Cryptology ePrint Archive: Report 2011/248

Fast Password Recovery Attack: Application to APOP

Fanbao Liu and Yi Liu and Tao Xie and Yumeng Feng

Abstract: In this paper, we propose a fast password recovery attack to APOP application in local which can recover a password with 11 characters in less than one minute, recover a password with 31 characters extremely fast, about 4 minutes, and for 43 characters in practical time. These attacks truly simulate the practical password recovery attacks launched by $malware$ in real life, and further confirm that the security of APOP is totally broken. To achieve these dramatical improvements, we propose a group satisfaction scheme, apply the divide-and-conquer strategy and a new suitable MD5 collision attack to greatly reduce the computational complexity in collision searching with high number of chosen bits. The average time of generating an ``\textit{IV Bridge}" is optimized to 0.17 second on ordinary PC, the average time of generating collision pairs for recovering passwords up to 11 characters is about 0.08 second, for 31 characters is about 0.15 second, for 39 characters is about 4.13 seconds, for 43 characters is about 20 seconds, and collisions for recovering passwords as long as 67 characters can be theoretically generated. These techniques can be further applied to reduce the complexity of producing a 1-bit-free collisions for recovering the first 11 characters, whose main target is that to reduce the number of challenges generated in APOP attack, to about 2^{36} MD5 compressions.

Category / Keywords: MD5, APOP, Challenge and Response, Password Recovery, Group Satisfaction Scheme, Divide-and-Conquer, Collision Attack.

Date: received 19 May 2011

Contact author: liufanbao at gmail com

Available formats: PDF | BibTeX Citation

Version: 20110519:191811 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]