Storing Passwords

Carlos Padilla

Institute of Cybersecurity

Storing Passwords

Storing Passwords

Key Derivation Functions (KDF)

Lab 1: Password Dumps and Password Cracking. This section covers the essential concepts of key derivation functions, password dumps, and password cracking.

Specialized Attacks

Password Cracking Tools

Various tools and techniques are used to crack passwords, highlighting the need for robust key derivation functions.

Key Derivation Functions

Key derivation functions are based on an irreversible hash function. A hash function takes an arbitrary amount of data as its input and uses it to calculate a fixed-length output value called a digest. The fascination of hashing the password lies in the fact that after hashing, the value is entirely unrecognizable, and the original input value cannot be retrieved.

> *"To ensure the security of stored passwords, key derivation functions must be robust and resistant to attacks."*

Hash Function

A KDF implements a so-called difficulty factor. This value makes it intentionally more difficult to calculate the resulting hash to slow down any brute-force guessing attacks.

What Determines the Strength of a Password Hash

The strength of a password hash is determined by several factors:

- Confusion
- Diffusion
- Hash collision
- Quality of key derivation function
- Password and derived key length
- Character set support
  - 26 letters
  - 52 characters
- Password length
- Possible passwords
  - Approximately 1 trillion
- Key derivation function

Key Derivation Functions (KDF)

MD5 Message Digest

MD5 is a cryptographic hash algorithm that produces a hash value in hexadecimal format. This algorithm has serious weaknesses as it is known to have hash collisions. A collision happens when two unique plaintexts hash to the same hash value.

Secure Hash Algorithm (SHA)

SHA stands for Secure Hash Algorithm. SHA is a family of cryptographic functions with several iterations: SHA, SHA1, SHA2, SHA3.

LAN Manager Hash

The LAN Manager (LM) hash was introduced by Microsoft in 1980 and has multiple weaknesses. The LM hash is typically stored in the SAM/NTDS database system. Two severe weaknesses are a maximum password length of 14 characters and passwords being converted to uppercase.

NT LAN Manager

NT LAN Manager (NTLM) is the Microsoft authentication protocol created to be LM's successor.

Lab 1: Hashing Basics

This lab covers the basics of hashing and the importance of using secure hash functions.