Investigation of 'cognitive fingerprints' to bolster computer passwords

September 10 2012

(Phys.org)—It won't make passwords passé, but a team led by Southwest Research Institute (SwRI) intends to use "cognitive fingerprints" to make sure you are you, and not an imposter.

Even the strongest password can be used freely once it has been compromised by a computer hacker. However, a novel software-based authentication tool called covert-conditioned biometrics will attempt to use a unique sequence of problem-solving moves to distinguish between a legitimate user and an identity thief. Research in support of the system is sponsored by the Defense Advanced Research Projects Agency (DARPA).

Covert-conditioned biometrics will incorporate principles of adaptive learning, behavior modification and game theory to capture and discriminate aspects of the cognitive fingerprint that authenticate a user's identity.

"It will deploy covert games, mimicking ordinary human computer interactions. Authenticated users are likely to unknowingly develop strategies for playing the games, even if the games are imperceptible," said Jenifer Wheeler, a senior instructional specialist in the Learning Sciences and Systems Department of SwRI's Aerospace Electronics, Systems Engineering and Training Division.

"While legitimate users will unconsciously learn how to overcome the anomalies, imposters who have never seen the anomalies will respond

differently, triggering an alert within the authentication system," Wheeler explained.

SwRI has teamed with Sentier Strategic Resources LLC to combine SwRI's experience in behavioral modeling, educational software development and learning science with Sentier's experience in cognitive psychology and human-subjects testing. The team will use adaptive learning system principles to design the two major components of the system: a user model to represent a user's game strategies, and an assessment model to deploy varied games based on user model data and user behavior.

The nine-month project comprises four major phases: collecting behavioral information related to computer use and developing a persona of a typical user; design and development, determining which types of covert game-like interactions best authenticate users with minimal disruption; developing prototype user and assessment models; and final evaluation by testing the efficacy of the system with a large group of volunteer participants.

Provided by Southwest Research Institute