Beunardeau, Marc; **Ferradi, Houda**; **Géraud, Rémi**; **Naccache, David**

Honey encryption for language. Robbing Shannon to pay Turing? (English) Zbl 1410.94046

Phan, Raphael C.-W. (ed.) et al., Paradigms in cryptology – Mycrypt 2016. Malicious and exploratory cryptology. Second international conference, Mycrypt 2016, Kuala Lumpur, Malaysia, December 1–2, 2016. Revised selected papers. Cham: Springer. Lect. Notes Comput. Sci. 10311, 127-144 (2017).

Summary: Honey encryption (HE), introduced by *A. Juels* and *T. Ristenpart* [Eurocrypt 2014, Lect. Notes Comput. Sci. 8441, 293–310 (2014; Zbl 1332.94069)]), is an encryption paradigm designed to produce ciphertexts yielding plausible-looking but bogus plaintexts upon decryption with wrong keys. Thus brute-force attackers need to use additional information to determine whether they indeed found the correct key.

At the end of their paper, Juels and Ristenpart leave as an open question the adaptation of honey encryption to natural language messages. A recent paper by *R. Chatterjee* et al. [2015 IEEE Symposium on Security and Privacy, 481–498 (2015; doi:10.1109/SP.2015.36)] takes a mild attempt at the challenge and constructs a natural language honey encryption scheme relying on simple models for passwords.

In this position paper we explain why this approach cannot be extended to reasonable-size human-written documents e.g. e-mails. We propose an alternative solution and evaluate its security.

For the entire collection see [Zbl 1369.94005].

MSC:

94A60 Cryptography

Full Text: DOI