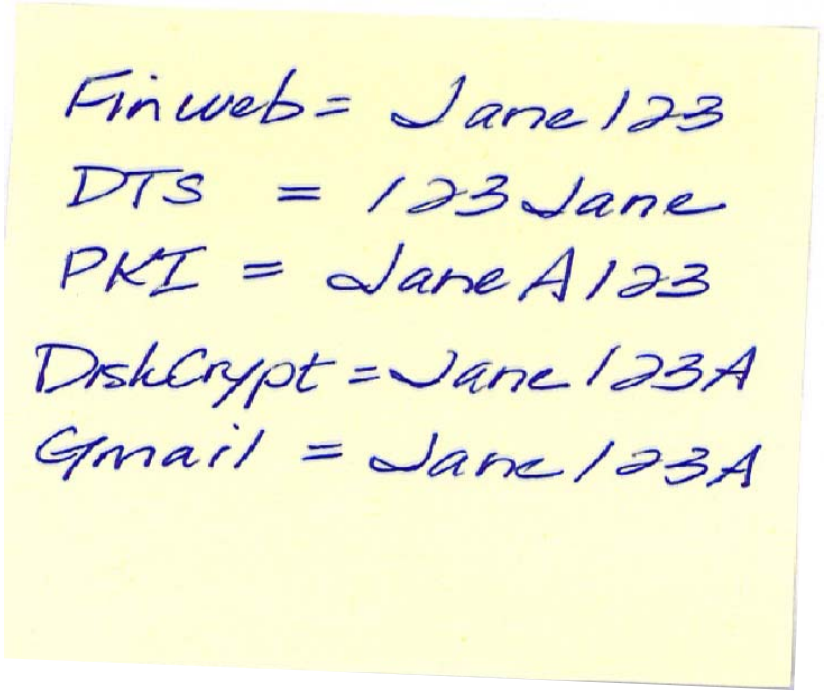
Active Authentication
Moving Beyond Passwords

Richard Guidorizzi, I2O Program Manager (Cyber)

SECOND ROUND TABLE:
From Biometric To Augmented Human Recognition
10 May 2012

Users are the weak link...



How many passwords do we really use?

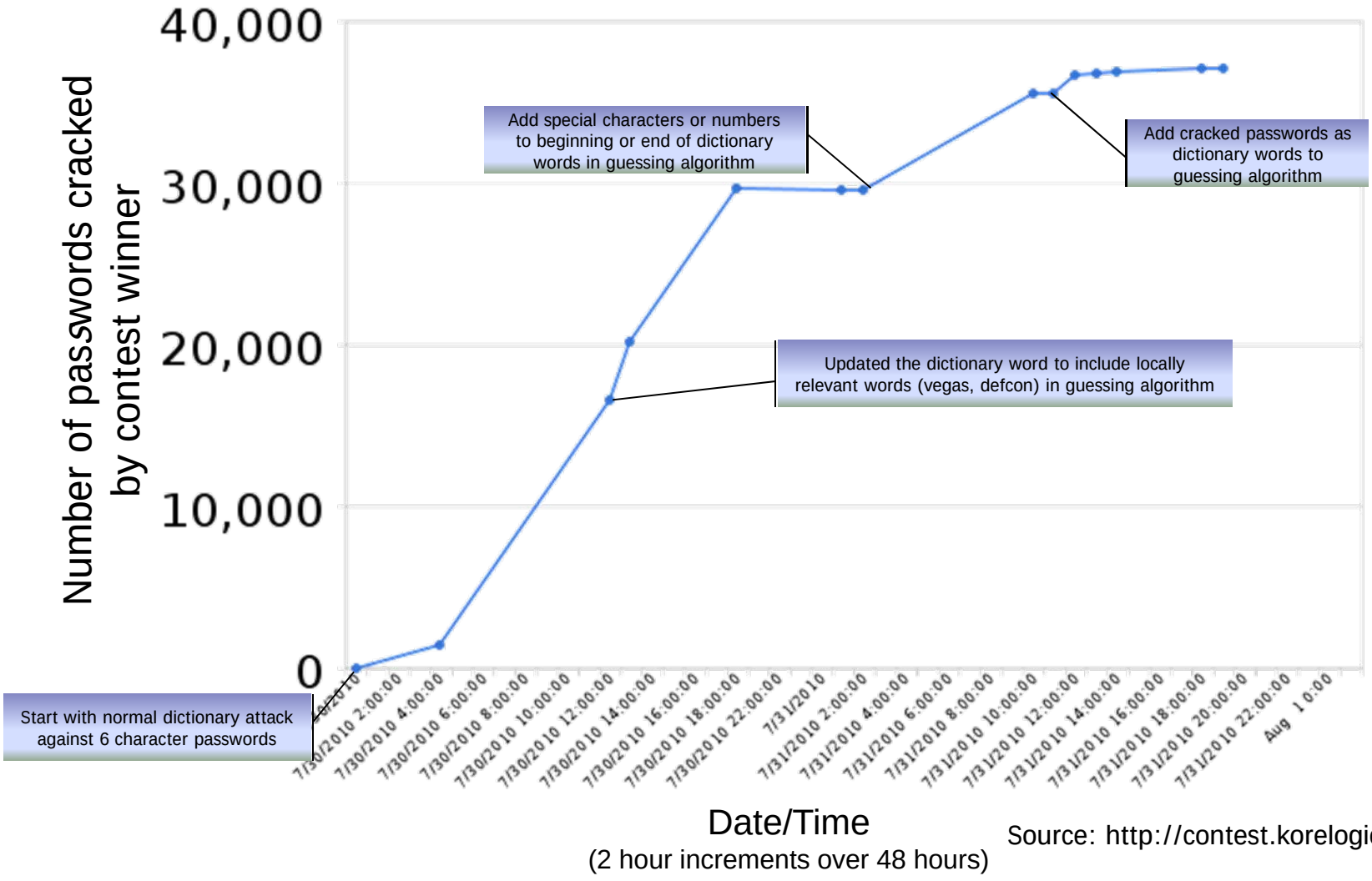
DoD IT Asset Type	DARPA Reference System
DARPA Unclass network	Windows DMSS
Laptop Encryption	Guardian Edge
DARPA VPN	Nortel
PDA	Blackberry/iPhone
DARPA Secret network	Windows DSN
DARPA TS network	Windows DJN
Source Selection	TFIMs, I2O BAA Tool
Contract Management	GSA Advantage, SPS
Contract Invoicing	Wide Area Workflow
Payroll	MyPay
Benefits	Benefeds.com
HR	hr.dla.mil
Training	DAU
Collaboration	Defense Connect Online
Financial System, Local	Momentum
Financial System, Agency	DFAS
Credit Union	PFCU, NCU, etc.

Non-DoD IT Asset Type	Hacked on	Credentials lost
American Honda Motor Co.	27-Dec-10	4.9m
Bank of America	25-May-11	1.2m
Carnegie Mellon University	8-Oct-07	19k
Citigroup	27-Jul-10	30m
Clarkson University	10-Sep-08	245
Countrywide Financial Corp.	2-Aug-08	17m
Fidelity Investments	24-Sep-07	8.7m
Heartland Payment Systems	20-Jan-09	130m
IBM	15-May-07	2k
Johns Hopkins Hospital	22-Oct-10	152k
SAIC	7-May-08	630k
Sony	27-Apr-11	12m
Stanford University	6-Jun-08	82k
TD Ameritrade Holding Corp.	14-Sep-07	6.5m
Texas A&M University	9-Nov-08	13k
TJMax Stores	17-Jan-07	100m
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

Patterns will always be hackable

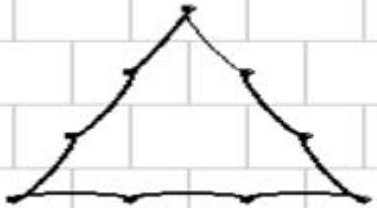
Defcon 2010 Contest on Password Hacking of 53,000 passwords



Source: http://contest.korelogic.com/

Why will passwords always be a problem?

*Keyboard



6tFcVbNh^TfCvBn

*Keyboard

R%t6Y&u8I(o0P-[

*Keyboard

#QWqEwReTrYtUyI

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

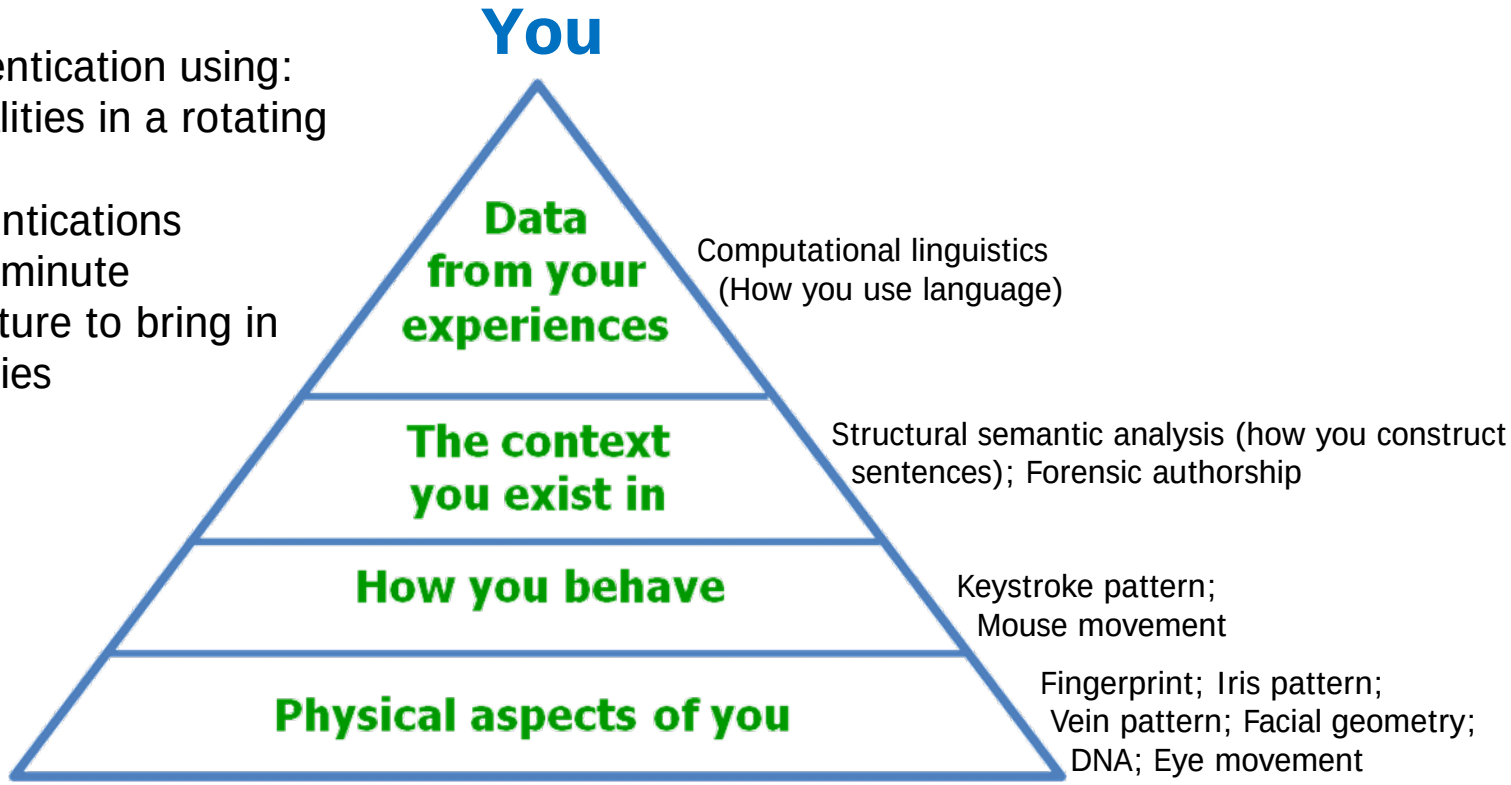
How do we move from proxies for you to the actual you?

DARPA's Potential Solution: **Active Authentication**

We seek an open solution that provides **meaningful** and **continual** authentication to our computer systems leveraging that which makes up **you**

Continuous authentication using:

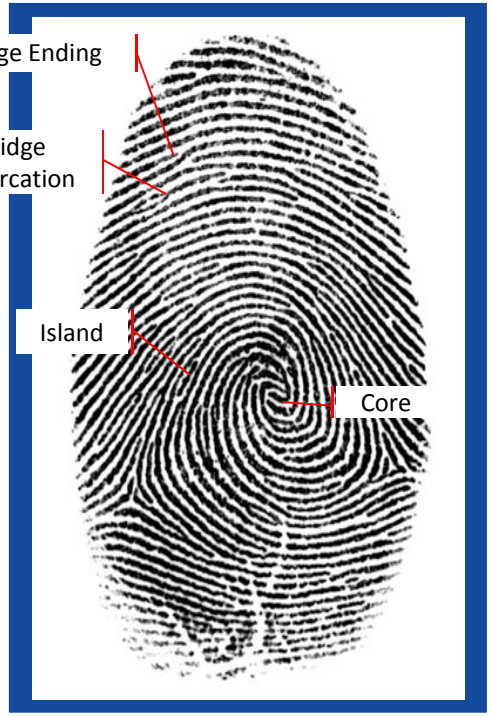
- Multiple modalities in a rotating fashion
- Multiple authentications initiated each minute
- Open architecture to bring in future modalities



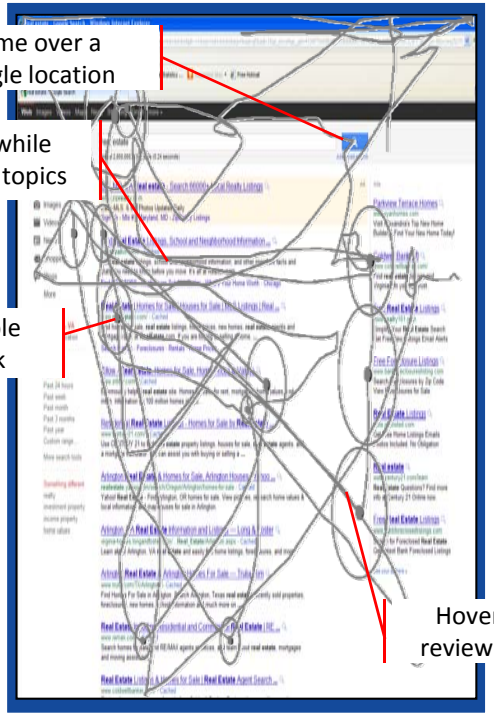
Transparent validation of the person at the computer
Without passwords
Without proxies
Without hassle

Biometric Modality Examples

Fingerprint

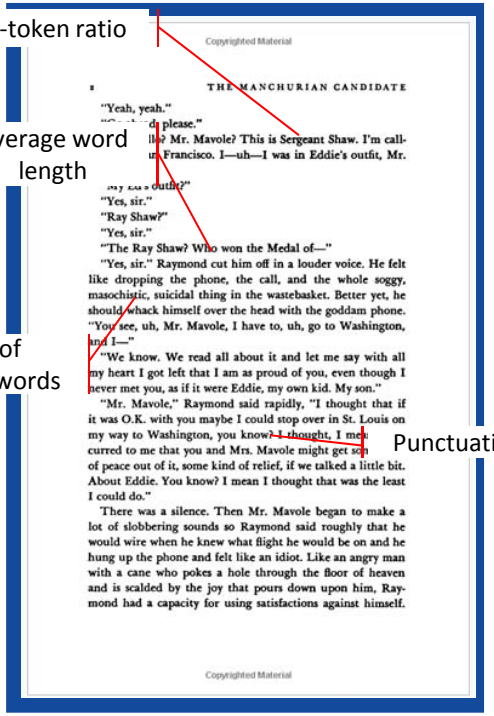


Mouse tracking[1]



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

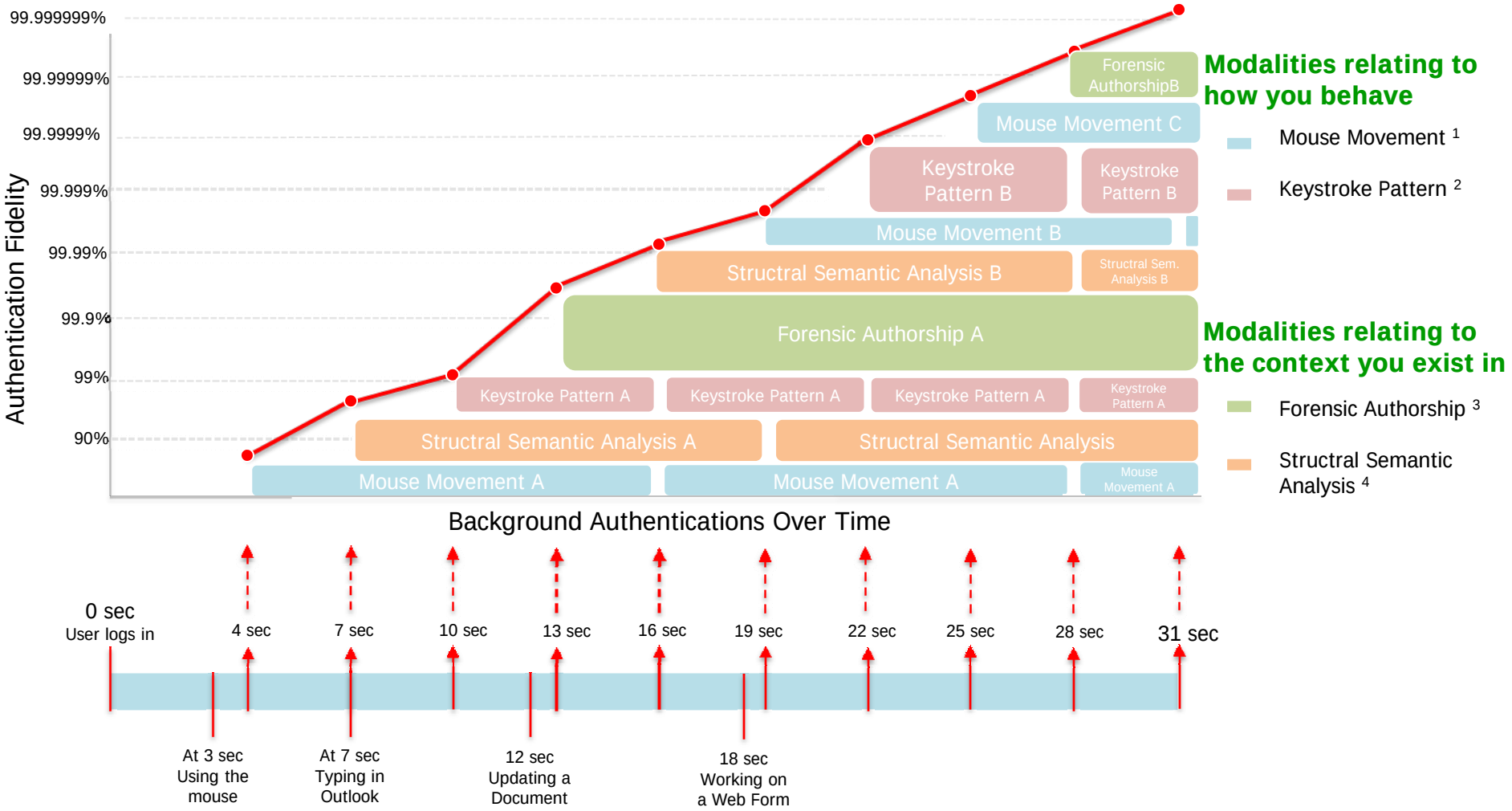
Forensic authorship[2]



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

Physical aspects of you | **How you behave** | **The context you exist in**

Active Authentication Sample Scenario



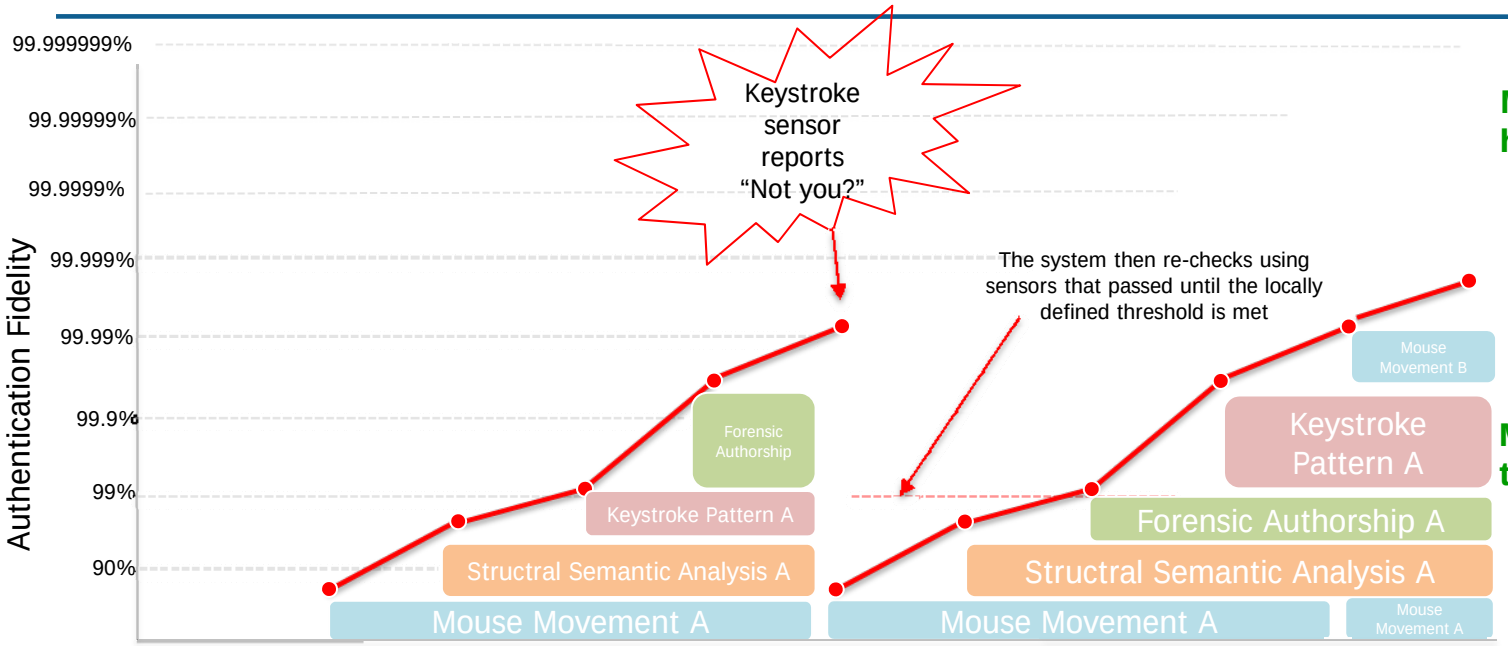
1 - Mouse Movement (Mon-Chu Chen, John R. Anderson, Myeong-Ho Sohn 2001) (73-80% True Positive Rate)

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 - Structral Semantic Analysis (de Vel et. al., 2002) (86-91% True Positive Rate)

Active Authentication Scenario

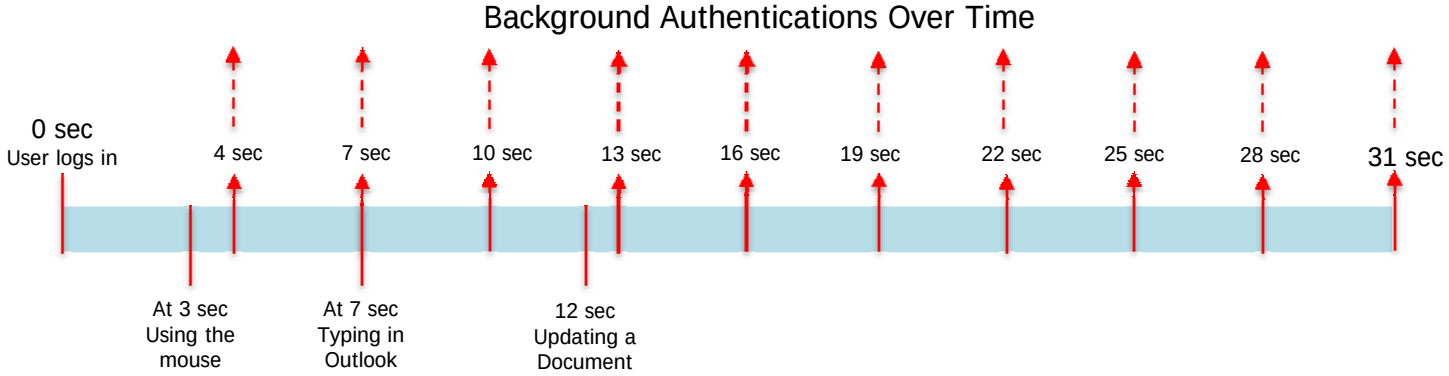


Modalities relating to how you behave

- Mouse Movement
- Keystroke Pattern

Modalities relating to the context you exist in

- Forensic Authorship
- Structral Semantic Analysis



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, locked, logged off, disconnected)

Program Focus Areas

1. Emerging Authentication Modalities:

Developing new methods for verifying the identity of the user of the computer focusing on software biometrics in an office automation environment

2. Integrated Multifactor Authentication:

Developing an integrated platform that can connect multiple biometric modalities into a single authentication solution using open architecture and communication standards (so it is not limited to the solutions of today)

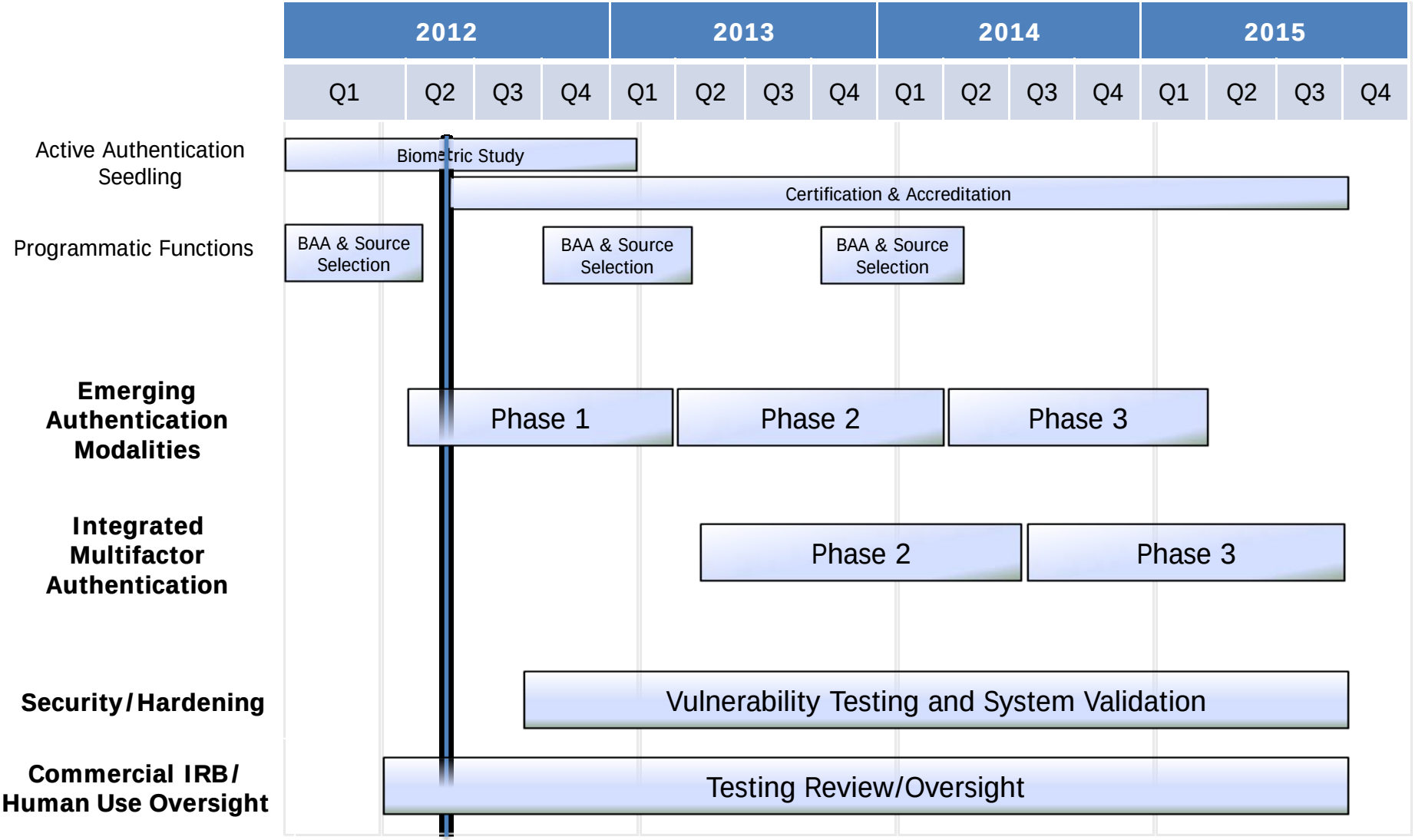
3. Security/Hardening of the Platform and Biometrics:

Provide both Independent Verification & Validation of the any code developed and provide an active Red Team analysis of all aspects of the solution; the intention is to ensure that the solutions developed do not increase the current available attack surface when used outside of a lab

What are we working on?

Neuro-cognitive patterns – National Defense University	
	Using established neuro-cognitive patterns to develop individual digital "cognitive fingerprints" from various biometric sources (physiological and behavioral) to identify an individual and may provide a framework for identification of other behavioral biometric solutions. The digital neuro-patterns will be 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. Also using honeytokens to find adversaries in the environment.
Keystroke and Mouse Dynamics – BehavioSec	
	Taking traditional keystroke dynamics and expanding them to incorporate mouse dynamics for a greater accuracy and better range of coverage.
User Behavior Patterns as seen from the Operating System – Coveros	
	Taking traditional computer based IDS algorithms and apply them to user behavior (as seen in OS interactions) to determine when someone other than the user is present.
Stylometry – Drexel University[1], Iowa State University[2], NYIT[3]	
1	Using traditional stylometric methods to validate a user based on what they are typing. Also researching detecting how adversaries can attempt to impersonate users through typing methods. [1]
2	Using stylometric methods to validate the user based on natural pauses in the way they type. [2]
3	Using stylometric methods to validate the user based on how they type (ignoring content/language) [3]
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	
	Determine the user's pattern of behavior by evaluating the screen is setup, pixel by pixel.

Active Authentication Notional Program Plan



www.darpa.mil

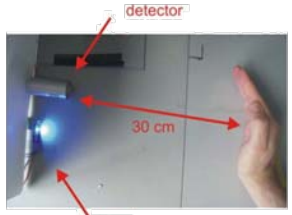
How Could the Physical Sensors Integrate?

The technology exists
Vendors are simply integrating single biometrics

Commercial integration of a Fingerprint sensor (SecuGen shown)

Skin Spectroscopy sensor designed at the University of Vaasa, Finland

Fujitsu prototype Vein Pattern sensor



Distance Pulse detection designed in a study involving Uni. Of Toulouse, France

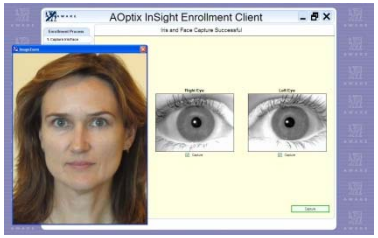
Fujitsu PalmSecure Vein Pattern sensor

One single device that measures:
Vein Pattern
Pulse
Fingerprint
Skin Impedance
Skin Spectroscopy
Without interrupting the user

Hobbyist integration of Skin Impedance sensor to a standard Dell Mouse

How Could the Software Sensors Integrate?

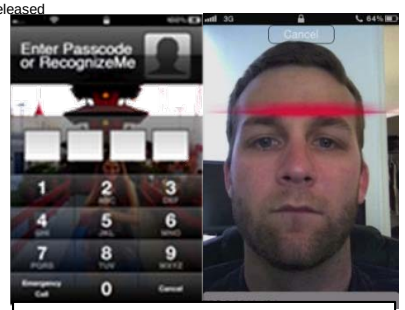
www.aoptix.com\iris-recognition-blog\wp-content\uploads\2010\10



AOptix InSight Iris & Facial recognition system

Software exists that can use common technology

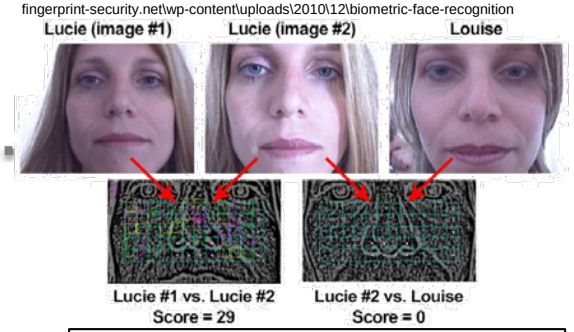
www.techcedo.com\wp-content\uploads\2011\06\Face-Recognition-Security-System-For-Your-iPhone-Released



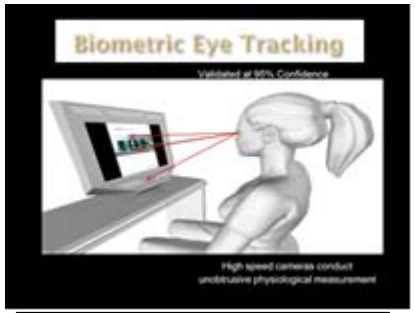
iPhone Facial Recognition

Oki Iris Scanner

fingerprint-security.net\wp-content\uploads\2010\12\biometric-face-recognition

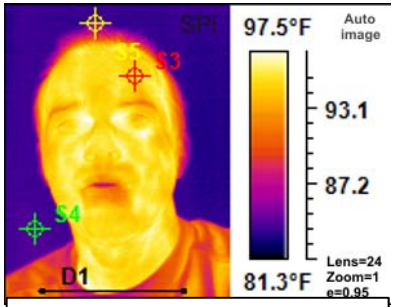


Visual Skin Print Facial Recognition



IC International Eye Movement software

Existing cameras can measure:
Iris Pattern
Eye Movement
Face Geometry
Lip Pattern
Skin Thermography
Without interrupting the user



Raptor-X thermal image

www.imaging1.com\thermography_infrared.jpg

A Large Scale Study of Web Password Habits

- Data collected from 544,960 users over a 3 month period
- Average user:
  - Has 6.5 passwords and used 8 passwords each day
  - Has 25 accounts requiring passwords
  - Each password a user has is shared across 3.9 different sites

Source: Dinei Florencio and Cormac Herley, Microsoft Research

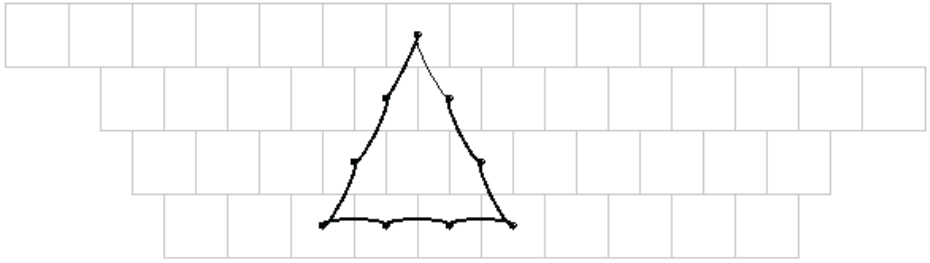
How is Technology Making the Situation Worse

Length	26 Lower-case letters		36 lower-case letters and digits		62 alpha-numeric characters		95 printable characters	
	1979	2011	1979	2011	1979	2011	1979	2011
1	30 msec	Instant	40 msec	Instant	80 msec	Instant	120 msec	Instant
2	800 msec	Instant	2 sec	Instant	5 sec	Instant	11 sec	Instant
3	22 sec	< .02 sec	58 sec	Instant	5 min	Instant	17 min	Instant
4	10 min	0.6 sec	35 min	Instant	5 hrs	Instant	28 hrs	Instant
5	4 hrs	3 min	21 hrs	Instant	318 hrs	Instant	112 days	0.1 sec
6	107 hrs	84 min	760 hrs	Instant	2.2 yrs	0.8 sec	29 yrs	10 sec
7	Not tested	Not tested	Not tested	Not tested	Not tested	46 sec	Not tested	16 min
8	Not tested	Not tested	Not tested	Not tested	Not tested	40 min	Not tested	26 hrs

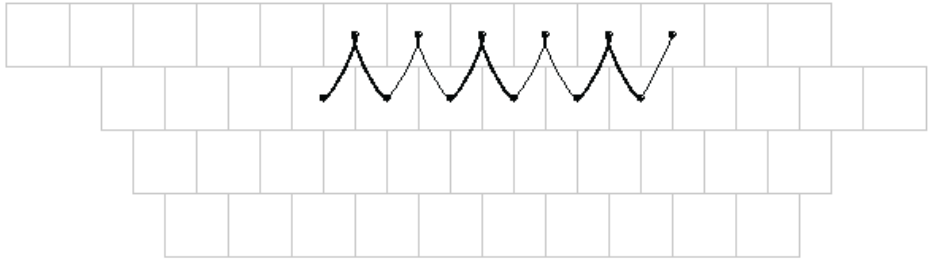
Source 1979 test: Robert Morris and Ken Thompson. Password security: a case history. Commun. ACM, 22(11):594–597, 1979
Tests performed on a PDP-11/70

Source 2011 test: http://www.lockdown.co.uk/?pg=combi&s=articles
Tests performed on Distributed.net's Project Bovine RC5-64

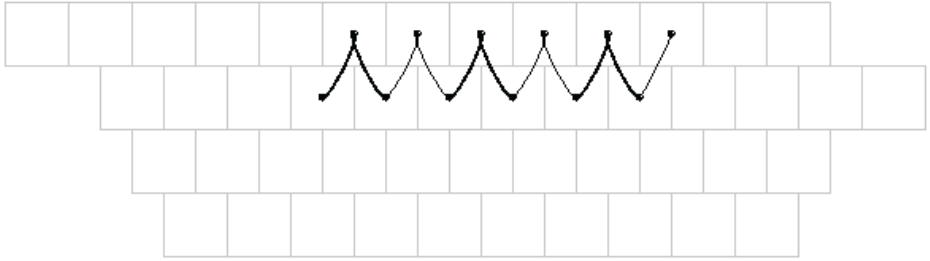
Password Complexities and Patterns



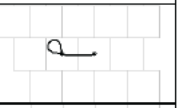
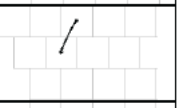
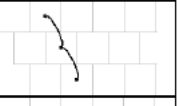
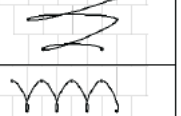
6TFCVBNHY6



0o(l8u&Y6t%R



0o(l8u&Y6t%R

Pattern Name	Description	Example
Doubles	Same key pressed twice in succession	
Triples	Same key pressed three times in succession	
Twos	Two keys in a continuous line	
Threes	Sets of three keys in a continuous line	
Fours	Sets of four keys in a continuous line	
Down-the-row	Five or more keys in one row	
Snake	Sequence of contiguous keys	
Grouped 2/3/4's	Sets of 2's, 3's, 4's offset by row or diagonal	
Split Snake	Two discontinuous snake parts	
Reflected	Sequence of mirrored keystrokes	
Zig-zag	Alternating contiguous keys from two rows	

Gawker Hacking

- The Gawker Media network, which includes popular websites such as Lifehacker, Gizmodo, Jezebel, io9, Jalopnik, Kotaku, Deadspin, Fleshbot, and of course Gawker, was compromised Dec 14, 2010.
- The hacker group Gnosis posted a torrent containing a full dump of Gawker's source code as well as the entire user database consisting of ~1.3 million usernames, email addresses, and DES-based crypt(3) password hashes.
- While this dump is not nearly on the scale of the RockYou incident, it is certainly a serious exposure.
- 99.45% of the cracked passwords were alphanumeric and did not contain any special characters or symbols:

Top 10 sites:

173942 gmail.com
101959 yahoo.com
72847 hotmail.com
20551 aol.com
8106 comcast.net
6078 msn.com
5835 mac.com
4341 sbcglobal.net
3397 hotmail.co.uk
2531 verizon.net

Top 10 passwords:

2516 123456
2188 password
1205 12345678
696 qwerty
498 abc123
459 12345
441 monkey
413 111111
385 consumer
376 letmein

Source: http://blog.duosecurity.com/2010/12/brief-analysis-of-the-gawker-password-dump/

Sony Network Hacking

- The Sony Network included ~77 million accounts was compromised 2011.
- The Lolzsec hacker group posted a torrent containing a several database files with ~37k of the alleged ~1 million customer passwords and related information stolen in the compromise.
- Only 4% of passwords had three (3) or more character types
- Half of the passwords had only one character type and nine out of ten of those where all lowercase
- Less than 1% of passwords contained a non-alphanumeric character
- 82% of passwords would fail to a basic rainbow table attack
- Within the Sony databases, 92% of passwords were reused across systems
- When compared to the Gawker breach, 67% of common accounts had identical passwords

Top 10 passwords:
seinfeld
password
winner
123456
purple
sweeps
contest
princess
maggie
9452

Source: http://www.troyhunt.com/2011/06/brief-sony-password-analysis.html

DoD Urged to Enforce Biometric Standards

GAO: Army Biometrics Collection Device Fails to Meet Standards
May 2, 2011 - Eric Chabrow, Executive Editor, GovInfoSecurity.com

Though the Defense Department has adopted standards for the collection of biometric information to help share the authentication information among agencies, one collection device mostly used by the Army does not meet those DoD standards, the GAO said in an audit published Monday.

As a result, the Government Accountability Office said, DoD isn't able to automatically transmit biometric information it collects to other agencies, such as the FBI. This can pose problems because the non-standardized Army collection device is responsible for 13 percent of the records maintained by DoD, the largest number of submissions collected by a handheld device, GAO said. This represents some 630,000 DoD biometric records that cannot be searched automatically against FBI's database of about 94 million records.

Source: http://www.govinfosecurity.com/articles.php?art_id=3600

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.

Source: http://www.msnbc.msn.com/id/43570012/ns/technology_and_science-tech_and_gadgets/t/cyber-attack-gannett-targets-us-soldiers/ 6/28/2011 6:49:26 PM ET