




Password storage

Gianluca Dini
Dept. of Ingegneria dell'Informazione
University of Pisa
Email: gianluca.dini@unipi.it
Version: 2022-04-12

1

Storage of password



UNIVERSITÀ DI PISA

- Passwords are stored in hashed form
 - <username, hash>
- Example
 - alice 4420d1918bbcf7686defdf9560bb5087d20076de5f77b7cb4c3b40bf46ec428b
 - jason 695ddccd984217fe8d79858dc485b67d66489145afa78e8b27c1451b27cc7a2b
 - mario cd5cb49b8b62fb8dca38ff2503798eae71bfb87b0ce3210cf0acac43a3f2883c
 - teresa 73fb51a0c9be7d988355706b18374e775b18707a8a03f7a61198eefc64b409e8
 - bob 4420d1918bbcf7686defdf9560bb5087d20076de5f77b7cb4c3b40bf46ec428b
 - mike 4b529ac375b4217be17fef1a4a6f1624185cc99909e92278c0759e12ab3d61fa

apr. '22

Hash functions

2

2

Criticalities



UNIVERSITÀ DI PISA

- If different users choose the same password, they have the same hash
 - Example: Alice and Bob
- Dictionary attack (brute force attack)
 - E.g.: <https://www.onlinehashcrack.com/>
- Rainbow table attack:
 - Pre-computed database of hashes for fast access
 - Trade storage for computation
 - E.g. <https://crackstation.net/>
 - E.g.: Mike / “friendship”

apr. '22

Hash functions

3

3

Salting password



UNIVERSITÀ DI PISA

- Salt is a fixed-length cryptographically-strong random value that is added to the input of hash functions to create unique hashes for every input, regardless of the input not being unique.
- Salt makes a hash function look non-deterministic
 - Don't reveal password duplications through hashing.

apr. '22

Hash functions

4

4

Salting password



- Salting a password
 - Upon creation of a new user
 - Compute salt = random()
 - Compute hash = $H(\text{salt} \parallel \text{pwd})$
 - Store <username, salt, hash>
- Advantages
 - Salting makes a Rainbow Table Attack infeasible
 - If stored elsewhere than hash, salt also makes a Dictionary attack infeasible

apr. '22

Hash functions

5

5

Salting password



- Example
 - Alice
 - Password: admin
 - salt: 317029;
 - hash: f9ea5ab02d83138e4f0f1f87ffd2c62a
 - Bob
 - Password: admin
 - salt: 450982
 - hash: 8c13e26985d3972bff4063861194c98c

apr. '22

Hash functions

6

6