

ITS335 – User Authentication Notes

username	password
john	mysecret
sandy	ld9a%23f
daniel	mysecret
...	...
steve	h3lp_m3?

Figure 1: Password Storage - Cleartext password; Lecture 07

username	H(password)
john	06c219e5bc8378f3a8a3f83b4b7e4649
sandy	5fc2bb44573c7736badc8382b43fbae
daniel	06c219e5bc8378f3a8a3f83b4b7e4649
...	...
steve	75127c78fd791c3f92a086c59c71ece0

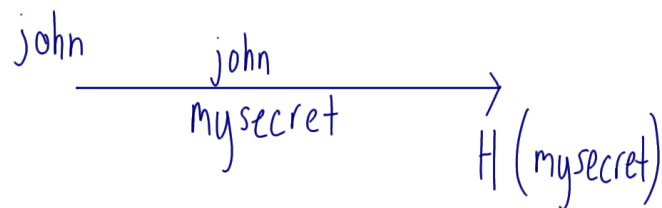


Figure 2: Password Storage - Hash of password and verification; Lecture 07

Brute force : 2^n
 n -bit hash
 MD5 128-bit hash
 2^{128} attempts
 10^9 /sec : 10^{21} years

Figure 3: Password Storage - Brute Force on One Way Hash; Lecture 07

8 char. : a-z, A-Z, 0-9, +32
 Possible passwords : 94^8

P_1	$H(P_1)$	10^{10} /sec
P_2	$H(P_2)$	
\vdots	\vdots	
P_{94^8}	$H(P_{94^8})$	

 ~ 7 days

Figure 4: Password Storage - Try all passwords; Lecture 07

94^8 entries
 Entry : password 8 B
 hash 16 B
 Size : 146,000 TB
 Rainbow table : 576 GB
 Lookup < 1 hour

Figure 5: Password Storage - Rainbow Table Summary; Lecture 08

username	salt	H(password salt)
john	a4H*1	ba586dcb7fe85064d7da80ea6361ddb6
sandy	U9(-f	816a425628d5dee17839fffeafb67144
daniel	5<as4	11842ced4203d4067ed6a6667f3f18d9
...
steve	LqM4^	184b7f9c6126c568ee50cd3364257973

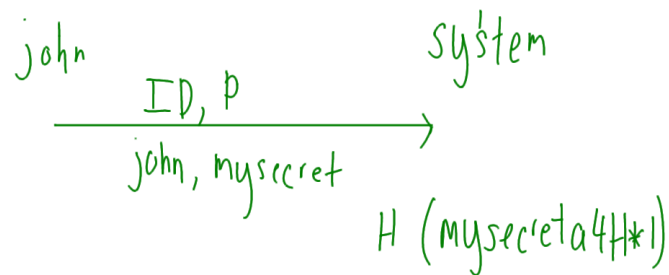


Figure 6: Password Storage - Salted Password; Lecture 08

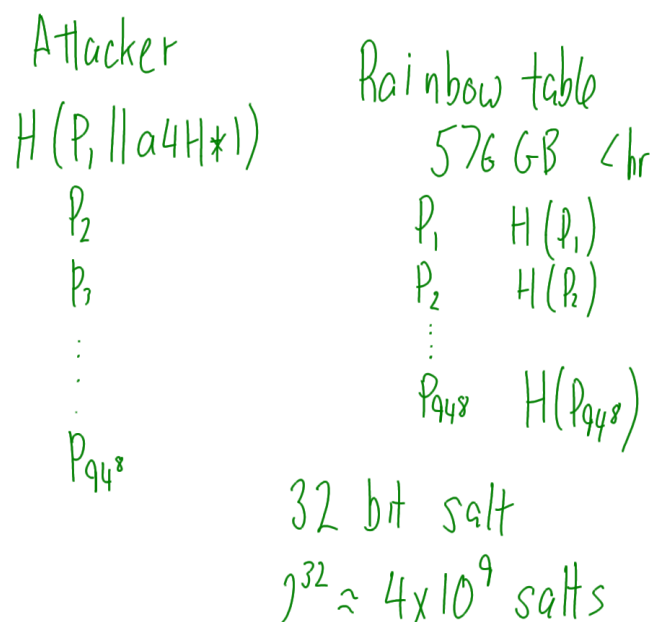


Figure 7: Password Storage - Salted Password and Rainbow Table; Lecture 08

[illegible]

$$2^6 = 64$$

Hash: SHA 512

Salt : 8 char, 48 bits

$$h = \text{SHA512}(\text{Password} \parallel \text{Salt})$$

h: 86 char, 512 bits

Figure 8: Linux Password Storage Example; Lecture 09