

B.8. Sichere Passwortverwaltung

Dimcho Georgiev

Überblick

- Hash-Algorithmen
- Passwortentropie
- Hash-Table vs Rainbow-Table
- PBKDF2
- Live Demo

Hash-Algorithmen

- Was passiert wenn der Input mehr/weniger Symbolen enthält als dem fest definierten Hashwert Output?
- Verschiedene Hash-Algorithmen:
 - SHA256 – 64 Rounds, 8 Segments (32 bits each), 64 Constants
 - SHA512 – 80 Rounds
 - MD5 – 128-bit hash value, 4 Rounds, collision found
- Ist es erkennbar, wenn mehrere Benutzer(-innen) das gleiche Passwort haben?
- Kollisionen – je kürzer der Hash, desto höher die Wahrscheinlich
- Salt
- Pepper

Passwortentropie

- Maß für die Schwierigkeit
- Simple guesses (die meist 1000 verwendete Passwörter)
- Brute force (alle möglichen Kombinationen von Zeichen [mit Länge 8])
- Research (Adresse, Name von Haustier)
- R – Pool of unique characters
- L – Number of characters in your password

$$E = \log_2(R^L)$$

Hash-Table vs Rainbow-Table

- Rainbow-Tables fassen ähnliche Hashes zusammen, um Platz zu sparen, indem sie das Präfix nicht für jeden Hash speichern
f2ca5152b0... and f2ca513a13... can be stored as f2ca51 -> 52b0... and 3a13...
- Beide werden zum Speichern der Ergebnisse eines Vorberechnungsangriffs verwendet
- Rainbow-Table ist langsamer zugreifbar, benötigt aber weniger Platz
- Hash-Table ist schneller zugreifbar, erfordert aber mehr Speicherplatz
- Bevor eine Rainbow-Table erstellt werden kann, wird zuerst eine Hash-Table erstellt
- Salt verhindert beide Angriffsmethoden gleichmäßig (absolute, wenn der Salz wert geheim ist)

PBKDF2

- Password-Based Key Derivation Function Version 2
- Salted password hash
- NIST - salt length of 128 bits.
- Slowness durch Wiederholung
- In 2000 the recommended number of iterations was 1 000,
- In 2021 the number of recommended iterations reached 310 000
- Computers become faster over time (Gordon Moore). Human brains do not

Live Demo

```
SL Y w^ m fyX S^ v l X%ib 1 & A w Y1Bn yf 1L6LY yw n S 7 55 Wf Dvvr k bZkZY BZbxx^ 0 0 SMY r1Yak70 TBAr w 5X M YX D aBL G &
n YL G &n b ^LS ZB ML D SfyX f 0 & & Xwk1 LA fa0LG L% i Z Y ^ %A SLL5 b 1xbxX kx1BBM i i Zw 5wY7bY1 Wk65 & ^r v Yr S 7DXa T 0
1 YD T 01 X nLZ xk va S Z^Lr A i M 0 S&bf 16 A7iDT lf f x X MM f6 Yaa^ 1 wB1BS bBwkkv y y xL& ^G6Y1Xy %bM^ 0 M5 L L5 Y YSrF W i
f nS W 1f r 1dx Bb L7 Y xn15 6 y b i Z01A DM 6YySW D^ A B S v v ^M Y7Ym w 6kwxZ 1k&bbL L L Ba0 MOTXwSL f1bM i vM a l^ Y XY5Y % y
A iY % ya 5 fSB k1 aY Y B1D^ M L X y x1w6 Sb MKLY% Sn 6 k Z LL nb 0YVv & 0b6bx wb011a l l k7i v1WS&ZL ^wXv y LM 7 DM G SY^X f f
6 fy f L6 ^ AYk bw 7X kFSM b l r l By&M YX bSLYf Yi M b x aa iX iXXL 0 i010B 6liw7 D D bYy Ly%Z0x0 n&rL L av Y Dv T ZGMS ^ l
M A ^ LM M 6Yb 16 YS bAYv X D 5 L kL0b Yr XZDG^ Yf b b 1 B 77 fr ySSa i ywiwk 0wy66Y S S 1XL aLfxiBS i05a l 7L X TL W xTvZ n D
b 6 n Db v MGI w0 XZ 16YL r S ^ D bLiX G5 rxSTN A X w k YY A5 LZ27 y L&y6b 16L00X Y Y wSL 7L^ByKy f1^7 D Ya S pa % BWLx i S
X M i SX L bTw 6i Sx wM a 5 Y M 0 S 1Dyr T^ SBYw1 6 r & b XX 6^ LxxY L L0L01 y0Liis Y Y 6ZD YDnKLbY AyMY S X7 Z G7 f k%aB f Y
r b f Yr a XW6 0y ZB 6b 7 ^ Y v Y wSL5 WM ^kY% M 5 0 1 SS MM bBBX l Di1iw LiDyyZ b G 0xS XS1b116 6LvX Y SY x TY ^ b7fK A Y
5 X A Y5 7 r^0 iL xk OX Y M v L Y 6YL^ %w MbGfA b ^ i w ZZ bx skkS D SyD& lySLLx i T iBS SYf1DwT MLLS Y ZX B WX n 1^Yb 6 G
^ r 6 G^ Y 5f1 yL Bb ir X v L a G OYDM fL v1T^6 X M y & xx VL TbbZ S YLSL0 DLY1LB w W ykp ZYAwS6W bDaZ xS k %S i wnX1 M T
M 5 M TM X ^y LD k1 y5 S L a 7 T iASv ^a LwWM r v L 0 BB ra p1lx Y YLY1 SLYDDk w % Lb6 xG66Y0% XS7x BZ b fZ f 6iSw b W
v ^ b Wv S MnL LS bw L^ Z a 7 Y W y6YL n7 a6%ib 5 L l i kk 57 GwWb Y XDYD YDGSSb h f L1T BTM0Y1f rYYB kx i ^x A 0fZ6 X %
L M X %L Z v1l DY 16 LM x 7 Y Y % LMYa iY 70ffX a D y bb ^Y T6&v w SSGSL YSTYY1 8 ^ Dww Kwb1Gy^ SYXk b8 w n6 i AaX0 r f
a v r fa x LFD SY w0 Dv B Y X S f 1b 7 fX Yi^Ar M 7 S L 11 MX W00b L ZYTYL GYwYw ^ n S6% b%XYTLn ^GSb 1k & ik M y6B1 5 ^
7 L X 5 ^7 B aAS YG 6i SL k X S Z ^ DX Y AS Xyn65 v Y Y l ww vS %i1l a xYwYD TY% G6 A i Y0f 1frLwL1 MTZ1 wb 0 fb b LMky ^ n
Y A ^ nY k 76Y YT 0y Ya b S Z x n Sr X 6Z SL1M^ L X Y D 66 LZ fyww 7 BG% S WGF T0 T f Yi^ w^5L^Df vWxw 6i i A1 X 1bbL M i
X 7 M iX b YMY W iL Y7 l Z x B i Y5 S Mx ZLfbM a S G S 00 ax ^LL6 Y BTf Y %T^ Wl b A Gyn 6n^DfSA L%86 0w y 6w r DX1L v f
S Y v fS 1 Xb % yL GY w x B k f Y^ Z bB xDAXv 7 Z T Y Y i 7B n110 X gW^ Y fWn %y s 6 TL1 01MS^Y6 afk0 L M6 5 SrwD L A
Z X L AZ w SX f LD TX & B k b A GM x Xk BS6R Y x w Y yk iD0i S 6n ^6i fL T M Wlf ifvYnYb 7^bi y0 l B0 M ^ Y56S 7 6
x S a 6x & Zr ^ lS WS 0 k b 1 6 Tv B r b kYMSA X B % LL Xb fSSY Z hfi nff ^l p b %DA yALYiGb Ynly Li D X1 X M Y^OY 7 a
B X Z 7 MB 0 x5 n DY %Z i b i w M WL k 51 bYb^7 S k f l1 SL 6YYL x b^f i^A nD G X fS6 L6aGfTX Xiwl ly S ry v M1Y Y X
k x Y bk i B^ i SY fx y 1 i 6 b %a b ^w LMXY Z b ^ DD Zw 6YVX x ^nA fn6 iS T r ^YM LM7TAWr Sf6L DL Y 5L L vyG X b
b B X Xb y kM f YG ^B L w 0 0 X f7 l M6 w rVX x 1 n SS x6 M GD @ A16 A1M fY W 5 nYb DbYw6%5 ZA0D SL Y ^l a LLT S r
l k S r1 L bv A YT nk l & h i r ^y w v0 & 5LS B w i YY B0 b TS F Tfm 6fb AY % ^ 1GX SXX^Mf^ x61S YD MD 7 aLW Z 5
w b Z 5w l 1L 6 GW 1b D 0 h y 5 nX & L1 0 ^aZ k & f Y Y k1 X WY l bAb MAX 6 f M fTr YrSfb^M BMyy YS vS Y 7D% x ^
6 l x ^6 D wa M T% f1 S i ^ L ^ iS 0 ay i M7x b 0 A G by r Y F 6X b6r M ^ v AW5 Y5Z^Xnv kbLY GY LY X Ysf B M
0 w B MO S 67 b Wf Aw Y Y A L M fZ i 7L y yVB 1 i 6 T l 5 fG A TMR XMS b n L 6%^ b^xnriL bXLY TY A Y S XY^ k v
i & k vi Y OY X % ^ 66 Y L T D v Ax y YL L L Xk w y M W wL ^ ^T t pb5 rb^ X i a MfM sMBi5fa 1rDT W 7G Z Svn b L
y 0 b Ly Y iX r fn MO l b 6L L d aSb & L b % 6D M nW q GX^ 5XM r f 7 b^v Tvkf^A7 w5SW % YT x Z6i 1 a
L i l aL G yS 5 ^1 b1 D s Y a Mk l SS D 721 0 l X f OS v 1% v TrM ^rv 5 A Y XnL pLbAM6Y 6^Y% f XW B xTf w 7
D l y w 7L T LZ ^ nf Xy S T Y Y b k D ZY S Yxw i D r ^ iY L f f & W5v MSL ^ 6 X r1a Ga16vMX OMVf ^ S% k BWA & Y
L Y & YD W lx M iA rL Y p G Y X S xY Y Xb6 y S 5 n yY A A^ y %L v^a M M S 5f7 T7wMLbS 1vG^ n Zf b k%6 0 X
S l 0 XS % DB v f6 5D Y G T X r Y BG Y Sk0 L Y ^ i L 7 6n u fMA LM7 v b Z ^AY WY&baXZ yLTn i x^ 1 bFM i S
Y L l i SY f Sk L AM ^1 G T W S 5 Y Y f l Y M1 l ^vY avY L X x M6X %X0X7rx LaWi f Bn w 1^b y Z
Y s y ZY ^ Yb a 6b MS T W % Z ^ G bw xly D v A D X bf ( nLY 7LX a r B vMS fS1rY5B 17%f A ki 6 wnX L x
G T L x n Y1 7 MX vY W % f x M T 1% BwL S L 6 S S XA M 1aX YaS 7 5 k LbZ ^2y5X^k DYfA 6 bf 0 61r l B
T p l b i Gw Y br LY % f ^ B v W wf k6L Y a M Y Z r 6 h f7S X7Z Y ^ b aXx nxL^SMb SX^6 M 1A i 01R 5 Dk
W G D k f T6 X X5 ah f ^ n k L % 6^ b0D Y 7 b Y x ^M i fYZ SYX X M 1 7rB iB1MZv1 YSnm b w6 y iA^ S b
% T S b A W0 S r^ 7B ^ n i b a f 0n 1iS Y X G B ^b h tXx ZXB S v w Y5k FkDvxLw bZib X 6M L y6M Y 1
```

Quellen

- <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf> - NIST
- <https://security.stackexchange.com/questions/3959/recommended-of-iterations-when-using-pbkdf2-sha256/>
- PBKDF2
- https://i.ytimg.com/vi/u6_E2ggMchs/maxresdefault.jpg - Image
- <https://specopssoft.com/wp-content/uploads/2021/05/Password-Entropy-of-Password-Policies-Formula.png>
- Image
- <https://www.okta.com/identity-101/password-entropy/> - Entropy
- <https://security.stackexchange.com/questions/92865/what-is-the-difference-between-a-hash-table-and-a-rainbow-table-and-how-are-the>
- Hash-Table vs Rainbow-Table