ENTROPHY

30/1/2016

David Marciel
Pariente

PROBLEM

Today many threats made easy get your password while typing it.

Current devices make it easy to find out personal passwords due to the fixed position of characters in the screen/keyboard

PRODUCT | ACTUAL

Example:

- Alice uses her credit card in a cash machine
- A thief (Bob) has placed a camera and a card reader at the cash machine.
- When Alice uses her password, the camera will record it. The same will happen with her credit card, so Bob will know her credentials.
- From that moment on Bob could use her credentials as he wants.
- Alice knows the situation can happen and she feels unsafe.

PRODUCT | ACTUAL

Example 2:

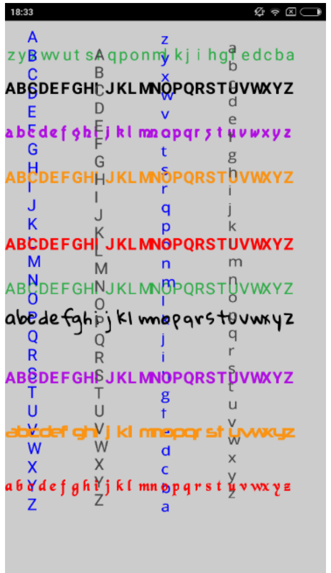
- Alice uses her mobile phone/computer and connects to her bank account. She writes her password while Bob is present.
- Bob takes advantage of the situation and spies her password.
- Bob takes control of Alice account.

The same will happen if Alice uses the Dataphone at Bob’s shop.

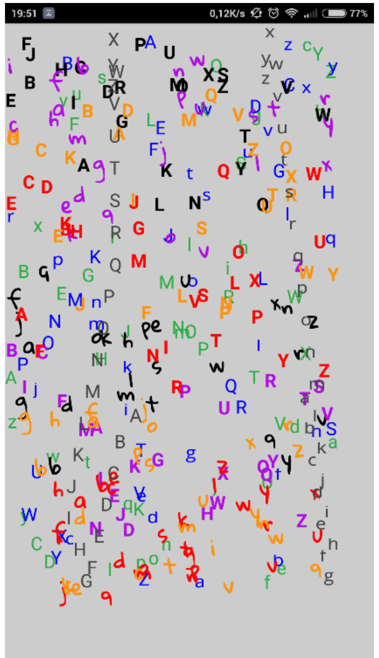
And it happens just because we can not crypt passwords given by a user to a server.

The first node (dataphone/mobile phone) always gets the information unencrypted.

PRODUCT | ENTROPHY

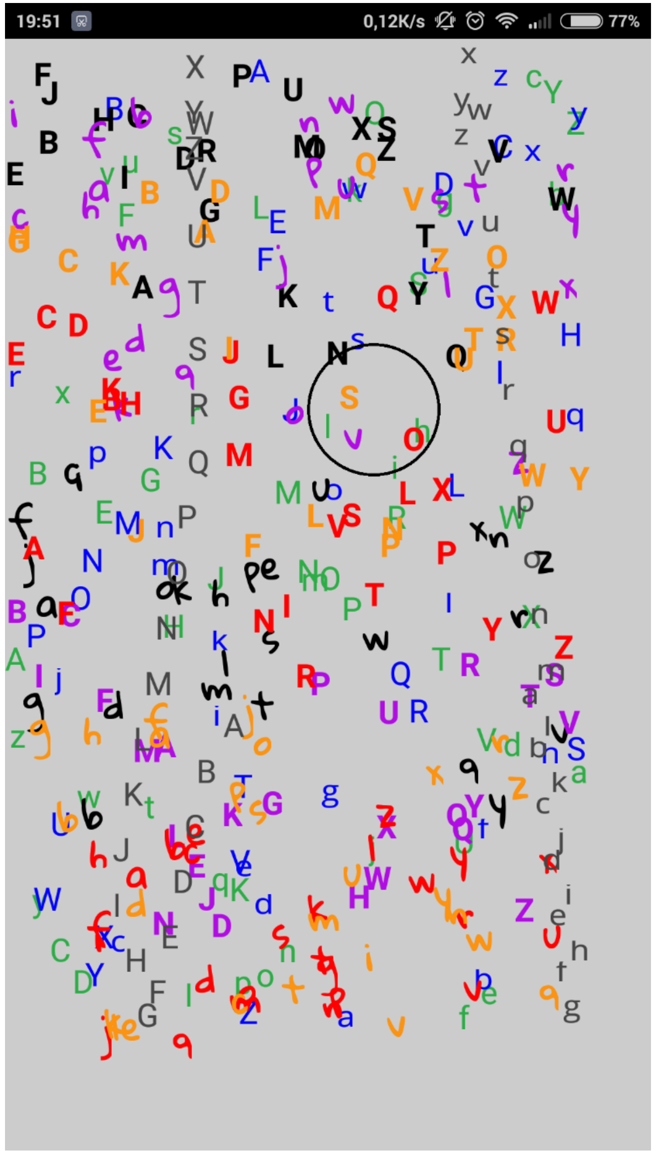


1



2

3



How it works:

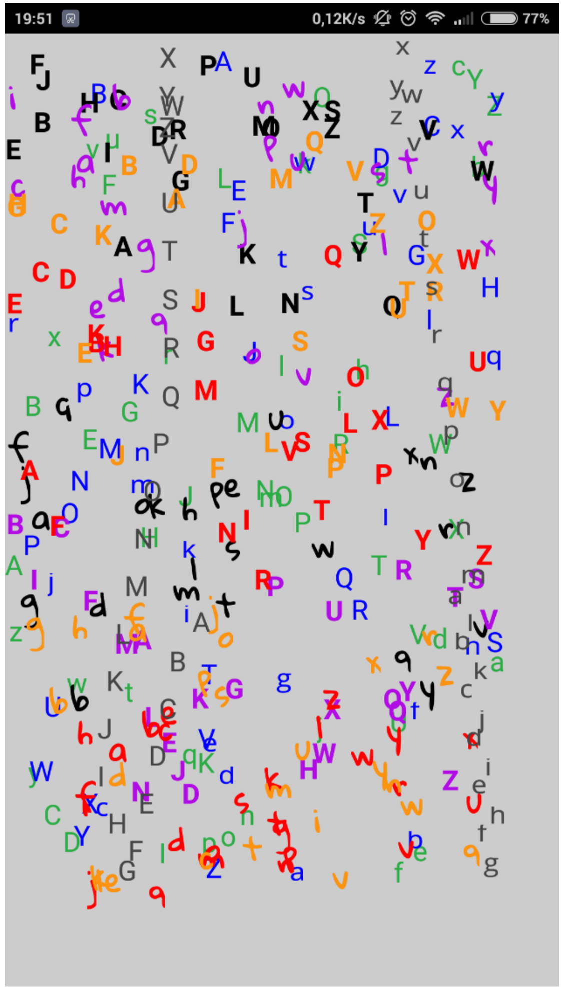
- Sorted information is shown in the screen (image 1).
- After touching the screen, the letters start to shuffle (image 2).
- Now you have to **press on your password letters.** For example, if our first password letter is a yellow “S” you would press near to the yellow “S” location.
- Any letter close to the place we have pressed is a **solution candidate** (image 3).
- If each candidate collection contains the solution letter for it’s position, the user gets authorization.

In this way we get some random passwords (in addition to our real one).
Observers (people, hackers and cameras) aren´t able to know which is the right one.

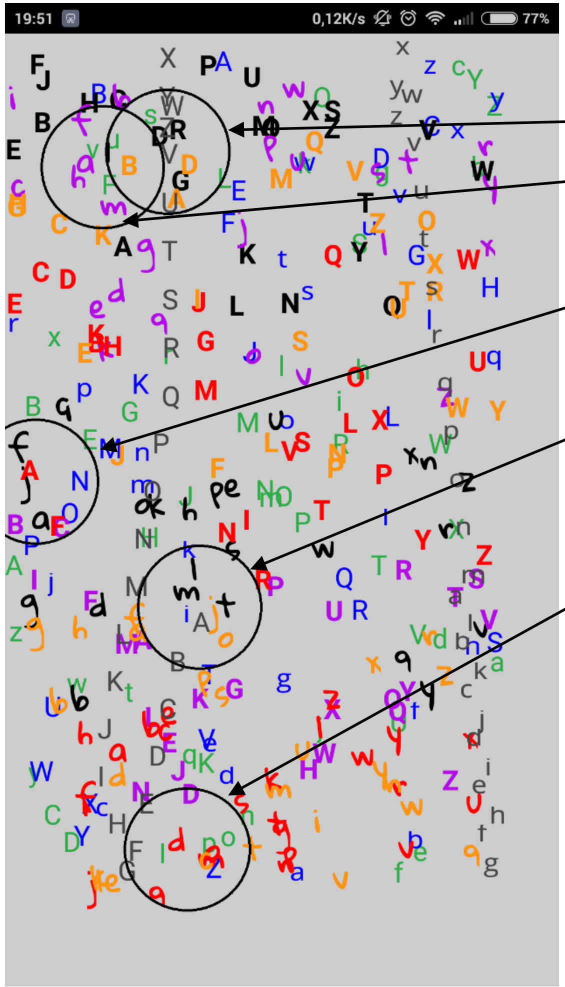
PRODUCT | ENTROPHY

1 Choose your password:

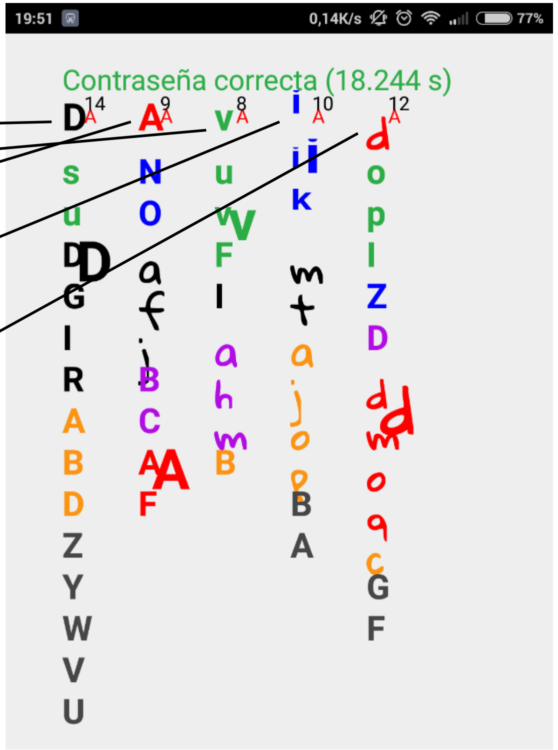
2 Program shuffles the letters:



3 Press on you password letters (in order)



4 System gets the following information:

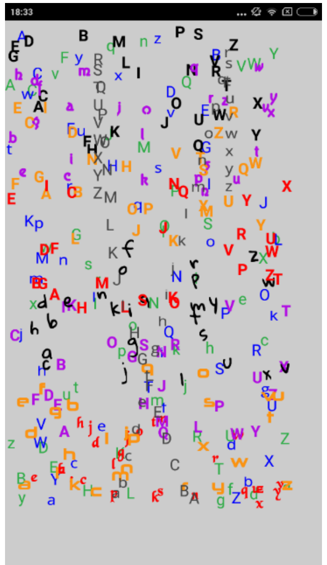


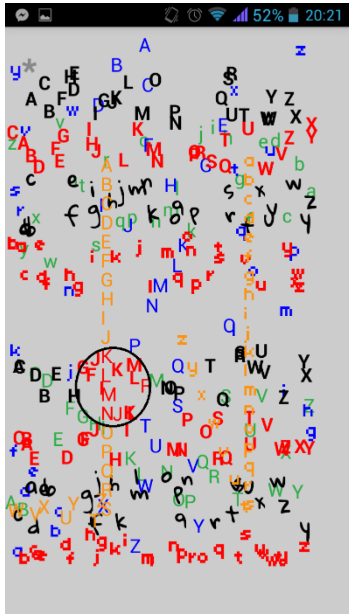
Contraseña correcta (18.244 s)

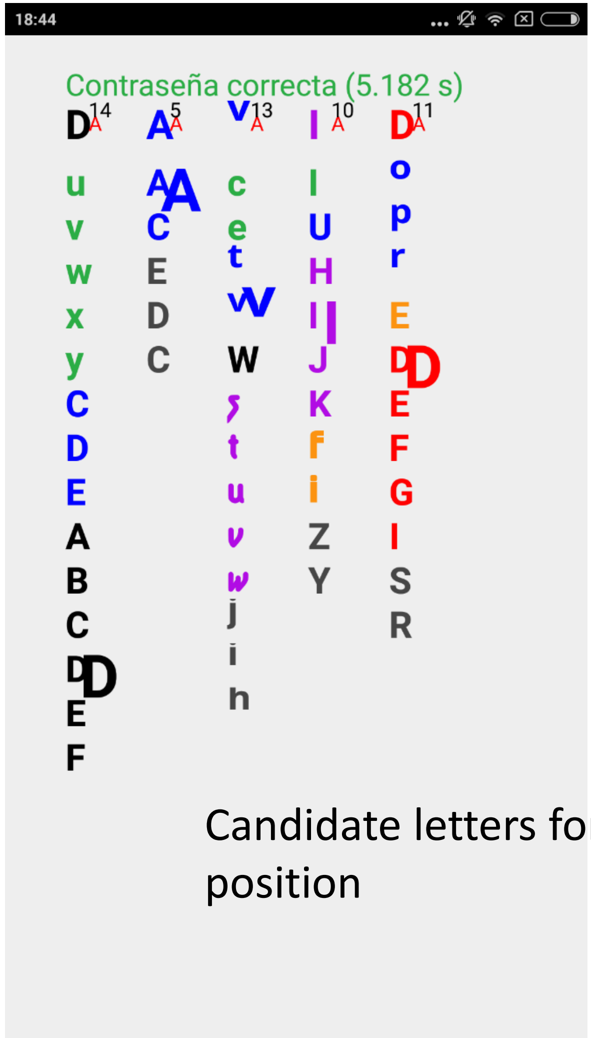
5 System response:

Acceso concedido. (18.244 s)

PRODUCT | ENTROPHY







Contraseña correcta (5.182 s)

Candidate letters for each position

Example:

- Alice uses her credit card in a cash machine
- In that cash machine Bob has placed a camera and a card reader.
- When Alice uses the cash machine Bob gets her password and her credit card information.
- Bob will try to write Alice’s password but **he wont know wich one is** (14*5*13*10*11 = 100.100 possible combinations)
- Bob doesn’t know Alice’s password
- **Alice knows it and she feels safe.**

Attackers don’t see a single password
But just a single one is valid

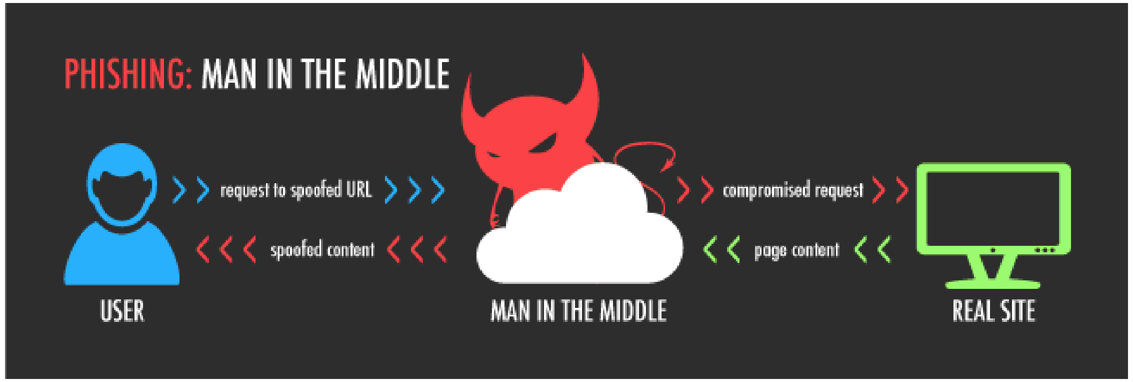
ENTROPHY | TECNOLOGY

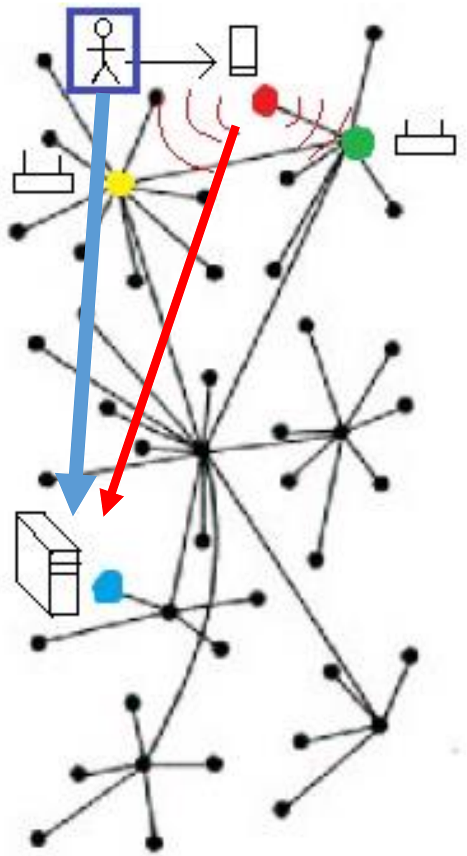
Entrophy prevents outside observers from finding out our password.

Even if someone observes Alice writing her password and gets all the information (by recording her, hacking her information or modifying the dataphone) her password would remain safe and the observer would have no chance observe again the same keystrokes.

Encryption happens in the head of the user not in the device

Preventing password theft
even if we are hacked or recorded





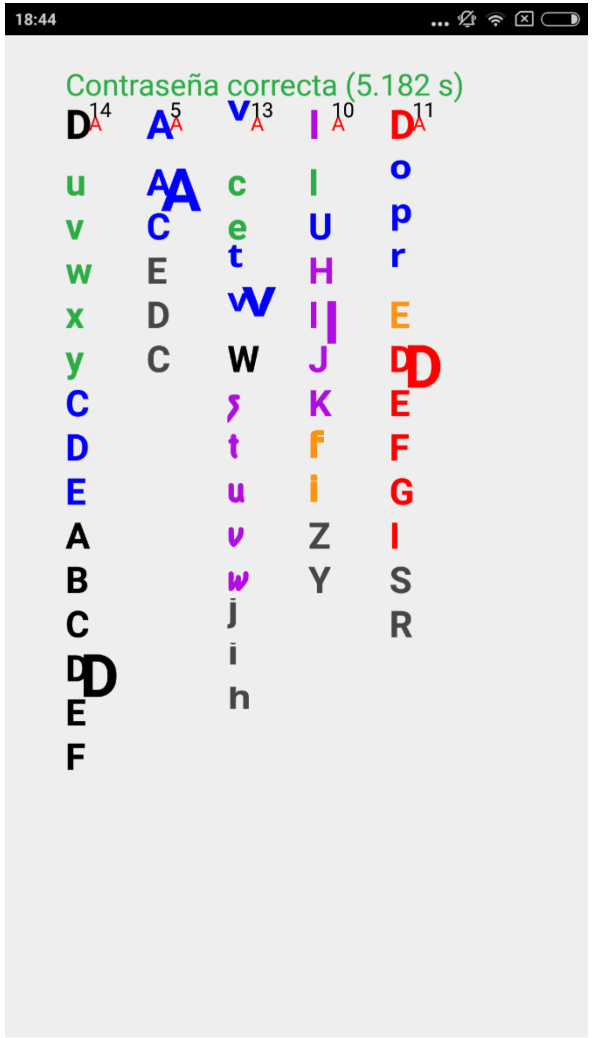
ENTROPHY | TECNOLOGY

The program is **full customizable**, you can change the number of alphabets, colors, fonts, waiting times, letters in the password… **Everything is as customer preferences.**

Dynamic mode (the one used in the presentation) contains 378 letters and the average number of candidate letters is 11.77

There are **more than 34.000.000** total possible combinations, and in case you are been spied there are still too many possible combinations **(around 100.000)**

Even when the communication is known brute forcé attacks are inviables.



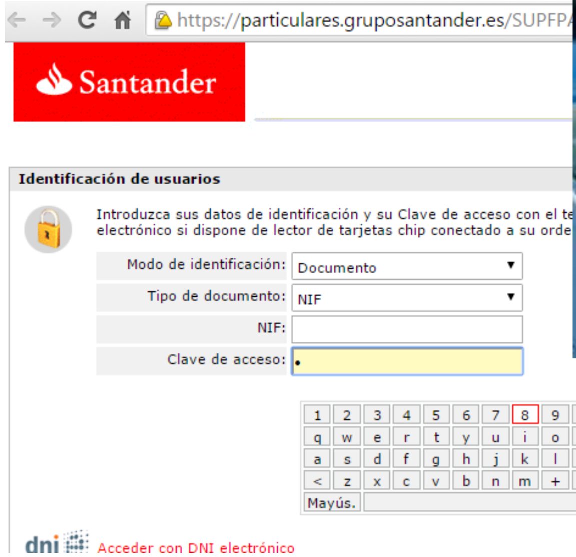
18:44

Contraseña correcta (5.182 s)

D 14 u v w x y C D E A B C D D E F
A 5 A A C E D C
V 13 c e t w W ş t u v w j i h
I 10 I U H I I J K f i Z Y
D 11 o p r E D D E F G I S R

BUSINESS APPLICATIONS

Increase your perceived security while **increasing your real security**



https://particulares.gruposantander.es/SUPFP
Santander

Identificación de usuarios

Introduzca sus datos de identificación y su Clave de acceso con el te
electrónico si dispone de lector de tarjetas chip conectado a su orde

Modo de identificación: Documento

Tipo de documento: NIF

NIF:

Clave de acceso: •

1 2 3 4 5 6 7 8 9 0 Borrar
q w e r t y u i o p ` +
a s d f g h j k l ñ ´ ç
< z x c v b n m + . -
Mayús. Mayús.
dni
Acceder con DNI electrónico

Nowadays there are no competitor products using **Entrophy advantages.**

- It prevents "Shoulder surfing"
- **It prevents the insecurity of been recorded**
- It offers human-server instead client-server encryption
- It does not reveal passwords
- It makes imposible to repeat previous observations
- **Clients won't feel unsafe anymore**

It can be used in cash machines, dataphones, mobile devices and any other haptic screen

CONTACT

David Marciel Pariente
Tlf: 616980969
davidmarciel@hotmail.com

https://es.linkedin.com/pub/david-marciel/1b/805/803