CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

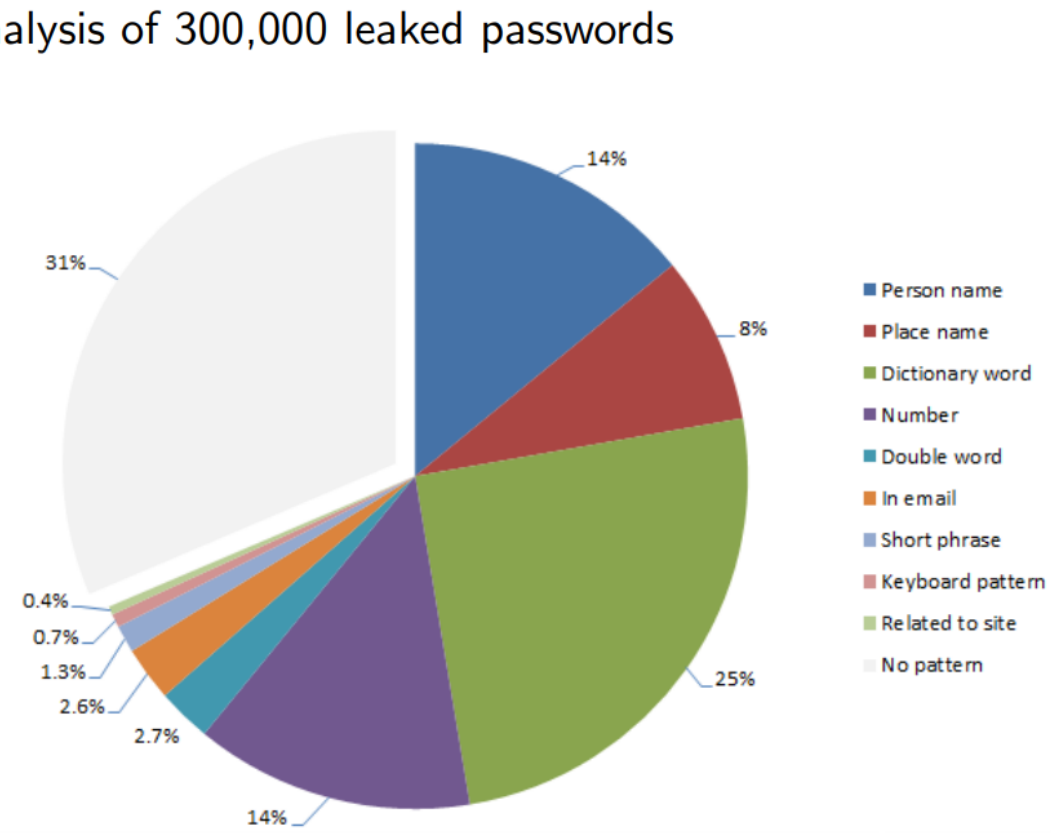
User Authentication, Access Control, and Operating System

Storing Passwords

Video Summary

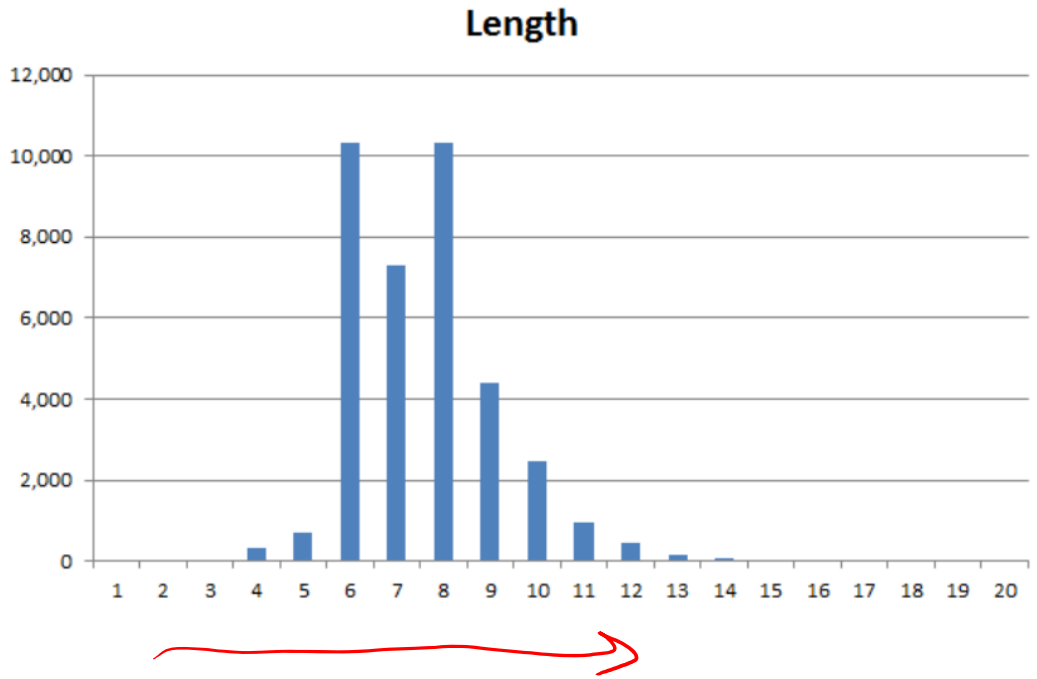
- How to Select A Password
- How to Store A Password
- Hashing Passwords

Selecting Passwords



How Long Are Passwords?

Analysis of 37,000 leaked passwords



Credit: Troy Hunt, *A brief Sony password analysis*, www.troyhunt.com, CCBY3.0

Other Common Characteristics of Passwords

poopoo
maximus
genius
cool
vampire
lacrosse
asd123
aaaa
christin
kimberly
speedy
sharon
carmen
111222
kristina
sammy
racing
ou812
sabrina
horses
0987654321
qwerty1
pimpin
baby
stalker
enigma
147147
star
poohbear
boobies
147258
simple
bollocks
12345q
marcus
brian
1987
qweasdzxc
drowssap
hahaha
caroline
barbara
dave
viper
drummer
action
einstein
bitches
genesis
hello1
scotty
friend
forest
010203

- Most use only alphanumeric characters
- Most are in (password) dictionaries
- Many users re-use passwords across systems
- Some very common passwords: 123456, password, 12345678, qwerty, abc123, letmein, iloveyou, . . .
- When forced to change passwords, most users change a single character

Storing Passwords

- Upon initial usage, user ID and password are registered with system
- ID, password (or information based on it), and optionally other user information stored on system, e.g. in file or database
- To access system, user submits ID and password, compared against stored values
- How should passwords be stored?

Storing Passwords

ID, P

Insider attack: normal user reads the database and learns other users passwords

- Countermeasure: access control on password database

Insider attack: admin user reads the database and learns other users passwords

- Countermeasure: none—admin users must be trusted!

Outsider attack: attacker gains unauthorised access to database and learns all passwords

- Countermeasure: do not store passwords in the clear

Encrypting Passwords

$$ID, E(K, P)$$

- Encrypted passwords are stored
- When user submits password, it is encrypted and compared to the stored value
- Drawback: Secret key, K, must be stored (on file or memory); if attacker can read database, then likely they can also read K

Hashing the Passwords

$$ID, H(P)$$

- Hashes of passwords are stored
- When user submits password, it is hashed and compared to the stored value
- Practical properties of hash functions:
  - Variable sized input; produce a fixed length, small output
  - No collisions
  - One-way function
- If attacker gains database, practically impossible to take a hash value and directly determine the original password

Hashing the Passwords

username	password
john	mysecret
sandy	ld9a%23f
daniel	mysecret
...	...
steve	h31p_m3?

Hashing the Passwords

username	password
john	mysecret
sandy	ld9a%23f
daniel	mysecret
...	...
steve	h31p_m3?

username	H(password)
john	06c219e5bc8378f3a8a3f83b4b7e4649
sandy	5fc2bb44573c7736badc8382b43fbeae
daniel	06c219e5bc8378f3a8a3f83b4b7e4649
...	...
steve	75127c78fd791c3f92a086c59c71ece0

Hash

Video Summary

- How to Select A Password
- How to Store A Password
- Hashing Passwords