



# Security: Active Authentication

Richard P. Guidorizzi, *Defense Advanced Research Projects Agency*

**T**he current standard method for validating a user's identity for authentication on information systems requires humans to do something inherently unnatural: create, remember, and manage long, complex passwords. Moreover, as long as sessions remain active, typical systems incorporate no mechanisms to verify that the person that originally authenticated is the same person still in control of the keyboard. Unauthorized individuals can thus improperly obtain access to information system resources if a password is compromised or if a user does not exercise adequate vigilance after the initial authentication.

The Active Authentication program at the Defense Advanced Research Projects Agency (DARPA) seeks to address this problem by changing the game, by moving the focus during authentication from the password to the person using the information systems. This shift would mean to most people authenticating using biometric sensors. DARPA, however, saw some challenges in the way biometrics are currently used and decided to try software-based biometrics focused more on the authenticating people than on deploying new sensors.

## Moving Beyond Passwords

Biometrics are defined as the characteristics used to uniquely recognize humans based on

one or more intrinsic physical or behavioral traits. The first phase of the Active Authentication program focuses on the behavioral traits observable through how people interact with the world, without the deployment of additional sensors. Just as touching something with a bare hand leaves behind a physical fingerprint, each person leaves behind a unique "cognitive fingerprint."

At the Colloquium on Future Directions in Cyber Security held on 7 November 2011, in Arlington, Virginia, DARPA presented the Cyber Analytical Framework. The Cyber Analytical Framework pointed out that despite best efforts, an asymmetric ease of exploitation exists between attacking Department of Defense (DoD) information systems and efforts to defend them. A significant component of this asymmetric advantage comes from current password-based constructs. These constructs enable continuous access to information systems based on the proxy of someone—the password—rather than by focusing on who that someone actually is by confirming a cognitive fingerprint.

Information systems currently do not actively and continuously authenticate users—once a user acquires authentication for an information system, the system uses that authentication approval until told otherwise or some time window

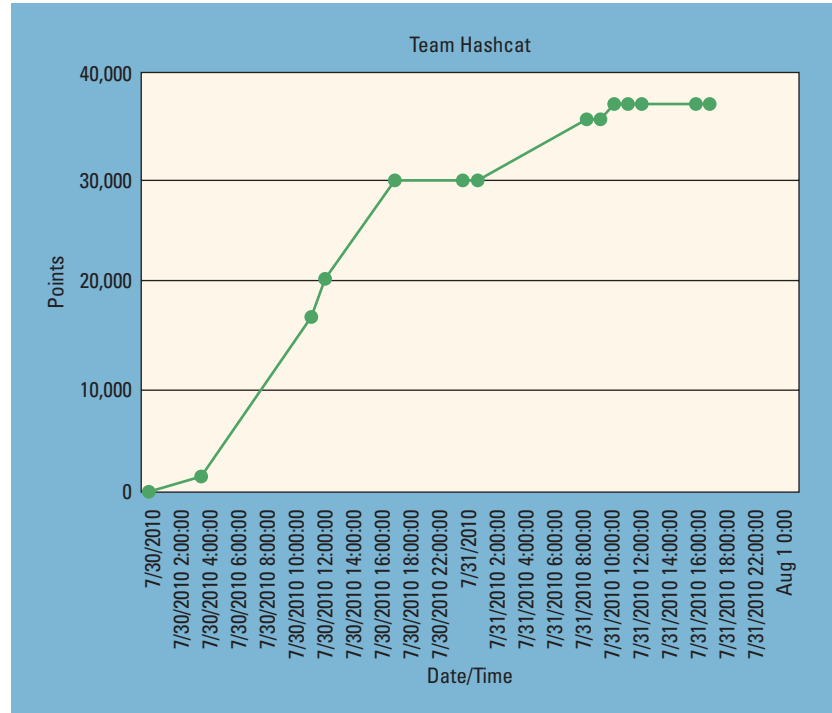
has passed. This “authenticate once based on a proxy” system is akin to common lock and key technology developed in the Middle Ages. The primary problem with this system is that with increasing ease, attackers are able to collect and use these keys (passwords) to exploit information systems.

Figure 1 shows the results of a password-hacking exercise at the DEFCON 2010 conference that challenged participants to crack 53,000 passwords in the shortest amount of time. In 48 hours, the winning team (Team Hashcat) had cracked 38,000 passwords. The two steep increases in password-cracking efficiency came from the team including specific human behavior—for example, adding a number on the end of the password or adding specific words.

In an effort to make passwords less susceptible to cracking or outright guessing, information system administrators have increased the complexity of the password itself. This approach is widely used across the US Government, including the DoD, Department of Homeland Security, and other major agencies.

Unfortunately, this approach does not strengthen the overall security posture of information systems. Requiring increasingly complex passwords does not address the root problem of authenticating proxies for users rather than the users themselves. Furthermore, not only can computers easily overcome human-created complex passwords, the added complexity can encourage humans to make bad security decisions as outlined below.

Humans are not computers and computers are not humans. Humans cannot remember random letters and numbers as well as computers can. Because of the widely used approach of increasing the length and complexity of passwords, humans often use “keyboard walking” as a password creation and recall method. Unfortunately, this technique exacerbates the overall security problem. A United States Air Force Academy study in October 2009 illustrated<sup>1</sup> that patterns from keyboard walking

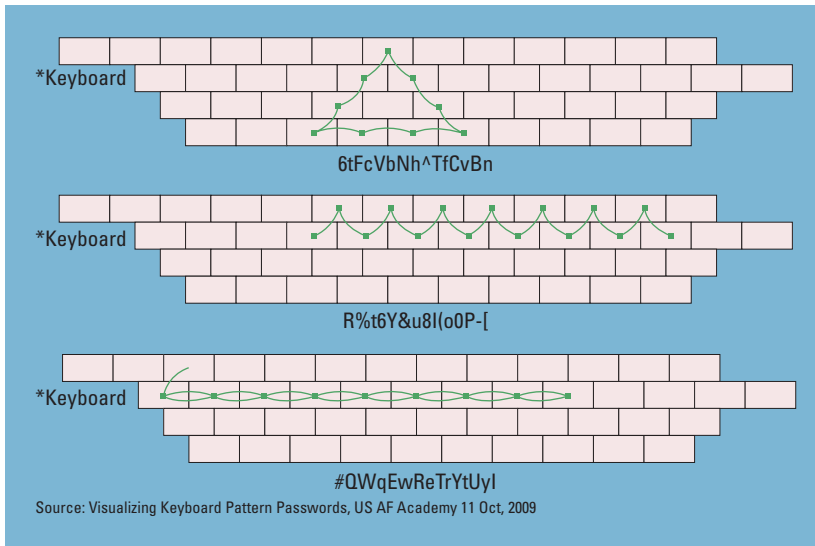


**Figure 1. Results of a password-hacking exercise that challenged DEFCON 2010 participants to crack 53,000 passwords in the shortest amount of time. In 48 hours, the winning team (Team Hashcat) cracked 38,000 passwords.**

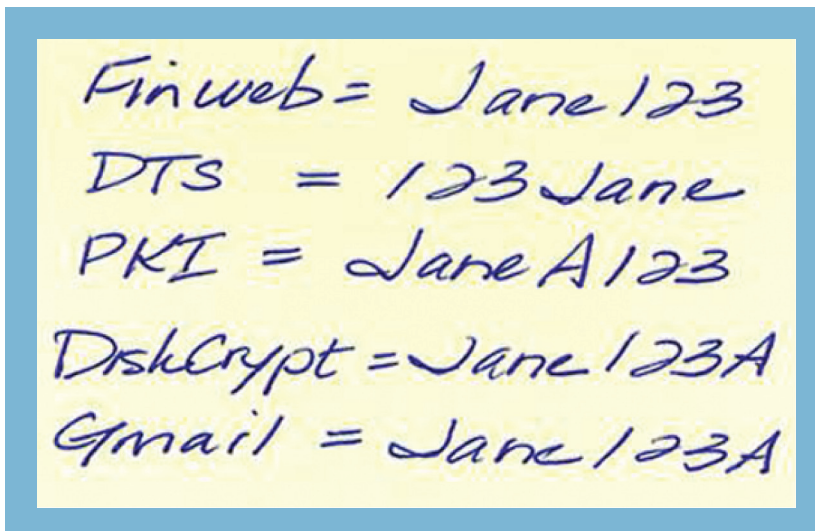
**The second phase of the Active Authentication program plans further research in individual biometric modalities with a heavier focus on mobile use.**

are no less challenging for computers to discover than passwords humans created without using keyboards to create security patterns. The passwords shown in Figure 2 are compliant with DoD standards, yet from a computer’s perspective, they are easily identifiable and thereby a serious security concern.

Additionally worrisome is the increased pressure that complex and lengthy password requirements impose upon users. To cope with the myriad of passwords in their daily life, users cheat by creating password systems of their own; Figure 3 provides a hypothetical example. Unfortunately, this type of non-random grouping of characters—such as the name of loved one—is exactly the help that password crackers seek. Also problematic is that the pattern usually holds true



**Figure 2.** These passwords comply with DoD standards, yet from a computer's perspective, they are easily identifiable and thus present serious security concerns.



**Figure 3.** These hypothetical passwords illustrate how patterns in password content present potential security concerns.

to all information systems both military and civilian, so a weak password on any system provides a risk to all systems because of their similarity. For example, Figure 3 depicts that the password for one system might be Jane123, while the password for another system is 123Jane. Cyberattackers frequently use this method of gleaning passwords from some systems to target other systems.

### Active Authentication

To move from authenticating proxies for users to authenticating actual users, DARPA is

spearheading research within the Active Authentication program in three phases.

### Phase 1: Cognitive Fingerprints

The first phase, which began in 2011 and ends 2013, aims to research biometrics that do not require the installation of additional hardware sensors, and instead develop ways to capture aspects of cognitive fingerprints through computer mice and keyboards. Approaches could include, for example, how users handle mice and craft written language in an email or document. The program places a heavy emphasis on validating any potential new biometrics with empirical tests to ensure the biometrics would be effective in large-scale deployments. Table 1 lists the ten performers for the first phase.

### Phase 2: Going Mobile

The second phase of the Active Authentication program, starting in 2013 and running to 2015, plans further research in individual biometric modalities with a heavier focus on mobile use, and begin integration efforts with DARPA's expected transition partner. DARPA's goal is to develop a prototype solution that integrates any available biometrics using a new authentication platform suitable for deployment on standard DoD desktops and laptops. The intent is an approach combining multiple modalities for continuous user identification and authentication to deliver a system that is accurate, robust, and transparent to users' normal computing experience. The authentication platform would include open Application Programming Interfaces (APIs) to allow the integration of future software or hardware biometrics from other sources.

approach combining multiple modalities for continuous user identification and authentication to deliver a system that is accurate, robust, and transparent to users' normal computing experience. The authentication platform would include open Application Programming Interfaces (APIs) to allow the integration of future software or hardware biometrics from other sources.


### Phase 3: Integration

The third phase of the program (2015) is expected to concentrate on integrating biometric

**Table 1. Phase 1 projects for the Active Authentication program.**

Research area	Company/university	Description
User search patterns	Allure Security Technology	Using users' patterns for searching for information through the deployment of decoy files that true users will never touch and can detect information-gathering activities by adversaries
Keystroke and mouse dynamics	BehavioSec	Enhancing keystroke and mouse behavioral biometrics with large-scale user trials, including research into the areas of continuous trust models and 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 users based on what they're typing. Also researching how to detect adversaries who attempt to impersonate users by mimicking typing methods.
Stylometry focused on cognitive processing times	Iowa State University	Using stylometric methods to validate users based on natural pauses in the way they type
Stylometry focused on cognitive rhythms	New York Institute of Technology	Using text productivity, pause, and revision behaviors to validate users based on how they type (includes content and language)
Screen interface	University of Maryland	Using spatiotemporal screen fingerprints to identify the user for authentication
Covert games	Southwest Research Institute	Determine users' pattern of behavior by introducing patterned system aberrations that users intuitively learns through games hidden in the computer interface
Behavioral Web analytics	Naval Research Lab (Funded by the US Navy)	Identification of users from Web browsing activities to include semantic (what kind of webpages are visited) and syntactic session features
Neurocognitive patterns	Naval Post Graduate School	Behavioral manifestations of human thought processes

modalities into the second phase of the authentication platform, with a heavy emphasis on producing a robust active authentication technology. Phase 3 would also consider development of a framework to integrate multiple biometrics on mobile devices as well as desktops. Extensive Individual Validation and Verification (IV&V) and adversarial partner efforts would be employed to ensure the authentication platform itself would not be susceptible to attack or misuse. This rigorous testing effort would be crucial to demonstrate to potential users and policy makers that this technology could be viable and trustworthy.


work accomplished in the first year of the program. 

### Reference

1. D. Schweitzer et al., "Visualizing Keyboard Pattern Passwords," U.S. Air Force Academy, 2009; [www.usafa.edu/df/dfe/dfer/centers/accr/docs/schweitzer2009a.pdf](http://www.usafa.edu/df/dfe/dfer/centers/accr/docs/schweitzer2009a.pdf).

*Richard Guidorizzi is a program manager in the Information Innovation Office at DARPA, where he develops and executes advanced R&D projects for the US Department of Defense. Contact him at [richard.guidorizzi@darpa.mil](mailto:richard.guidorizzi@darpa.mil).*

**A**s part of this special issue of *IT Professional*, the following articles describe some of the Phase 1 projects and the

 Selected CS articles and columns are available for free at <http://ComputingNow.computer.org>.