Bellevue University

Salts and Peppers

In Hashing

Timothy Jelinek

CIS313-T301 Cryptography

10/1/2023

Using salt and pepper in hash functions is important because it is difficult for attackers to reverse and get the original password. Salt is when random data is added to the input data before sending it into a cryptographic hash function. Salt can be stored next to the hash value. Pepper is added the same way to the input data before sending it to the hash function, however, the difference is that pepper is kept secret by storing it separately or not at all. These ways of securing data, like passwords, are needed so that your important, personal information is kept very secure and safe.

Modern versions of UNIX/Linux use salt to keep your password safe. When sending your password through their hashing algorithm, it first adds a numerical number that tells you that the hashing algorithm is being used. After that comes the salt value. The last field is the hash value. If there was no salt value applied before storing a password, then it would be easier to use a dictionary attack to guess the password. I am glad modern versions of UNIX/Linux use a salt value to keep passwords safe.

Windows does not salt their NTLM hashes. By not using salt, it is possible for attackers to use pre-computation attacks. It is also easier to notice similar passwords based on NT hashes solely where the encryption is not broken up. In many situations, NT hashes are equivalent to passwords. This allows for authentication solely on the knowledge of the hash itself. With this being the case, the attack known for figuring out the passwords by looking at the hashes is called Pass-the-Hash.

Sources:

"Cryptography: Salt vs Pepper" Spacey, https://simplicable.com/IT/salt-vs-pepper. Accessed 1 October 2023.

"How are passwords stored in Linux (Understanding hashing with shadow utils)" Pillai, https://www.slashroot.in/how-are-passwords-stored-linux-understanding-hashing-shadow-utils. Accessed 1 October 2023.

"Global Information Assurance Certification Paper" SANS Institute, https://www.giac.org/paper/gcih/34273/pass-the-hash-windows-10/174913. Accessed 1 October 2023.