Authentication Scheme using Honey Sentences

Nuril Kaunaini Rofiatunnajah[1] and Ari Moesriami Barmawi[2]

[1,2]School of Computing, Telkom University, Bandung, Indonesia
[1]nurilkaunainir@students.telkomuniversity.ac.id, [2]mbarmawi@melsa.net.ida

Abstract

Password-based authentication has dominated authentication schemes for decades because of its usability. However, password-based authentication is vulnerable to password-guessing attacks. To mitigate this attack, users have to choose a good password that is hard to guess. However, a password secured enough from password-guessing attacks will be difficult for users to memorize. One of the prior works that increase the complexity of password-guessing attacks without decreasing the usability is honey encryption (HE). HE produced a fake plausible-looking plaintext as the decoy message when the attacker guessed the incorrect password. Some research implements the HE into an authentication scheme. However, the authentication scheme using HE has some weaknesses. The decoy message just uses one word and is still suspicious to the attacker. All of the decoy messages also have to be stored in the database. To address these problems, we proposed an authentication system that used honey sentences as the confirmation message instead of a word. Honey sentence is dynamically generated using natural language and has to be natural enough to fool the attacker. When the attacker inputs the incorrect password, the honey sentence is returned to the attacker, such that he could not determine the correctness of the guessed password. The experiment result showed that 80,67% of the generated sentences are considered natural, and the complexity of finding the correct password from all possible passwords is higher than the previous methods.

Keywords: authentication, honey sentences, password-guessing attack.