THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

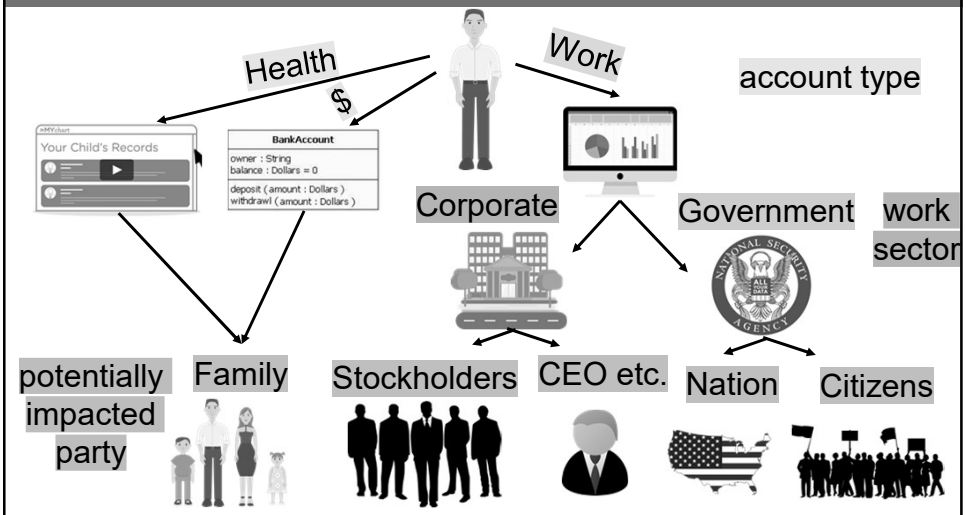
Password Security

Based on: D. Florêncio, C. Herley, and P. C. van Oorschot, “An Administrator’s Guide to Internet Password Research”, 28th Large Installation System Administration Conference, Nov. 2014.

1

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Impacts of Account Compromise



2

2

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Storage Schemes

- Plaintext / Reversibly Encrypted
- Hashing
- Hashing and Salting

3

3

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Password Storage Schemes: Plaintext

Storage in backend database

Username	Password
notSecureAtAll@hi.com	stupid

password entered: stupid

4

4

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Password Storage Schemes: Hashing

Problematic because of users who use the same password

`hash("password") =`
`2cf24dba5fb0a30e26e83b2ac5b9e29e1b161`
`e5c1fa7425e73043362938b9824`

Storage in backend database

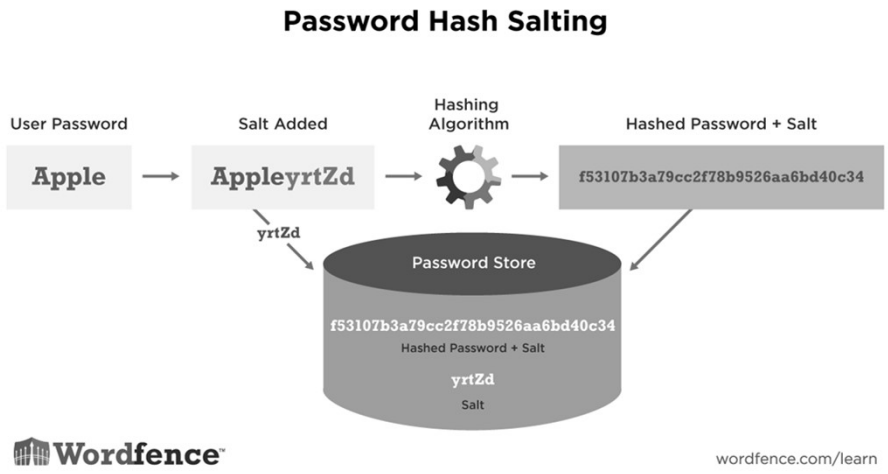
username	hashed password
user	**`2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824`**

5

5

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Password Storage Schemes: Hashing and Salting



6

6

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Clarification

As seen in the article:

Keyed hashing. Reversible encryption is one of the worst options for storing passwords if the decryption key leaks, but is among the best if a site can guarantee that it never leaks (even if the password file itself does). Justification for sites to store passwords reversibly encrypted is a need to support legacy protocols (see Section 3.5). Absent such legacy requirements, the best solution is salting and iterated hashing with a message authentication code (MAC) [37, 56] stored instead of a hash; password verification (and testing of guesses) is then impossible

ırge Installation System Administration Conference (LISA14) 43

Is any MAC suitable?

A PRF can be MACs, but not all MACs are PRFs

7

7

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Categorizing Accounts

Why is this important?

- recognition of the distinction raises awareness to highly sensitive accounts
- distribute user's (finite) effort according to priority of account

8

8

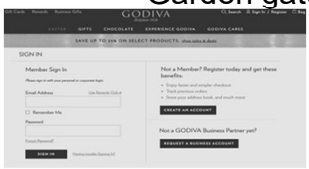
THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

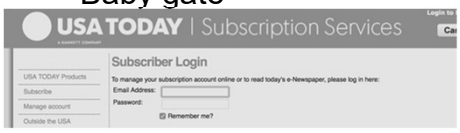
Category 0: Don't Care Accounts

One-time use accounts, nusicance accounts solely created to gain access to free articles, temporary subscriptions, etc

Garden gate

Baby gate





Seemingly innocuous if compromised, but problematic if same or similar password reused for higher category accounts

9

9

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Category 1: Low-Consequence Accounts

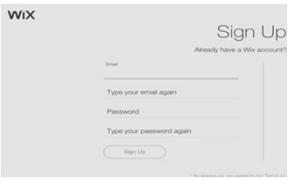
Accounts in which credit card details aren't stored, but may contain some personal information

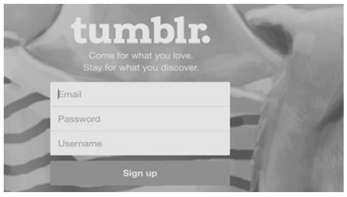
- E.g., rarely used social media sites or sites that allow users free access to some of the features

Screen door

Glass door

users often rely entirely on password recovery features





10

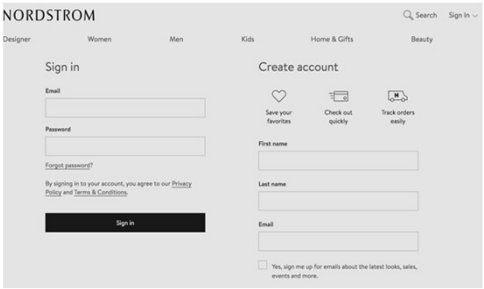
10

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Category 2: Medium-Consequence Accounts

Email accounts, online shopping sites that store credit card details

bedroom door lock



11

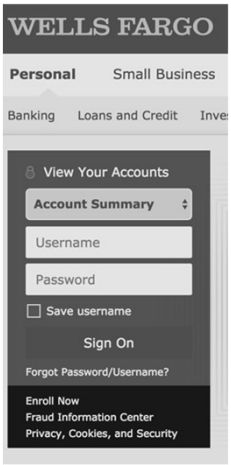
11

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Category 3: High-Consequence Accounts

Professional or primary email accounts, heavily used social media accounts, online banking accounts, access to corporate databases

dead-bolted door



12

12

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Category 3: High-Consequence Accounts

An overview of the security measures that can be taken

Implementation aspect	Attacks stopped or slowed	User impact	Remarks
Password stored non-plaintext	Full compromise on server breakin alone	None	Recommended
Salting (global and per-account)	Pre-computation attacks (table lookup)	None	Recommended
Iterated hashing	Slows offline guessing proportionally	None	Recommended
MAC of iterated, salted hash	Precludes offline guessing (requires key)	None	Best option (key management)
Rate-limiting & lockout policies	Hugely reduces online guessing	Possible user lockout	Recommended
Blacklisting (proactive checking)	Eliminates most-probable passwords	Minor for small lists	Recommended
Length rules	Slows down naive brute force attacks	Cognitive burden	Recommended: length ≥ 8
Password meters	Nudges users to "less guessable" passwords	Depends on user choice	Marginal gain
Password aging (expiration)	Limits ongoing attacker access; indirectly ameliorates password re-use	Significant; annoying	Possibly more harm than good
Character-set rules	May slow down naive brute-force attacks	Cognitive burden. Slows entry on mobile devices	Often bad return on user effort

13

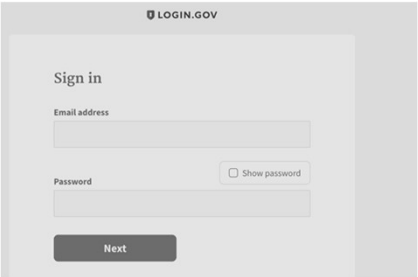
13

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Category 4: Ultra-Sensitive Accounts

Multi-million dollar irreversible banking transactions. Authorization to launch military weapons. Encryption of nation-state secrets.

vault



14

14

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Which Are of Interest Here?

Category 1, 2, 3

Category 0: very low risk

Category 4: likely (hopefully) rely on features that, unlike passwords, aren't dependent upon user effort, but may still be user dependent (e.g., biometrics)

15

15

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Attack Types

Offline and Online….. totally distinct and no middle ground

- Require very different resources
- Yield very different number of guesses and are susceptible to different defense strategies

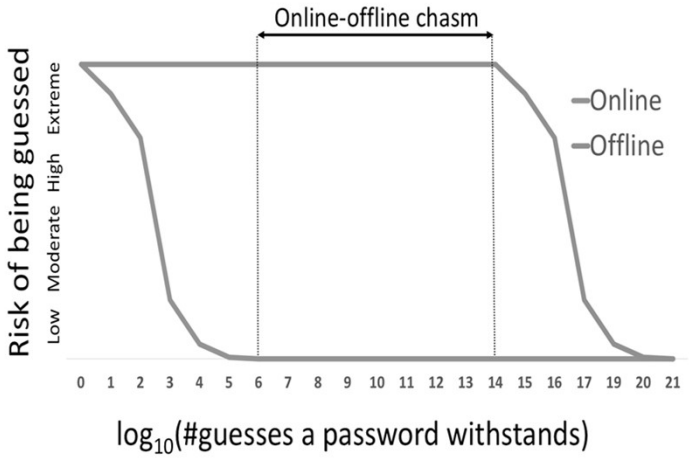
16

16

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Offline vs. Online Guessing Resistance

tincan24 and 7Qr&2M provide same security



17

17

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

What Does This Mean?

- Have passwords that can withstand online guessing, but don't worry about exceeding the threshold by much
- Passwords should withstand 10^6 guesses to be safe from online attacks
- Passwords should withstand 10^{14} guesses to be safe from offline attacks

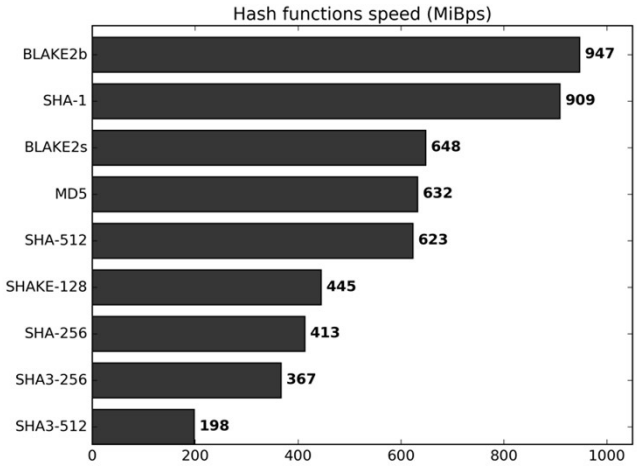
18

18

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Security Techniques (I)

Stretching of passwords to slow down brute-force attacks



19

19

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Security Techniques (II)

Password blacklists

1 -- 123456
2 -- 12345678
3 -- 123abc
4 -- a1b2c3
5 -- aaaaaa
6 -- abc123
7 -- abc123
8 -- abcdef
9 -- amanda
10 -- andrew
11 -- angel
12 -- asdfgh
13 -- august
14 -- avalon
15 -- bandit
16 -- barney
17 -- baseball
18 -- batman
19 -- biteme
20 -- brandy
21 -- buster
22 -- butthead
23 -- calvin
24 -- canada
25 -- changeme
26 -- chelsea
27 -- coffee
28 -- computer
29 -- cowboy
30 -- diamond
31 -- donald
32 -- dorothy
33 -- dragon
34 -- eeyore
35 -- falcon
36 -- fishing
37 -- football
38 -- freedom
39 -- f***me
40 -- f***you
41 -- gandalf
42 -- george
43 -- harley
44 -- hello
45 -- helpme
46 -- hockey
47 -- iloveyou
48 -- internet
49 -- jennifer
50 -- jonathan
51 -- jordan
52 -- letmein
53 -- maggie
54 -- marina
55 -- master
56 -- matthew
57 -- merlin
58 -- michael
59 -- michelle
60 -- mickey
61 -- mike
62 -- miller
63 -- molson
64 -- Monday
65 -- monday
66 -- monkey
67 -- mustang
68 -- natasha
69 -- ncc1701
70 -- newpass
71 -- newyork
72 -- pamela
73 -- password
74 -- patrick
75 -- pepper
76 -- piglet
77 -- poohbear
78 -- pookie
79 -- princess
80 -- qwerty
81 -- rabbit
82 -- rachel
83 -- ranger
84 -- rocket
85 -- secret
86 -- service
87 -- shadow
88 -- snoopy
89 -- soccer
90 -- sparky
91 -- spring
92 -- steven
93 -- success
94 -- summer
95 -- sunshine
96 -- thomas
97 -- tigger
98 -- trustno1
99 -- victoria
100 -- whatever
101 -- wizard
102 -- zapata
103 -- blackberry
104 -- blackberryid
105 -- bbidentity
106 -- playbook

20

20

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Security Techniques (III)

Password blacklists: Look for simple transformations of blacklist passwords, as well

letmein → Letmein!

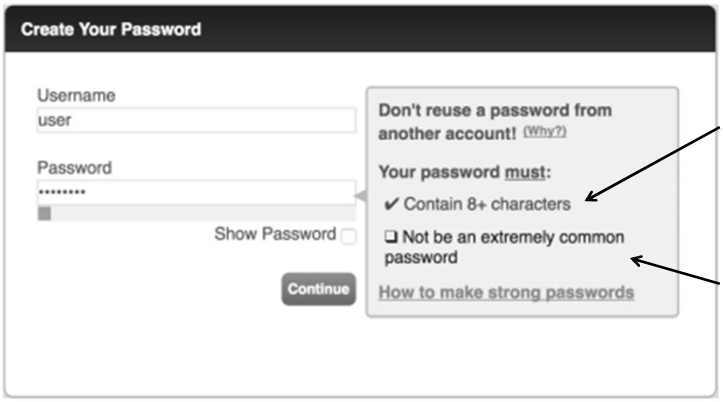
21

21

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Security Techniques (IV)

Password meters



"strength"

How is "extremely common" defined?

22

22

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Security Techniques (V)

Lockout policies

Challenges:
- Users locking themselves out, routinely
- Attackers locking out users

23

23

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Security Techniques (VI)

Include
- Fake accounts (“honey accounts”) or
- Fake passwords for real accounts (“honey passwords”)

in your site’s password database

Any access to a honey account or to a real account using a honey password suggests a password database breach

24

24

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Security Techniques (VII)

Password expiration

- Goal: Revoke access to an account by someone who compromised the password
- Reality: A large fraction of people modify their existing passwords in predictable ways

25

25

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Security Techniques (VIII)

- Two-factor authentication
- Second factor usually based on “something you have”
  - Email account
  - Phone
  - RSA SecureID key
  - …

26

26

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

References

"Authentication Cheat Sheet." Authentication Cheat Sheet - OWASP, www.owasp.org/index.php/Authentication_Cheat_Sheet#Use_of_authentication_protocols_that_require_no_password.

Encrypting Password Using md5() Function, www.phpeasystep.com/phptu/26.html.

"Fast Secure Hashing". BLAKE2. www.blake2.net/.

Florêncio, Dinei, and Cormac Herley. "An Administrator's Guide to Internet Password Research." Usenix, Microsoft Research, Paul C. Van Oorschot, Carleton University, 12 Nov. 2014, www.usenix.org/conference/lisa14/conference-program/presentation/florencio.

"Understanding Password Authentication & Password Cracking." Wordfence, 15 Feb. 2016, www.wordfence.com/learn/how-passwords-work-and-cracking-passwords/.