Is zero-effort computer security a dream? Breaking a new user verification system

25 February 2016, by Katherine Shonesy

Researchers from the University of Alabama at Birmingham and Aalto University have found vulnerabilities in a recently proposed user-verification security system for computers.

This new security system, developed by Dartmouth College researchers, was created in response to a need for easy-to-use systems that determine whether someone is, in fact, who he or she is declaring to be—a process known as authentication.

"In our technologically based society, we need a password to do just about everything—from banking to communicating," said Nitesh Saxena, Ph.D., the director of the Security and Privacy In Emerging computing and networking Systems (SPIES) lab and associate professor of computer and information sciences in UAB's College of Arts and Sciences. "Because people often have trouble remembering all of their various passwords for different platforms, there is a lot of value in identifying simple, yet secure, ways to log in and log out of whatever it is we are doing."

It is particularly crucial in multiuser organizations, such as hospitals involving confidential patient information, to prevent one person from using someone else's login session, even accidentally.

"The security community has made progress toward achieving the right authentication system," Saxena said. "But designing one that is both user-friendly and secure is not an easy task."

Researchers from Dartmouth College sought to address this issue and create secure, user-friendly authentication, through the development of ZEBRA,or Zero-Effort Bilateral Recurring Authentication. Zero-effort authentication systems such as ZEBRA take the user out of the equation so that little to no user effort is required to ensure secure sessions.

The new system was designed to address potential security problems with deauthentication, when ideally, the user's device logs out or locks itself promptly after exiting a session. ZEBRA offers a zero-effort method of deauthentication through continuously authenticating a logged-in user by comparing what the user is doing on a device, such as a computer terminal, with measurements from a wrist-worn bracelet.

"Now the device has two different, bilateral views of the same phenomenon: The first is the sequence of direct interactions, and the second is the sequence of predicted interactions inferred from the measurements," said N. Asokan, a professor from the Aalto University Department of Computer Science. "If the two sequences match, ZEBRA can conclude that the person who is interacting with it is the same person who is wearing the right bracelet for the current login session. On the contrary, if the sequences diverge, ZEBRA can promptly and automatically deauthenticate the current login session."

The UAB and Aalto University study, which was funded by the National Science Foundation and the Academy of Finland, shows that, although ZEBRA, a system intended to enable prompt and user-friendly deauthentication, works very well with honest people, opportunistic attackers can fool the system, Asokan explains.

In the study, 20 test participants played the roles of victims while the researchers acted as attackers. The attackers mimicked what the victims were doing on their devices.

"We wanted to evaluate whether or not ZEBRA could be defeated, to measure how secure it would be when faced with someone actively attempting to hijack a user's login session," Saxena said. "We found that an opportunistic attacker can take advantage of the user quite easily."

The opportunistic attacker can choose to be near the victim and see or hear what the victim is doing and decides what interactions to mimic. For instance, a keyboard-only attacker can stop typing before the victim does and ignore everything but the user's keyboard interactions.

"When the attacker accessed a computer with an open session and carefully chose what he did on the computer, ZEBRA was not able to log him out," Asokan said. "In fact, opportunistic attackers evaded detection 40 percent of the time, mimicking the victim only when he or she thought that it would be successful."

Although susceptible to opportunistic adversaries, ZEBRA still performs well against accidental misuse by innocent adversaries.

"Modeling what an attacker can do is difficult. We point to how inadequate modeling of the attacker can lead to incorrect conclusions about the security of a system," Asokan said. "With a realistic attacker model in place, shortcomings in a system will become more apparent and can be addressed."

This joint work between Aalto University and UAB is being presented today at the 2016 Network and Distributed System Security Symposium in San Diego.

More information: Pitfalls in Designing Zero-Effort Deauthentication: Opportunistic Human Observation Attacks. DOI: 10.14722/ndss.2016.23199

Provided by University of Alabama at Birmingham