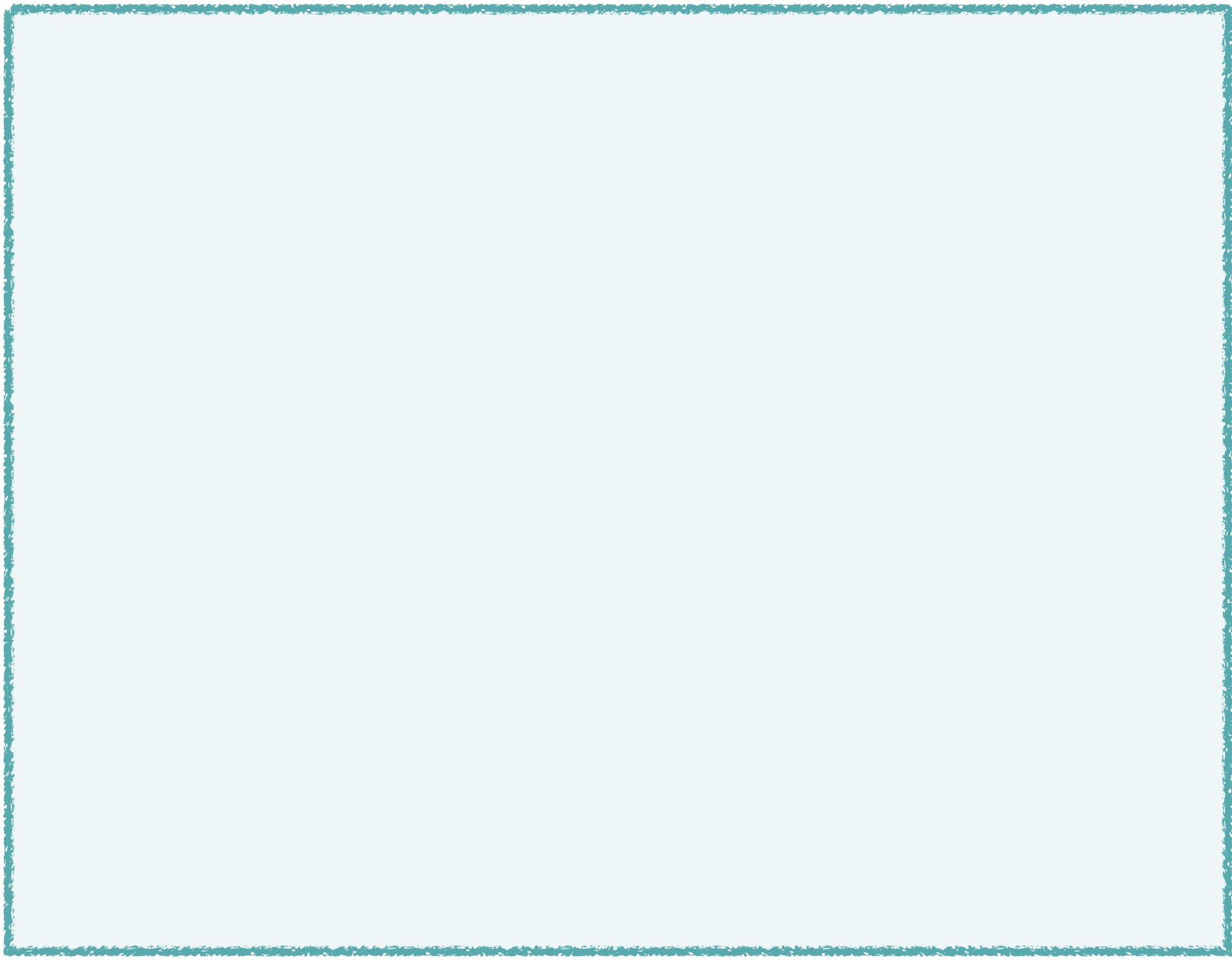




JENNER AREN





TIGER

SCOTT

USER LOGIN: Migrate Passwords



SLEEP BETTER WHEN COINTEGRATION

72

Problem: Migrate password hashes to new algorithms

Solution: Chain hashing functions







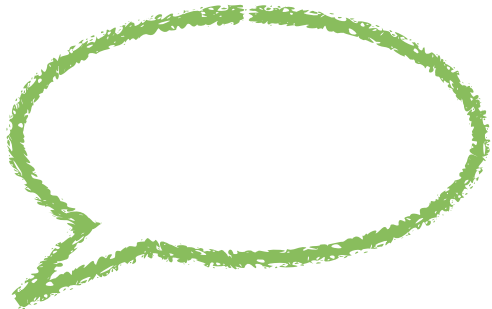












User	Algorithm	Hash
SCOTT	▶ MD5(PWD)	3959dc9...
...



validated Password



hashpassword.MD5



check in database

TIGER

SCOTT

3959DC9. . .





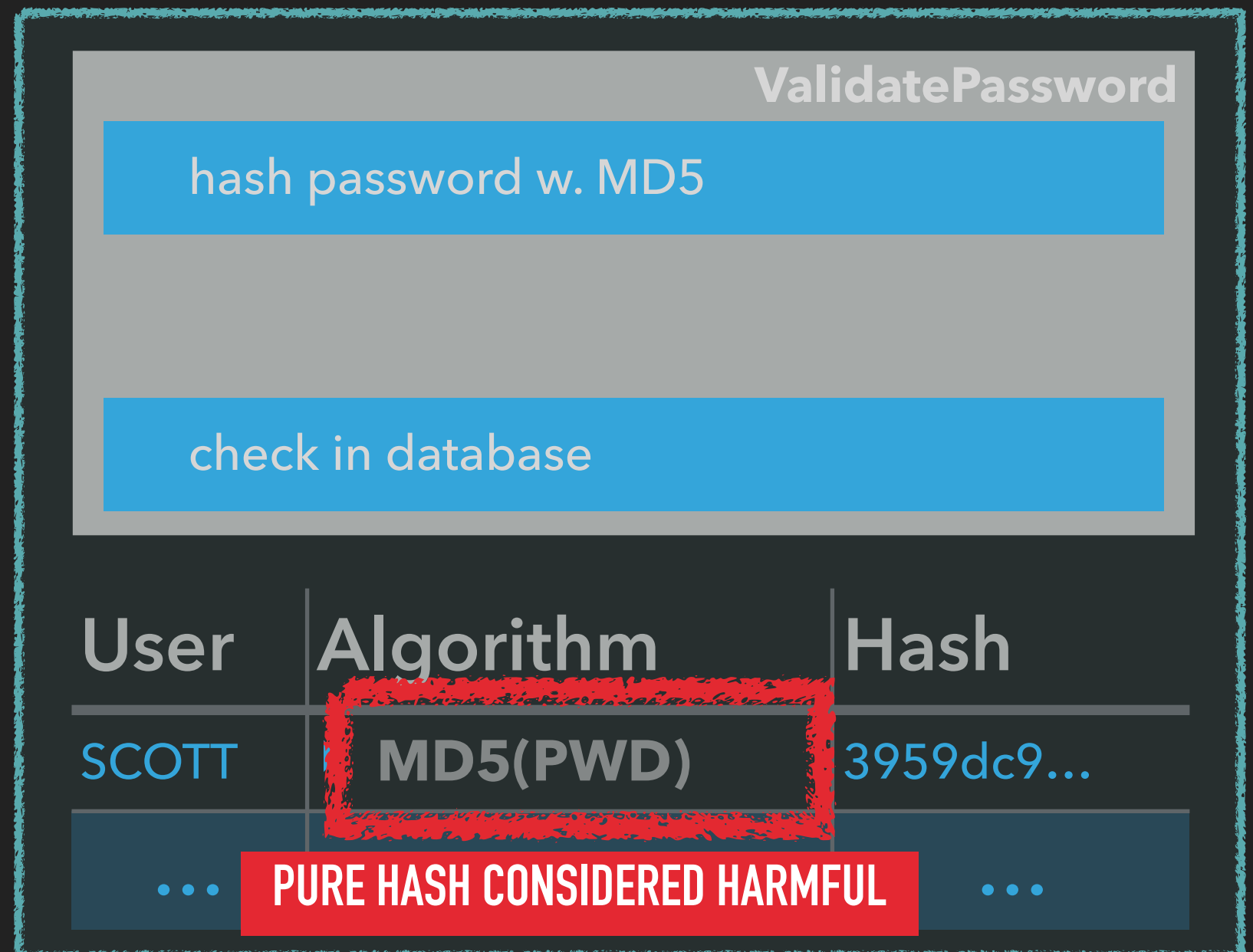
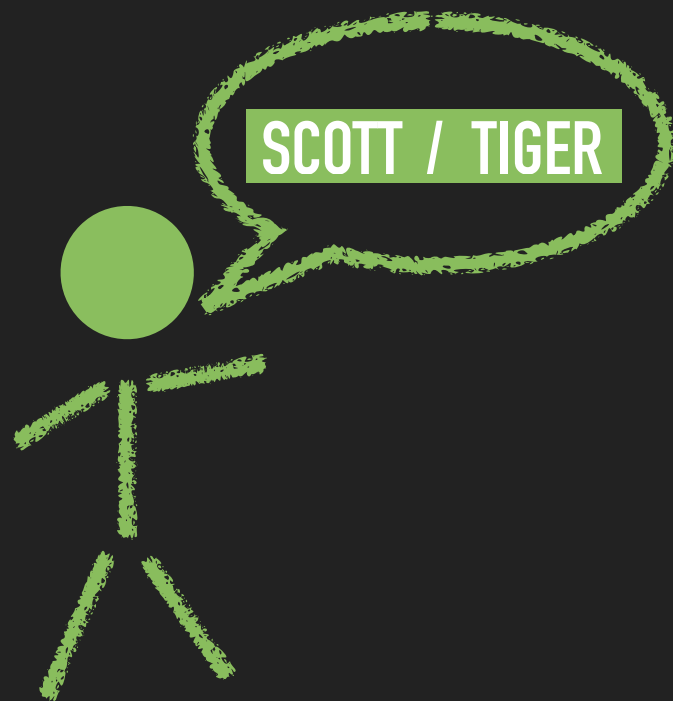
PURE HASH CONSIDERED HARMFUL

USER LOGIN: MIGRATE PASSWORDS



Problem: Migrate password hashes to new algorithms

Solution: Chain hashing functions



User	Algorithm	Hash
SCOTT	MD5(MD5)	3959dc9...
...	PURE HASH CONSIDERED HARMFUL	
...		...

Even consumer grade graphic cards calculates giga-hashes (2^{30}) per second.

- ▶ <https://www.troyhunt.com/our-password-hashing-has-no-clothes/>
- ▶ <https://gist.github.com/epixoip/a83d38f412b4737e99bbef804a270c40>
- ▶ <http://cynosureprime.blogspot.de/2017/08/320-million-hashes-exposed.html>
- ▶ https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet