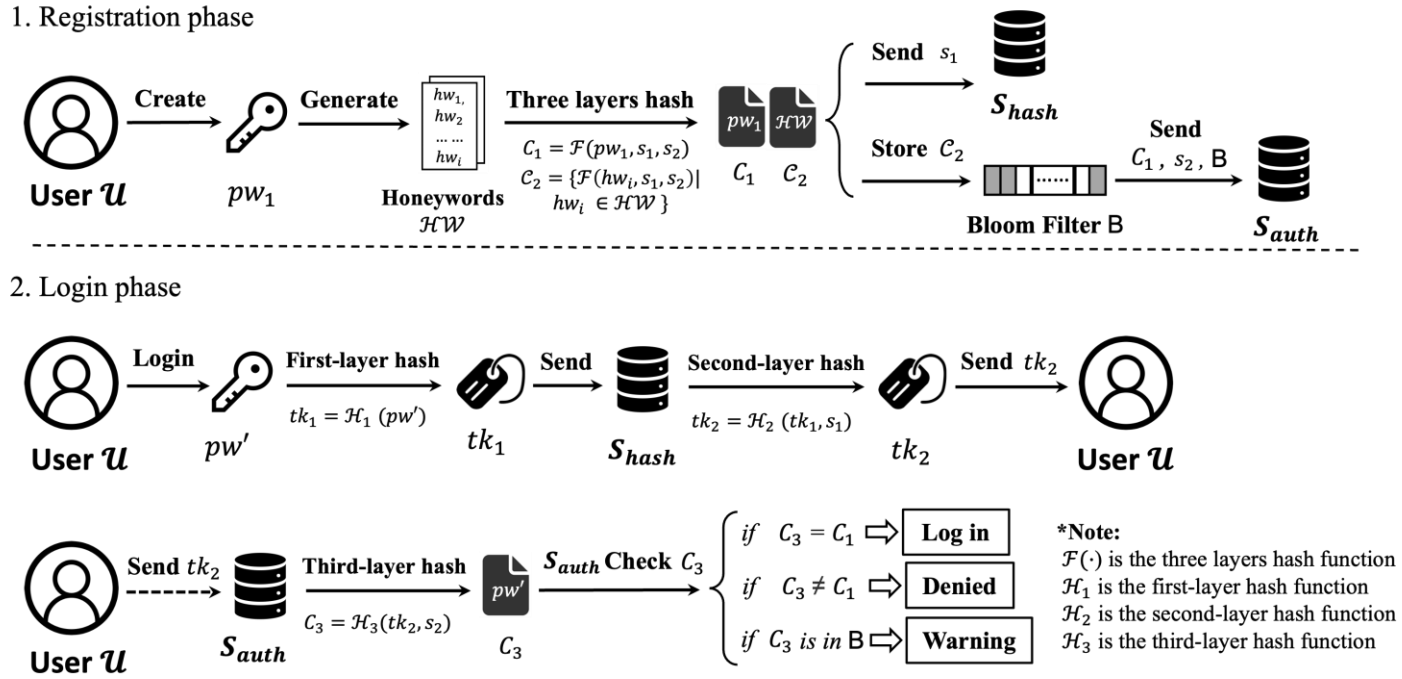
Stay Away from My Passwords! Revisiting the Security of Honeyword-Based Systems

Tingting Rao, Wanying XU, Peng XU, Wei WANG, Zhaojun LU, Mauro CONTI, Kaitai LIANG.

Frontiers of Computer Science, DOI: 10.1007/s11704-025-51375-z

Problems & Ideas

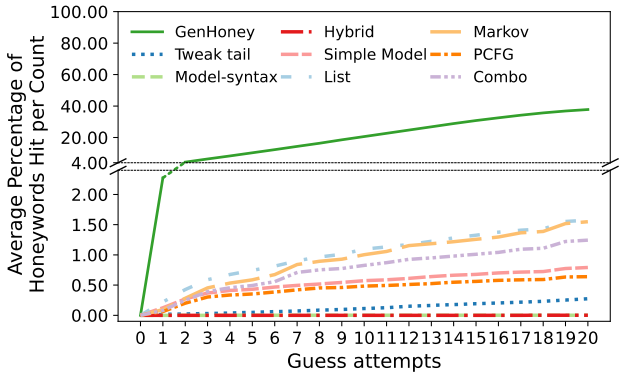
- Problems of Honeyword-Based Systems:
  - The authentication server is a single point of full trust (i.e., it is not allowed to be intruded upon or colluded with by attackers).
  - The stored real passwords are vulnerable to tweaking attacks once attackers gain knowledge of the passwords from other sources.
- Ideas: A secure three-layer honeyword-based authentication system with a novel honeyword generation method called GenHoney.



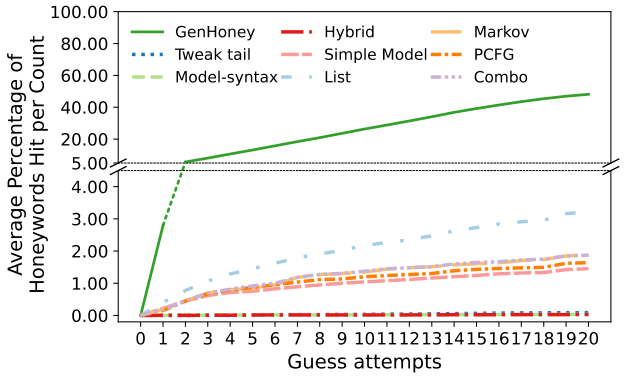
SecHive System Components and their Interactions.

Main Contributions

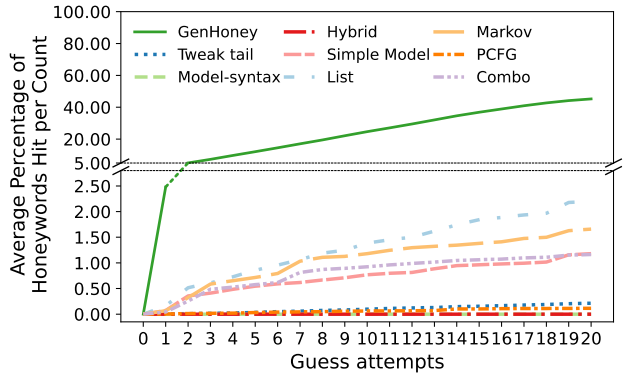
- Contributions:
  - A secure three-layer honeyword-based authentication system with a semi-honest authentication server and a hash-query server;
  - A novel honeyword generation method called GenHoney, which is embedded in SecHive to detect tweaking attacks effectively;
  - Extensive experimental results prove that SecHive improves security over state-of-the-art honeyword-based authentication systems, in particular, at least a 7.39x improvement in the accuracy of detecting tweaking attacks.



Taobao → 000Webhos.



Dodonew → Badoo.



Dodonew → CSDN.

Experimental results for targeted scenarios where the attacker breaches different sites. In each attack scenario A→B, the attacker utilizes a user's password from site A to compromise the same user's account at site B.