Preventing Information Leakage About Password Lengths

To obfuscate password lengths from potential attackers, a padding technique is proposed. By ensuring all stored passwords are of a fixed length, regardless of their original length, the true length remains hidden. This measure prevents adversaries from gaining insights into password complexity based on length.

Preventing Swap Attacks

A robust defense against swap attacks involves the implementation of HMAC integrity checks. By calculating and storing an HMAC for each password-domain pair, any unauthorized modification, such as swapping passwords, becomes detectable. A mismatch between the stored and recalculated HMAC signifies data tampering.

Defense Against Rollback Attacks

A trusted location for storing a SHA-256 hash is essential to prevent rollback attacks. This hash serves as a baseline for detecting any unauthorized alterations to the password database. By comparing the current hash with the stored trusted hash, any rollback attempts can be identified.

Implications of Using Randomized MACs

While randomized MACs offer additional security, they come with a performance penalty. Since each tag is unique, direct lookups are infeasible. Instead, a searchable structure (e.g., database, hash table) must be employed to store MAC tags and corresponding domains. This search process increases retrieval time compared to deterministic HMAC-based lookups.

Reducing Information Leakage About Record Count

Techniques like record padding and batching can help conceal the exact number of stored passwords. By adding dummy records and grouping passwords into fixed-size batches, an adversary can only estimate a range of password counts. Periodically adjusting the number of dummy records further enhances obscurity.

Conclusion

The proposed methods effectively address key vulnerabilities in password managers. By combining password length obfuscation, robust integrity checks, rollback protection, and record count concealment, the overall security posture of password managers can be significantly strengthened.
Note: While these measures provide substantial improvements, it is essential to consider additional security best practices, such as strong encryption algorithms, secure key management, and regular security audits.
Recommendation: Further research and development should focus on optimizing the

performance impact of randomized MACs and exploring alternative methods for record count obfuscation that minimize potential security trade-offs.