Baffle thy enemy: The case for Honey Encryption

January 30 2014, by Nancy Owano

Credit: Symantec

(Phys.org) —Database breaches are making today's headlines, revealing events where thieves scoff up millions of passwords. Security experts meanwhile think about, talk about and work towards fighting against such crimes. A fresh twist in the security arsenal might be to simply baffle criminals by unleashing a flood of data that appears real but is fake. "Honey Encryption" is an approach being proposed to protect sensitive data. You beat attackers by making it difficult to figure out if the password or encryption key they are trying to steal is correct or

incorrect.

A discussion about the approach on Wednesday in *Threatpost* said the tool results in the attacker seeing a plausible-looking password or encryption key which is actually incorrect, and the attacker cannot tell the information is incorrect. The two people behind this Honey Encryption approach is Ari Juels, former chief scientist at computer security company RSA, and Thomas Ristenpart, an assistant professor at the University of Wisconsin.

As it is now, a criminal intruder, with each try of an incorrect key, sees gibberish. The unsuccessful try clearly indicates it is not what he or she wants. With honey encryption, however, trying to guess the password or encryption key becomes mystifying; the attacker is dealing with thousands of, say, fake credit card numbers, and each one looks plausible. A report about their work in *MIT Technology Review* said Juels was convinced that "by now enough password dumps have leaked online to make it possible to create fakes that accurately mimic collections of real passwords."

In October, Juels had said that "Honeywords and honey-encryption represent some of the first steps toward the principled use of decoys, a time-honored and increasingly important defense in a world of frequent, sophisticated, and damaging security breaches." He said that the honeywords and honey encryption are joint work, respectively, with Ron Rivest and Tom Ristenpart. He said honey-encryption creates "ciphertexts that decrypt under incorrect keys to seemingly valid (decoy) messages."

The Honey Encryption system, meanwhile, will be the subject of a paper later this year when Juels and Ristenpart present their "Honey Encryption: Security Beyond the Brute-Force Bound" at the Eurocrypt conference in May, an event that is focused on cryptographic techniques,

in Copenhagen.