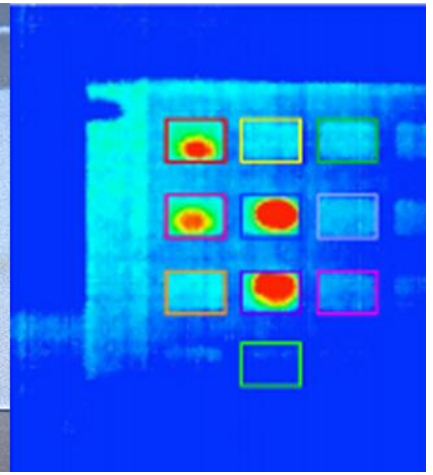
ENTROPHY

30/1/2016

David Marciel
Pariente

PROBLEMA



Actualmente existen muchos riesgos que hacen que el robo de contraseñas sea fácil cuando somos grabados tecleándolo.

Con los dispositivos actuales es fácil averiguar la contraseña debido a la disposición fija de los caracteres en el teclado/pantalla.

PRODUCTO | ACTUAL

Caso Práctico:

- Paco utiliza su tarjeta e un cajero
- En ese cajero un ladrón (Juan) ha colocado una cámara y un lector de tarjetas.
- En el momento en el que Paco introduzca su contraseña ésta será grabada por la cámara de Juan y éste la conocerá. Lo mismo pasará con su tarjeta.
- A partir de ese momento Juan podrá utilizar esta información para lo que desee.
- Paco lo sabe y se siente inseguro

PRODUCTO | ACTUAL

Caso Práctico:

- Paco utiliza su teléfono móvil/ordenador para ver su información bancaria e introduce su clave en presencia de Juan
- Juan aprovecha la confianza de Paco para averiguar su contraseña
- Juan obtiene control de las cuentas de Paco

Lo mismo pasaría si Paco utiliza un datáfono modificado en la tienda de Juan

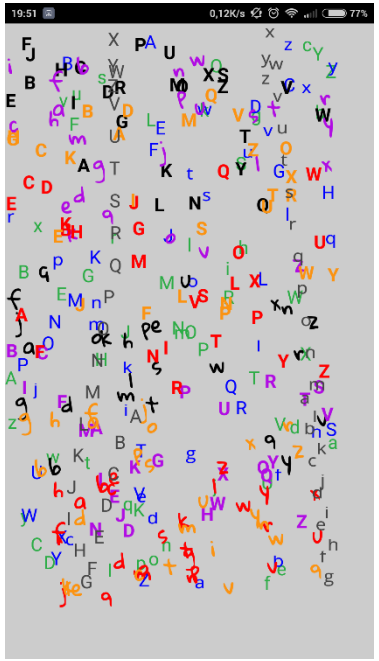
Y es que, no existe una forma efectiva de encriptar las contraseñas entre un usuario y un ordenador

El primer nodo (datafono/móvil) siempre recibe la información sin codificar.

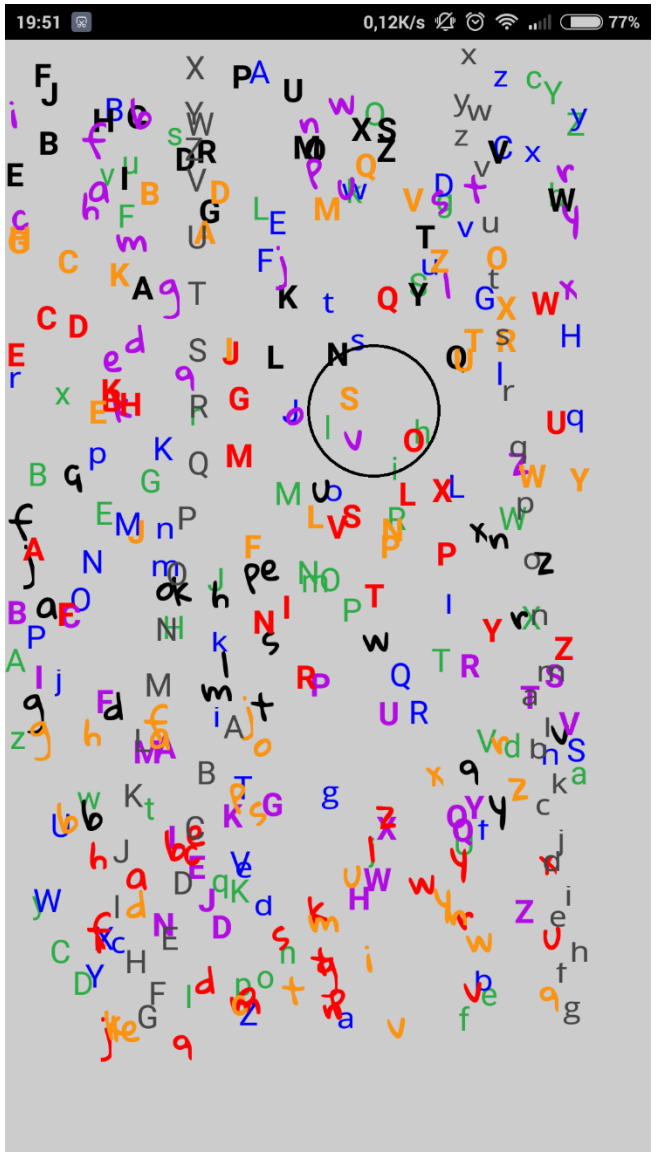
PRODUCTO | ENTROPHY

1

2



3



Como funciona:

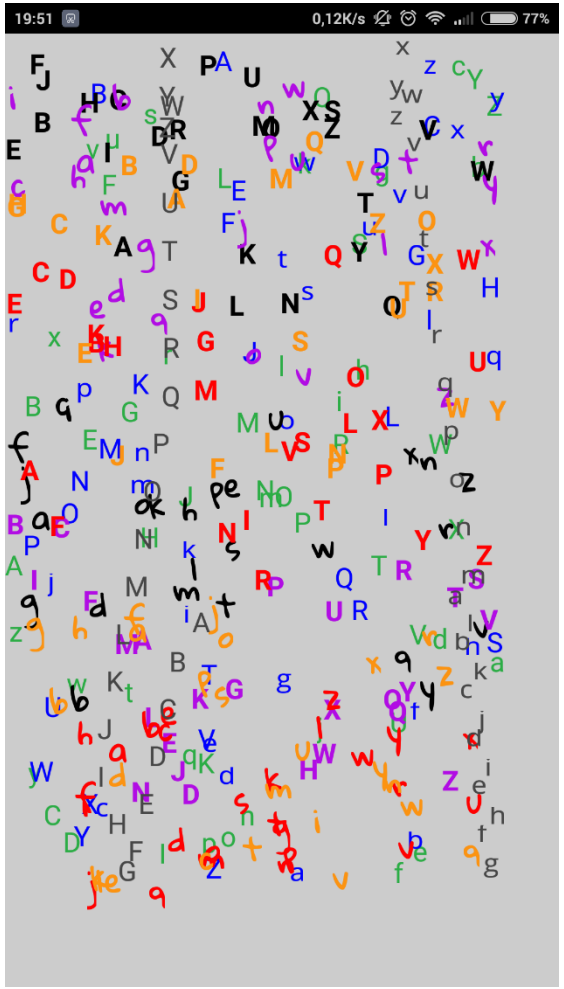
- La pantalla inicial muestra la información ordenada (imagen 1).
- Al pulsar sobre ella las letras empiezan a barajarse (imagen 2).
- Ahora tenemos que **pulsar cerca de las letras que forman nuestra contraseña**, por ejemplo si la primera es “S” amarilla pulsaremos cerca de donde se encuentre la “S” amarilla.
- Todas **las letras cercanas** al lugar pulsado se consideran **candidatas a solución** (imagen 3 derecha).
- Si todos los conjuntos candidatos contienen las letras solución el usuario será autorizado, en caso contrario no.

Así conseguimos varias contraseñas aleatorias (además de la nuestra).
Los observadores **(personas, cámaras y hakers) no saben cual de todas es la válida**.

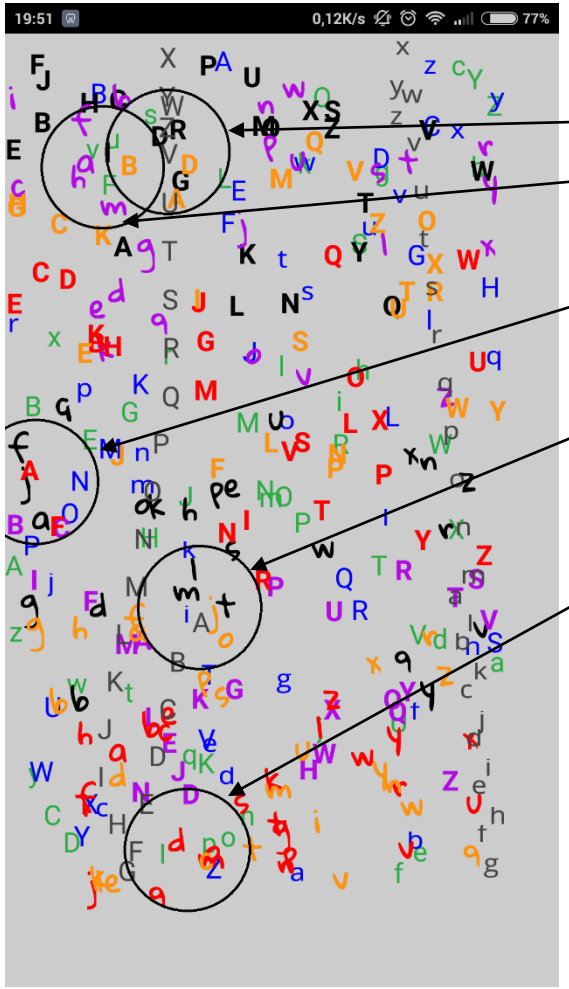
PRODUCTO | ENTROPHY

1 Elegimos la clave: **DAvid**

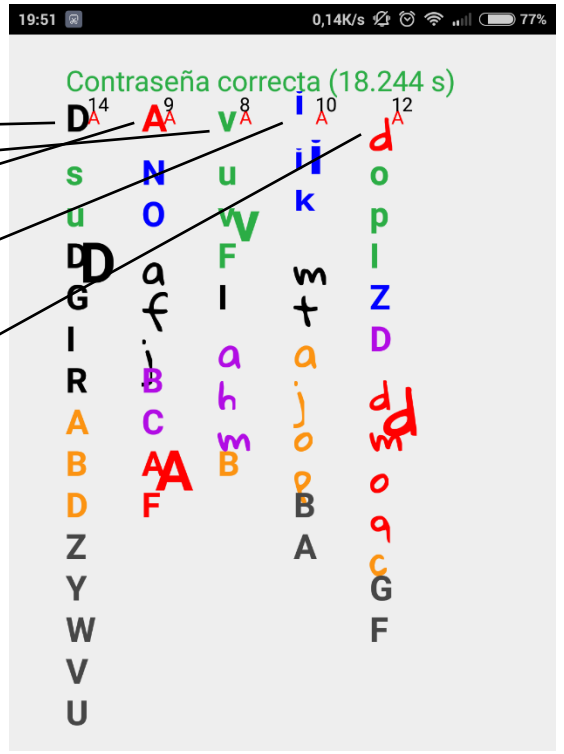
2 El programa baraja las letras:



3 Pulso sobre las letras de mi clave (en orden)

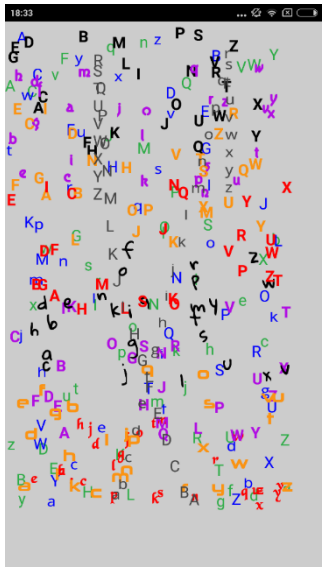


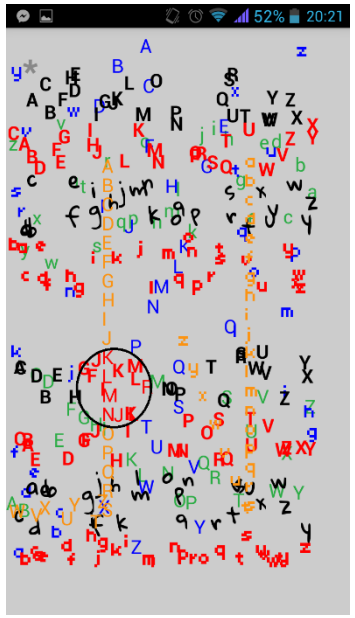
4 El sistema recibe la siguiente información:



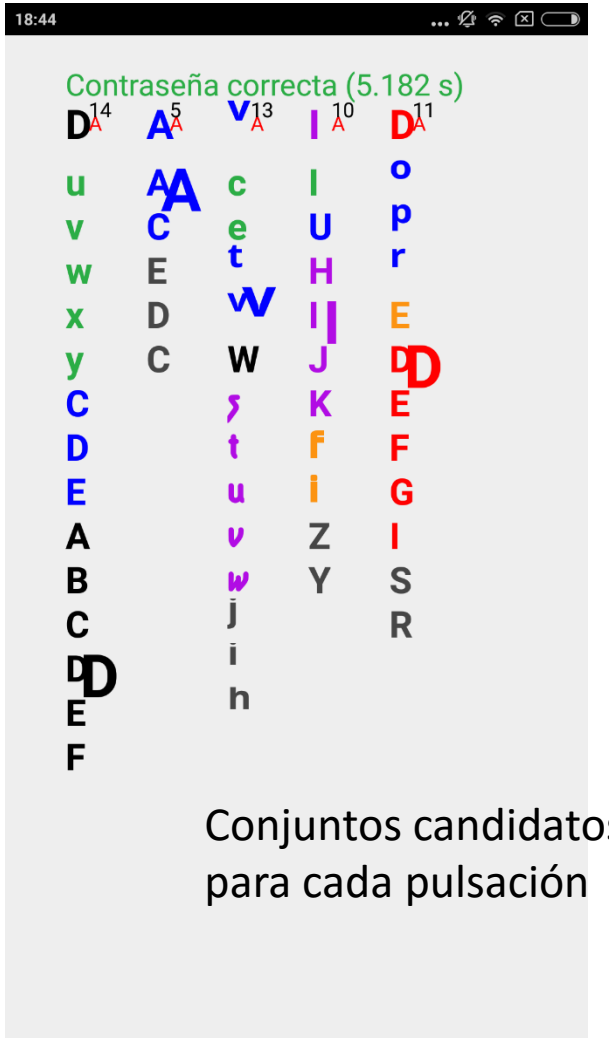
5 Respuesta del sistema:

Acceso concedido. (18.244 s)





PRODUCTO | ENTROPHY



Conjuntos candidatos para cada pulsación

Caso Práctico:

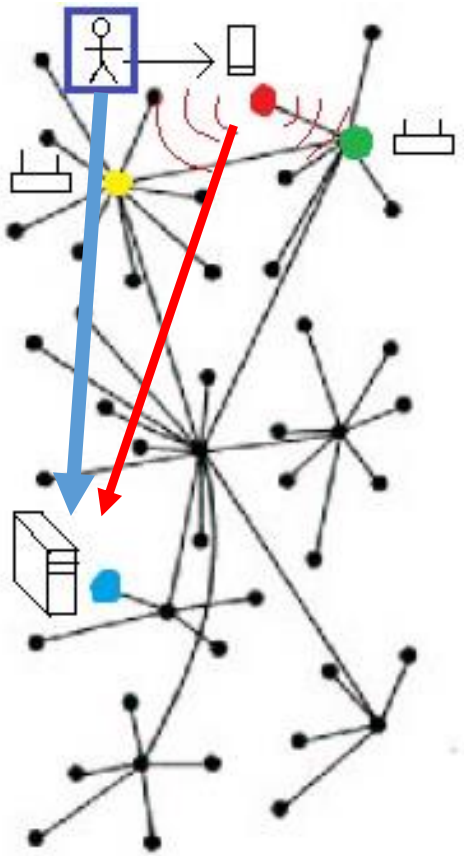
- Paco utiliza su tarjeta e un cajero
- En ese cajero un ladrón (Juan) ha colocado una cámara y un lector de tarjetas.
- En el momento en el que Paco introduzca su contraseña esta será grabada por la cámara de Juan, lo mismo pasará con su tarjeta.
- Juan intentará reproducir la contraseña de Paco pero **no sabrá cual de las 100.000 posibilidades es.** (14*5*13*10*11 = 100.100 posibles combinaciones)
- Juan no conoce la contraseña
- **Paco lo sabe y se siente seguro**

Los atacantes no ven una sola contraseña
Pero solo una es válida

ENTROPHY | TECNOLOGÍA

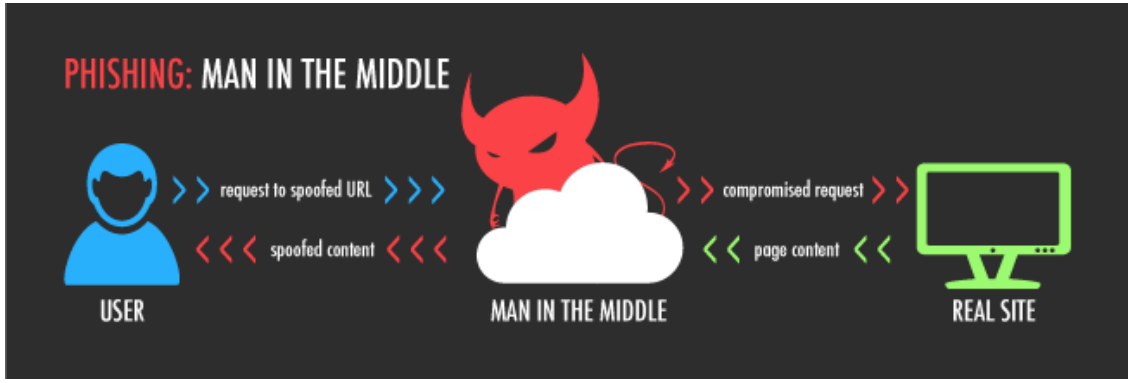
Entrophy evita que los observadores externos averigüen nuestra contraseña.

Aunque alguien observe a Paco introducir su contraseña y consiga toda la información (grabándolo, hackeando la información o modificando el datafono) no conseguiría la contraseña ni tendría capacidad de reproducir las pulsaciones observadas.



La encriptación sucede en la cabeza del usuario
y no entre dos dispositivos

Impedimos el robo de contraseñas
incluso **en caso de ser grabados o hackeados**



ENTROPHY | TECNOLOGÍA

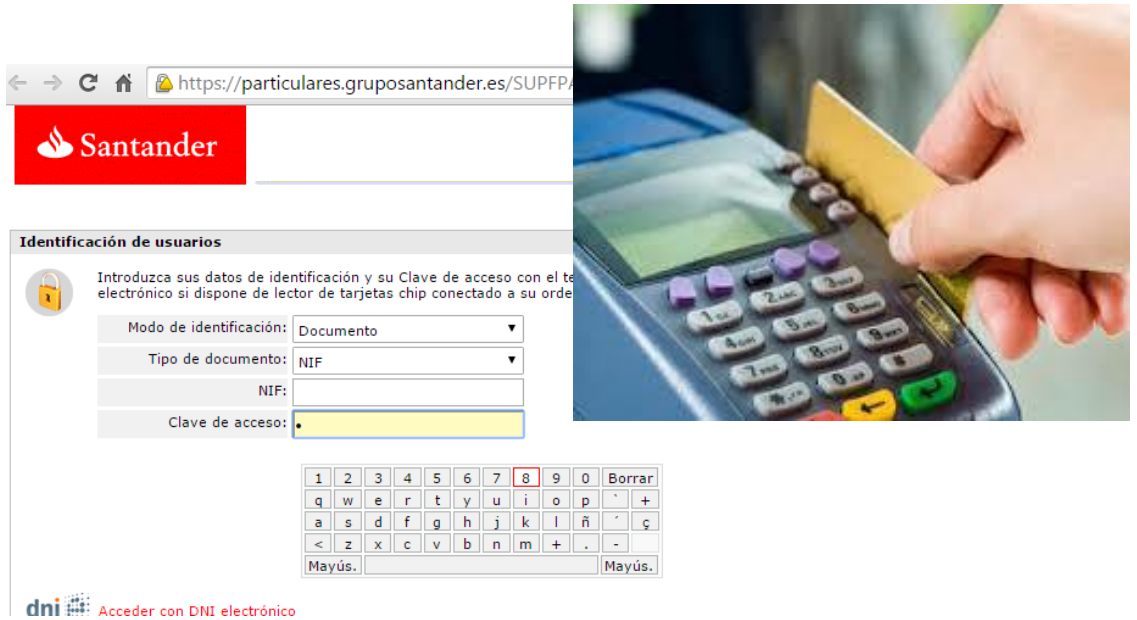
El programa es **completamente customizable**. Se pueden poner tantos alfabetos como se quiera, del color y fuente deseados, modificar los tiempos de espera, el numero de letras en la contraseña… todo es **a gusto del cliente**.

Las pantallas utilizadas como ejemplo tienen 378 letras y la media de letras candidatas por pulsación es de 11,77.

El número de posibles combinaciones es de más de **34.000.000** sobre el total, y en el caso de ser espiado mientras se teclea seguirán existiendo demasiadas combinaciones como para probarlas todas (en torno a **100.000**)

Aún conociendo la comunicación los ataques de fuerza bruta son inviables.

POSIBILIDADES DE NEGOCIO



Actualmente no hay productos competidores que exploten las **ventajas de Entrophy.**

- Evita el “shoulder surfing” (miradas indiscretas)
- **Evita la inseguridad al ser grabado**
- Encriptado humano-Servidor en vez del cliente-servidor
- No revela la clave
- No permite reproducir las observaciones previas
- **Los clientes ya no se sentirán inseguros usando sus cajeros**

Aplicación en cajeros, datafonos, dispositivos móviles y cualquier pantalla táctil

CONTACTO

David Marciel Pariente
Tlf: 616980969
davidmarciel@hotmail.com

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