Technical Perspective: The Interplay of Neuroscience and Cryptography (Preprint)

Ari Juels Bonnie Wong

May 2014

This technical perspective is an introduction in the May 2014 issue of *Communications of the ACM* to the article "Neuroscience Meets Cryptography: Crypto Primitives Secure Against Rubber Hose Attacks," by Hristo Bojinov, Daniel Sanchez, Paul Reber, Dan Boneh, and Patrick Lincoln.

There's an untapped resource, of vast but unknown size, lying hidden under the surface. As scientists explore and attempt to map it, they are only just beginning to understand its extent and how it can best be applied to important human needs. This description might describe natural gas or geothermal energy reserves. But it also applies to the human brain, particularly in the realms of memory and computer security. The best estimates of the memory capacity of the human brain (offered by Paul Reber, an author of the paper you're about to read) place it at around 2.5 petabytes. Thats 2.5×10^{15} bytes, equivalent to the combined capacity of thousands of ordinary hard drives. Yet it is difficult for most people to conveniently remember and reliably recall passwords that contain more than 20 bits of randomness, that is, passwords with guessing difficulty greater than a 20-bit random string. A random alphanumeric password such as "7UquO91," by comparison, contains a little more than 40 bits of randomness (Because password strength grows exponentially, this is about a million times stronger than a password with 20 bits of randomness.) Strangely, then, one of the big, unsolved challenges in computer security today is how a tiny secret such as "7UquO91" can be effectively read from and written to a storage device with highly limited bandwidth, but enough capacity to hold the contents of every book in the U.S. Library of Congress. The implications are huge. Weak passwords are easy to crack, as seen in recent high-profile breaches involving millions of passwords. Forgotten passwords lead to websites use of personal questions, such as What high school did you attend?, that are often even easier to attack than passwords themselves. (Just ask former Governor Sarah Palin.) Another problem with ordinary passwords is that they can also be given away inappropriately. People can be physically coerced or threatened into revealing their passwords, or choose to disclose them to others who should not be permitted to use them. An ideal scheme for password storage in the human brain, then, would enable a password with more than 20 bits of randomness to be input and output from the brain of a human being who is unconscious of the process and thus unable to give away the password or reveal it under coercion. The paper by Bojinov et al. that you're about to read describes a way to do exactly this. It involves a fun and unexpected mechanism: Having users play a video game. Players of the game acquire fairly strong passwords using implicit learning, a channel into long-term memory by which information is stored via practice, but not consciously accessible. As presented here, this approach isnt yet practical for common authentication tasks, such as logging into an e-mail account. Playing the game takes far too long (about 10 minutes). But thats not the point or major contribution of the paper. It offers an important result highlighting the rich and under-explored intersection between neuroscience and cryptography, not to mention neuroscience and computer security more generally. One exciting frontier in neuroscience is the use of interfaces to read and stimulate neural activ-

ity directly. Electroencephalography (EEG), for instance, permits noninvasive detection of patterns of neural activity. Low-cost EEG headsets are paving the way for consumer-grade brain-computer interfaces (BCIs). Some are even available today for gamers. Such interfaces could eliminate users need to type responses to stimuli and speed up implicit-memory-based user authentication. Even more advanced techniques could someday provide a fine-grained, real-time functional view of the brain, permitting challenge-response authentication protocols executed directly against neural matter, with no conscious effort by users. There is evidence too that technologies aiming to stimulate neuroplasticity, i.e., adaptation of the brain, can enhance many forms of learning and memory, possibly including passwords. One such technology, tDCS (transcranial direct current stimulation), is now available in low-cost headsets for cognitive doping by gamers. The ambitious Brain Research through Advancing Innovative Neurotechnologies (BRAIN) initiative recently announced by the Obama administration promises to catalyze the invention of more such tools. There are many other open questions about the interplay of neuroscience and computer security. Can the natural computing facility of the brain be leveraged to achieve the equivalent of a smartcard or hardware authentication token? Can existing implicit memories be elicited with the presentation of carefully crafted stimuli and perhaps with brain-computer interfaces? Ultimately, can the intentions of users be read directly from their brains to detect and prevent malicious activity? What will brain-computer interfaces mean for privacy? On now to a paper that is exciting for stimulating just such questions—and for giving a few answers too.