Hashing

Gus Khawaja

Gus.Khawaja@guskhawaja.me
www.ethicalhackingblog.com

Concept

Hashing == Integrity

One Way Hash Function

$$h=Hx$$

- The output **h** is called digest or checksum.
- The **H** is the hashing algorithm, example MD5 or SHA-2.
- The **x** is the input data.

Hashing Examples

- Generating a checksum for a file.
- Hashing passwords in the database.
- Hashing is also used in digital signatures.
- Intrusion detection systems and antiviruses.

Requirements

1. Applicable to any type of input.
2. The output must be of fixed length.
3. The output should be easy to compute.
4. The output should not be reversible to its original state.
5. **Hx ≠ Hy** (collision resistant).

Message Digest – MD5

Message Digest – MD5

- Predecessor MD4 is not used anymore (it's old and not secure).
- The output of MD5 is 128 bit (32 hexadecimal characters).
- Do NOT use MD5 to store passwords!

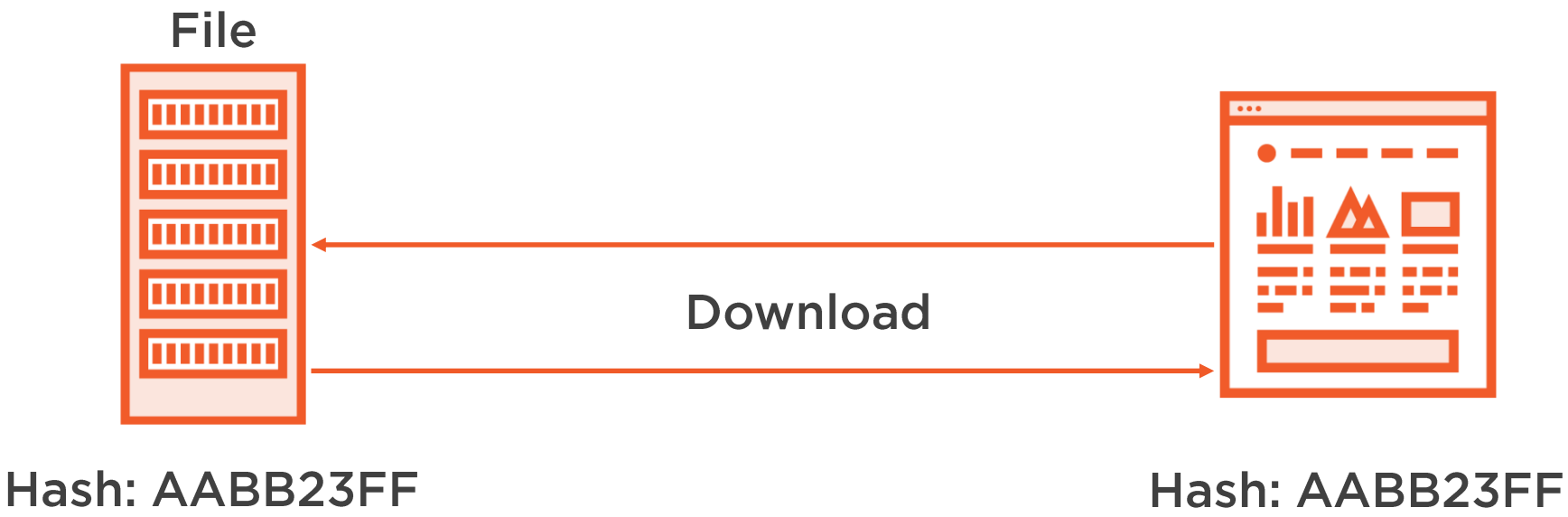
Secure Hash Algorithm - SHA

Secure Hash Algorithm - SHA

- SHA 0 – Not used anymore
- SHA 1 generates an output of 160bits
- SHA 2:
  - SHA 224
  - SHA 256
  - SHA 384
  - SHA 512
- SHA 3:
  - SHA 224
  - SHA 256
  - SHA 384
  - SHA 512

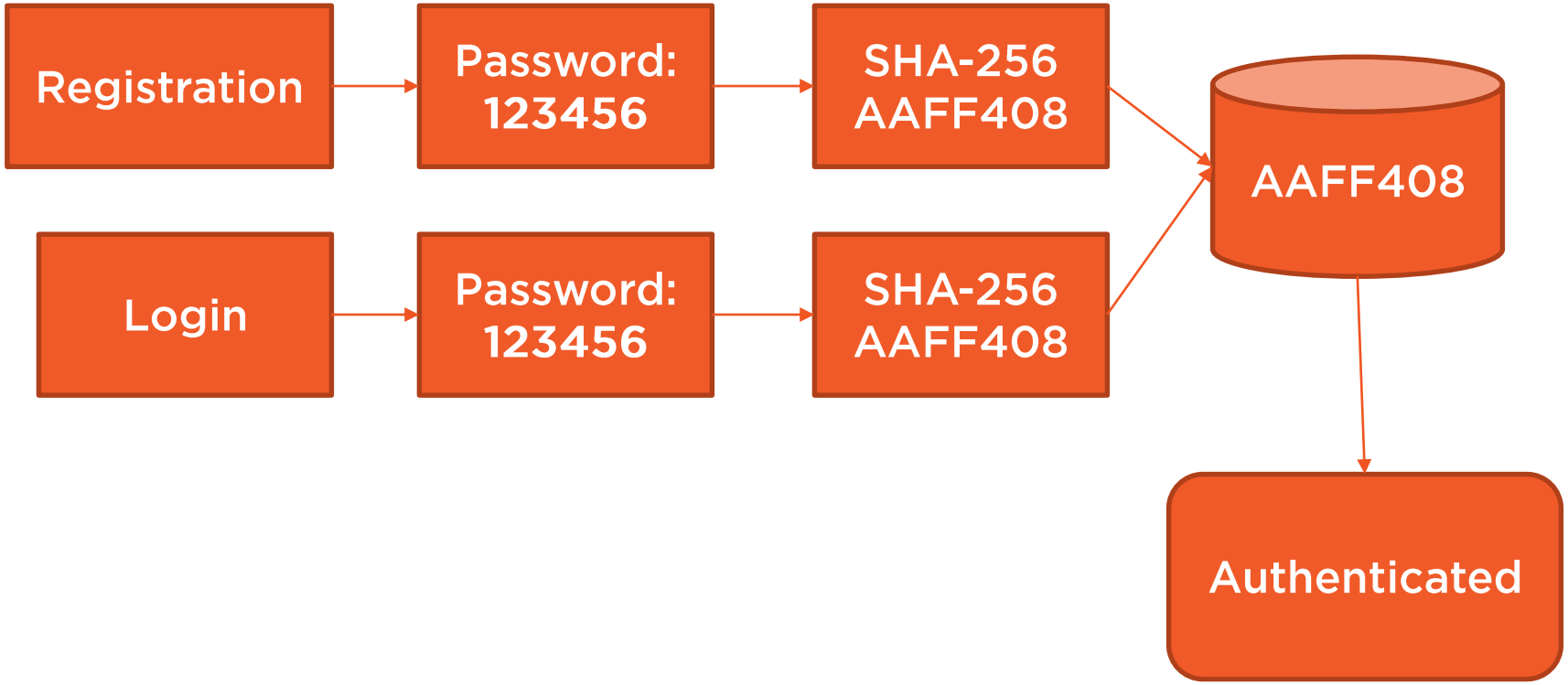
File Checksum

Example



Hashing Passwords

Hashing Passwords



Secure Method

To store passwords securely:

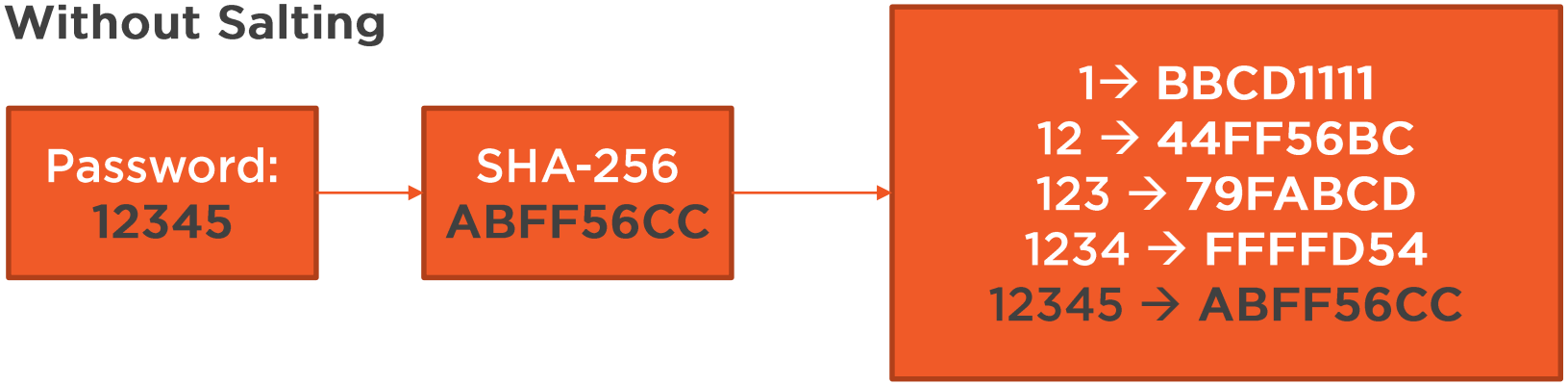
- Do **NOT** use MD5/SHA1 for storing passwords.
- **Use** SHA2 / SHA3.
- **Use** salt against password brute-force attacks.

Protection

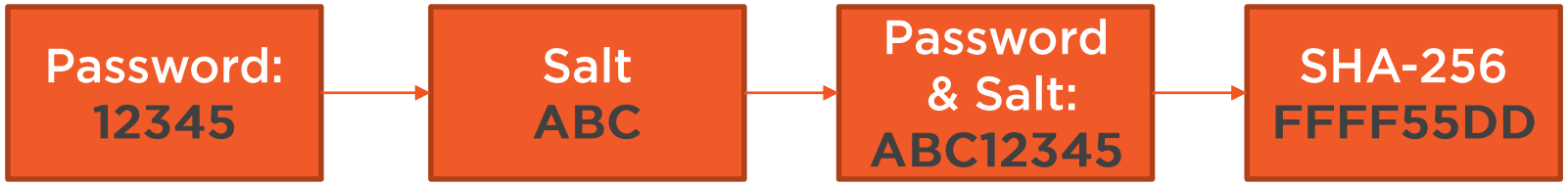
MD5	SHA-256
Fast Algorithm	Slow Algorithm
128-bit output	256-bit output

Salting

Without Salting



With Salting

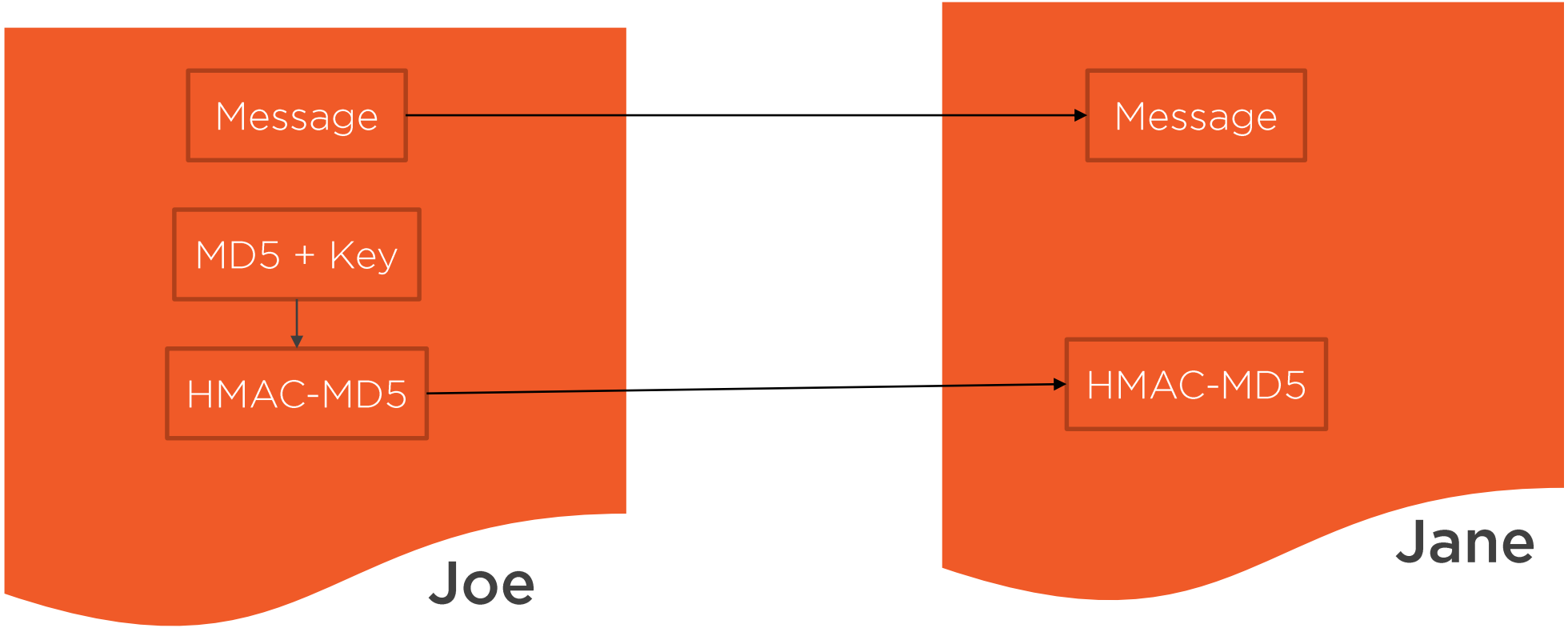


Hashed Based Message Authenticated Code
HMAC

Integrity & Authenticity

HMAC

HMAC-MD5 or HMAC-SHA1



Cracking Hashes

Benchmark

Hash Algorithm	Speed
MD4	103.8 GH/s
MD5	61,468.8 MH/s
SHA1	22,161.4 MH/s
SHA-256	7,311.3 MH/s
SHA-384	2,531.8 MH/s
SHA-512	2,544.4 MH/s

NTLM

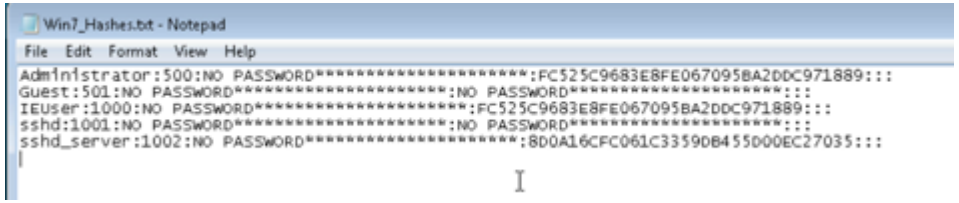
LM vs NTLM

LM - LANMAN

- Windows 95-98
- Limited to 15 Chars

NTLM – NT LAN MANAGER

- Version 1 (Not secure)
- Version 2



Summary

Hashing In Practice

- MD5 – 128 bits
- SHA 2 & 3
- HMAC – Authenticity & Integrity
- Long & Complex Passwords

  e.g. **aw@%plkMNBV--R**