



JENNER HALL FEN

0X123456...



User

Password Hash *

...

Alice

...

Eve

...

...

...

...



DATA INTEGRITY & ASSOCIATION





0X123456...

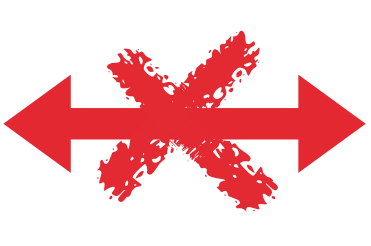
0XABCDEF...

*including the user name in the hash/hmac

0XABCDEF...



INTEGRITY PROTECTION BINDS USER TO SECRET



Problem: Protected data can be “replayed”.

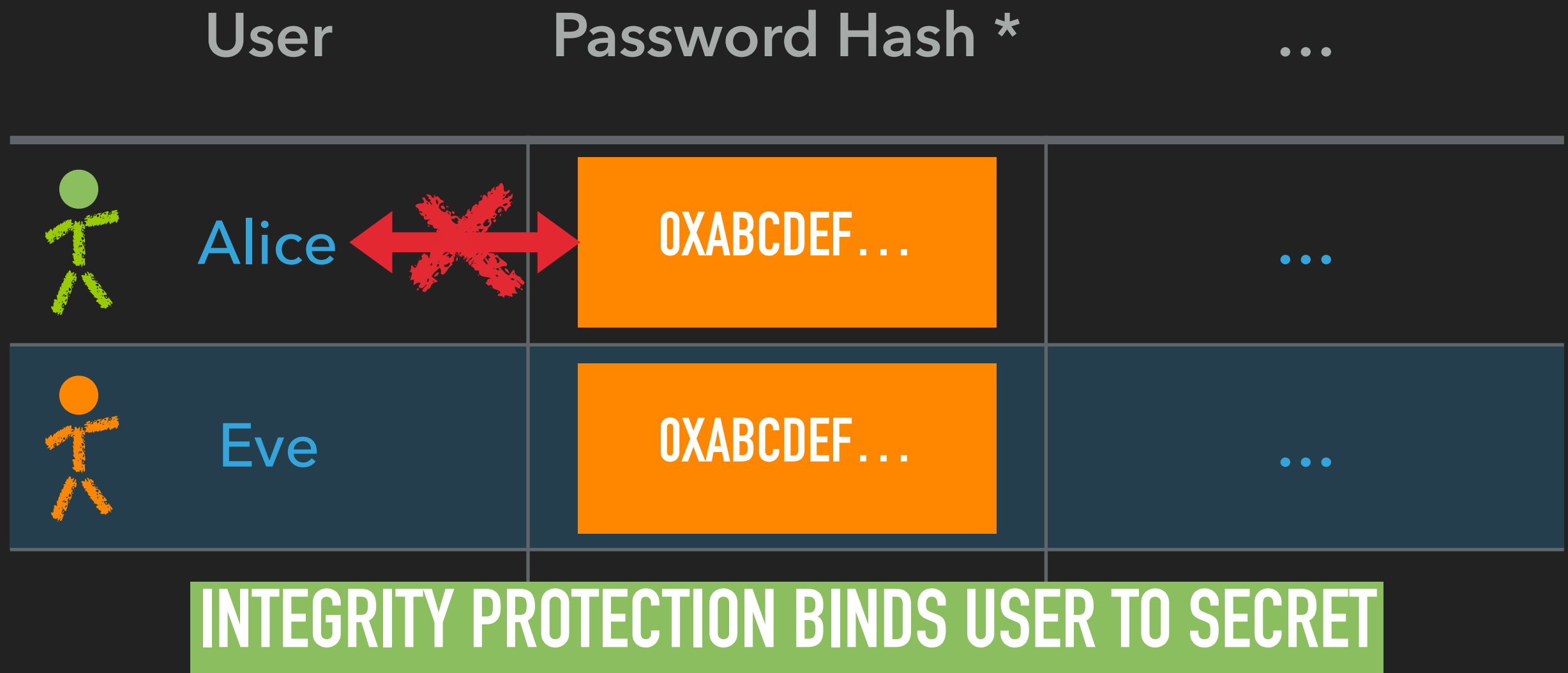
Solution: Cryptographically bind data to context.

DATA INTEGRITY & ASSOCIATION

0X123456... ✓

Problem: Protected data can be “replayed”.

Solution: Cryptographically bind data to context.



* including the username in the hash/hmac

DATA INTEGRITY & ASSOCIATION

0X123456... ✓



- ▶ Add integrity checks to the data (HMAC, AEAD encryption, signatures)
- ▶ Include an association (here: "User") in the integrity check