SCRYPT INTRO

It is a password-based key derivation function designed to make it costly to perform large-scale custom hardware attacks by requiring large amounts of memory

SCRYPT ADVANTAGES

The cost of a hardware brute-force attack against scrypt is roughly 4000 times greater than the cost of a similar attack against bcrypt OR PBKDF2

More resistant to ASIC and GPU attacks

SCRYPT DISADVANTAGES

The algorithm is designed to use a large amount of memory compared to other password-based KDFs, making the size and the cost of a hardware implementation much more expensive

PBKDF INTRO

Its a key derivation functions with a sliding computational cost, aimed to reduce the vulnerability of encrypted keys to brute force attacks.

PBKDF ADVANTAGES

it's very lightweight, easy to implement, and it uses only very strong, proven hash functions like the NSA's SHA.

PBKDF DISADVANTAGES

While its number of iterations can be adjusted to make it take an arbitrarily large amount of computing time, it can be implemented with a small circuit and very little RAM, which makes brute-force attacks using application-specific integrated circuits or graphics processing units relatively cheap

BCRYPT INTRO

Bcrypt is an adaptive hash function designed specifically for password "storage.".

It is the default password authentication mechanism in OpenBSD

BCRYPT ADVANTAGES

It has a “work factor” which determines how much processing is needed to produce a single hash digest. It is also easy to use:

The password salt and a number indicating the work factor are included in the output so that system designers can keep using bcrypt, but up the work factor over time, without worrying about users being unable to login

BCRYPT DISADVANTAGES

Unlike PBKDF2 and scrypt, it places a hard size limit of 72 bytes/ASCII characters on the input.

SHA 256 INTRO

Its a one way cryptographic hash function used in 32 bit systems. Used for assuring message integrity

SHA 512 INTRO

Its a one way cryptographic hash function used in 64 bit systems. Used for assuring message integrity

DISADVANTAGES OF SHA 512

Can suffer reduced round preimage attacks

Are prone to length extension attacks

Slower compared to md5

DISADVANTAGES OF SHA 256

Are prone to length extension attacks

Slower compared to md5

ADVANTAGES OF SHA 256 AND SHA 512

More secure because its stronger against brute force attacks.

Highly collision resistant.