

# User's behaviour on password selecting



Msc.Ing. Nertila Hoxha



## Content

- Passwords
- Basic password scheme
- Passwords Authentication
- Password Security
- Create a strong password
- Mechanisms to Defend Against Attacks

*Everything (well... a lot, anyway) you didn't know, or want to, but really actually need to.*

❖ <https://www.youtube.com/watch?v=sdpxdDzXfE>

## Passwords

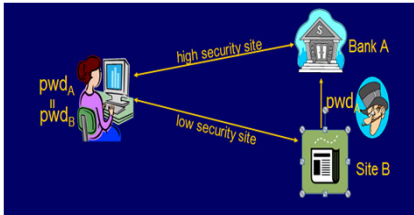
### What is a password?



Hello Caesar!  
You may not enter the coliseum without the correct password...

## Passwords

### Why Are They Important?



The diagram illustrates a user at a computer sending a password ( $pwd_A$ ) to Bank A, which is labeled as a 'high security site'. The user also sends a password ( $pwd_B$ ) to Site B, which is labeled as a 'low security site'. A third password ( $pwd$ ) is shown being sent from Site B to Bank A.

### Passwords

What they protect?

A cartoon illustration of a thief wearing a mask and a backpack, holding a laptop. Next to him is a computer keyboard, suggesting the theft of sensitive information like passwords.

### Basic password scheme

User Password file

kiwifruit

hash function

exrygbzyf  
kgnosfix  
ggjoklbsz  
...  
...

A diagram showing a user thinking of the password 'kiwifruit'. An arrow labeled 'hash function' points to a 'Password file' which contains the hashed versions: 'exrygbzyf', 'kgnosfix', 'ggjoklbsz', and two ellipses indicating more entries.

### Passwords Authentication

How do you prove to someone that you are who you claim to be?

"On the Internet, nobody knows you're a dog"

A cartoon illustration of a dog sitting at a desk with a computer monitor, looking at the screen. Below the illustration is the caption: "On the Internet, nobody knows you're a dog".

### Passwords Authentication

Authentication methods:

- What you know (Passwords, Secret keys)
- Where you are (IP Addresses)
- What you are (Biometrics)
- What you have (Secure tokens)

### Passwords Authentication

Does it matter if 2+ people use the same password?


Only if that same password is overly simple or obvious.

A screenshot of a game interface showing a top-down view of a character on a grid. At the bottom, there are five 'EMPTY' slots, each with a 'Capture' button and a red 'X' icon, suggesting a common password or action.

### Passwords Authentication


For the Pokemon Tower Defense game, 2000 accounts share the password of "pokemon." Though trivial in this case, matching application and password is an awful habit to develop.

A screenshot of the game 'Pokemon Tower Defense Generations' with the word 'HACKED' written in large red letters across the center. The game interface shows a tower defense setup on a grid.



### CONCERN: It's too easy to hack a password


This is true... but only IF the password is weak.



### Password Security

To protect your information:


- ❖ Use a STRONG password
- ❖ Keep your password safe
- ❖ Be smart when using the internet



### Create a strong password

Strong passwords:


- ❖ Are six characters or longer.
- ❖ Can't contain any part of a user's full name or username.
- ❖ Don't use any term that could easily be guessed by someone who is familiar with you.
- ❖ Should not include any personal information, e.g., the name of a spouse or a street address.



### Create a strong password

Strong passwords, cont.:


- ❖ Should not contain personal identification numbers, including those on a license plate, your telephone number, birth date, or any part of your Social Security number.
- ❖ Contain characters from three of the four classes of characters.



### Create a strong password


The four character classes are:

- ❖ English uppercase letters (A, B, C).
- ❖ English lowercase letters (a, b, c).
- ❖ Arabic numerals (1, 2, 3).
- ❖ Special characters ( !, \*, \$, or other punctuation symbols).




### Dictionary Attack

- Attacker can compute H(word) for every word in a dictionary and see if the result is in the password file
- With 1,000,000-word dictionary and assuming 10 guesses per second, brute-force online attack takes 50,000 seconds (14 hours) on average
  - This is very conservative; Offline attack is much faster!




❖ The length of a password is significantly more important factor from the point of view of security than the character types it consists of.

char set	length	Cracking time (rounded)
80	8	28 min
100	8	2.7 hours
80	10	124 days
80	16	10 <sup>11</sup> years



### Types of Password Cracking

- ❖ Dictionary Attack
  - Quick technique that tries every word in a specific dictionary
- ❖ Hybrid Attack
  - Adds numbers or symbols to the end of a word
- ❖ Brute Force Attack
  - Tries all combinations of letters, numbers & symbols
- ❖ Popular programs for Windows password cracking
  - LophCrack (discontinued by Symantec when acquired @stake)
  - Cain & Abel (UNIX)
  - John the Ripper (UNIX)
  - Sam Inside




### Examples of bad passwords

- ❖ Sports teams or terms: **LouvilleSlgr**
- ❖ Number sequence: **\*12345\***
- ❖ Letter string: **AAAAAA**
- ❖ Mixed-case sequence: **ABcdEFgh**
- ❖ Company name: **AcmeIT**
- ❖ Keyboard sequence: **QwERty** or **ASdFgh**




Variations on a theme are still weak

Original password:	Modified password:
▪ BobJones	▪ BJones25
▪ TechRepublic	▪ 1TechRepublic1
▪ Tiger	▪ Regit
▪ Login	▪ Log-in
▪ Password	▪ Always avoid this word or anything similar to it




### Better Password

Original password:	New password:
▪ LouvilleSlgr	▪ L*6v11E5Lgr
▪ AcmeIT	▪ aC&3i7
▪ QwERty	▪ Y7#RQ^e
▪ BJones25	▪ 890NEs2%
▪ 1TechRepublic1	▪ T3CH&R3pU8Lic




### Ten Common Mistakes

1. Leaving passwords blank or unchanged from default value.
2. Using the letters p-a-s-s-w-o-r-d as the password.
3. Using a favorite movie star name as the password.
4. Using a spouse's name as the password.
5. Using the same password for everything.
6. Writing passwords on post-it notes.
7. Pasting a list of passwords under the keyboard.
8. Storing all passwords in an Excel spreadsheet on a PDA or inserting passwords into a rolodex.
9. Writing all passwords in a personal diary/notebook.
10. Giving the password to someone who claims to be the system administrator



## IN A WORLD...

Where you don't have any access to your online life, how would you cope? What would you miss the most?




## Recent Major Security Breaches


Lulz Security hacks Sony Pictures website  
Releases 50,00 users' information

Rogue members of hacker-collective Anonymous hack Playstation Network and Quirioicity  
All user information made available

LulzSec strikes Sony again with and exploit of the PSN password reset solution URL  
Prevents owner of account from fixing prior hack




LulzSec logo




So... What can I do to make sure my information is safe?

In the case of the URL exploit and sonypictures.com hacks, very little

- These were simple errors made by Sony techs; a (technologically speaking) basic error was made in each case.




- ❖ Anything involving the internet is inherently more risky than anything not leaving your computer.
- ❖ Passwords are the front line of defense.
- ❖ Most people's are not strong enough to withstand a brute-force database attack; today we are going to look at how best to strengthen our passwords




## Issues to Consider in Password Systems

- ❖ Which types of attacks to defend against?
  - targeted attack on one account
  - attempt to penetrate any account on a system
  - attempt to penetrate any account on any system
  - service denial attack
- ❖ Whether to protect users against each other?
- ❖ Can users be trained? Will they follow the suggestions?
- ❖ Will the passwords be used in other systems?
- ❖ Whether the passwords will be used in a controlled environment



## Mechanisms to Defend Against Dictionary and Guessing Attacks

- **Protect stored passwords (use both cryptography & access control)**
- **Disable accounts with multiple failed attempts**



### Mechanisms to Avoid Weak Passwords

- ❖ Allow long passphrases
- ❖ Randomly generate passwords
- ❖ Check the quality of user-selected passwords
  - use a number of rules
  - run dictionary attack tools
- ❖ Give user suggestions/guidelines in choosing passwords
  - e.g., think of a sentence and select letters from it, "It's 12 noon and I am hungry" => "T1S12&IAH"
  - Using both letter, numbers, and special characters
- ❖ Mandate password expiration
- ❖ Things to remember: Usability issues

### Mechanisms to Defend Against Login Spoofing: Trusted Path

Attacks:

- write a program showing a login window on screen and record the passwords
- put su in current directory

Defense: Trusted Path

- Mechanism that provides confidence that the user is communicating with what the real server (typically Trusted Computing Base in OSes)
  - attackers can't intercept or modify whatever information is being communicated.
  - defends attacks such as fake login programs
- Example: Ctrl+Alt+Del for log in on Windows


### Defending Against Other Threats

Use ideas from recent research:

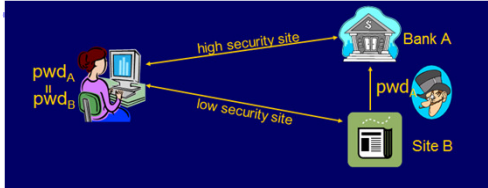
- graphical passwords,
- combine with typing

Go beyond passwords

- security tokens
- biometrics
- 2-factor authentication
  - US Banks are required to use 2-factor authentication by end of 2006 for online banking

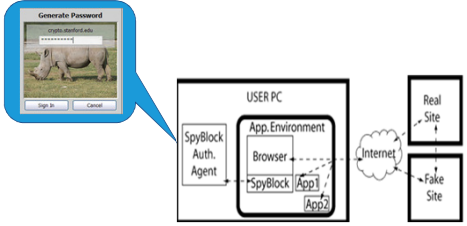


### Common Password Problem

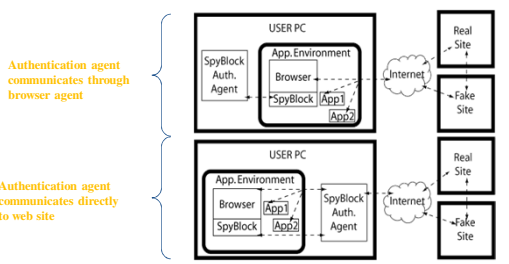


- ❖ Phishing attack or break-in at site B reveals pwd at A
  - Server-side solutions will not keep pwd safe
  - Solution: Strengthen with client-side support

### Defense: SpyBlock



### Defense: SpyBlock



### SpyBlock protection

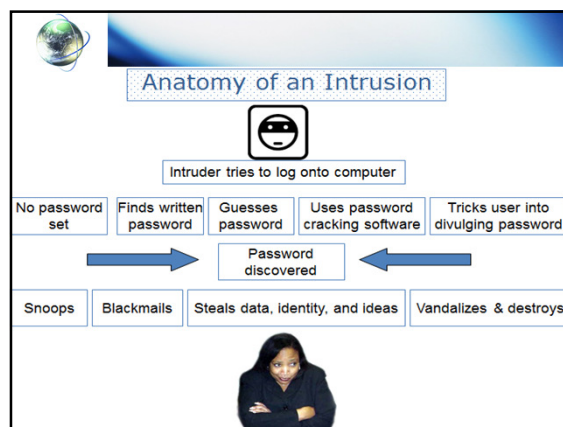
	Hashing	Injection	Hashing + Injection	HTTP Strong Pwd Auth	HTTPS Strong Pwd Auth	Transaction Confirmation
Common password						
Phishing	✓		✓	✓	✓	✓
Spyware keylogger		✓	✓	✓	✓	✓
Password sniffing				✓	✓	✓
Cookie stuffing					✓	✓
Pharming					✓	✓
Spyware session hijacker					✓	✓

password in trusted client environment

better password-based authentication protocols

trusted environment confirms site transactions


server support required



- ### Password
- #### How Are Passwords Stored? – Windows NT/2k/XP/Vista
- ❖ Uses 2 functions for “hashing” passwords:
    1. LAN Manager hash (LM hash)
      - Password is padded with zeros until there are 14 characters.
      - It is then converted to uppercase and split into two 7-character pieces
      - Each half is encrypted using an 8-byte DES (data encryption standard) key
      - Result is combined into a 16-byte, one way hash value
    2. NT hash (NT hash)
      - Converts password to Unicode and uses MD4 hash algorithm to obtain a 16-byte value

- ### Password
- #### ❖ How Are Passwords Stored? – Windows NT/2k/XP/Vista
- ❖ Hashes stored in Security Accounts Manager (SAM)
    - Locked within system kernel when system is running.
    - Location - C:\WINNT\SYSTEM32\CONFIG
  - ❖ SYSKEY
    - Utility which moves the encryption key for the SAM database off of the computer





### Conclusion

- ❖ A password is the key to your organization's resources.
- ❖ A strong password can protect your personal account.
- ❖ Take strides to make strong passwords that are not obvious to someone familiar with you.
- ❖ Remember to change your password on a regular basis.

# Thank you!

