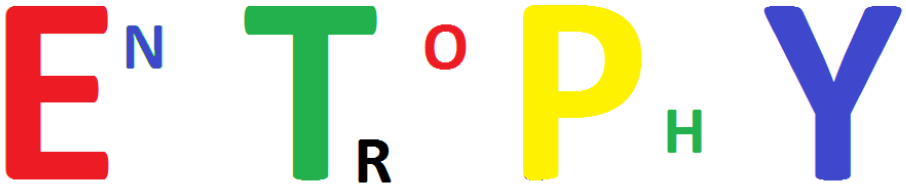


Entrophy: guía de usuario

David Marciel Pariente

davidmarciel@hotmail.com

Introducción

Entrophy es una aplicación diseñada para aumentar la seguridad en la introducción de contraseñas. Está inspirada en los principios del concepto que le da nombre, y fue presentada en septiembre de 2015 en la Universidad de Valladolid (Escuela de Ingeniería Informática) por David Marciel Pariente como su Proyecto Final de Grado.

En esta pequeña guía pretendemos dar una visión rápida y simple de la misma, explicando sus elementos, pero no la teoría en la que se basa.

Para su correcto funcionamiento es recomendable utilizar dispositivos móviles con gran cantidad de puntos (720x1280 o superior) y una api mínima de 17 (4.2.2). De no disponer de un terminal que coincida con las especificaciones, se podría utilizar una máquina virtual.

La naturaleza del SO Android simplifica mucho la instalación de la aplicación. Basta con ejecutar el archivo ".apk" y seguir los pasos marcados aceptando las posibles peticiones de permisos.

Aparte de lo ya dicho, conviene hacer una mención al primer uso: es necesario establecer una contraseña antes de poder utilizar la aplicación.

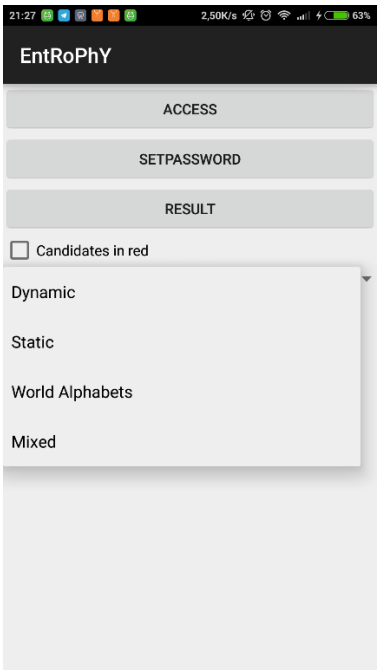
La aplicación consta de cuatro vistas, cada una encargada de una función:

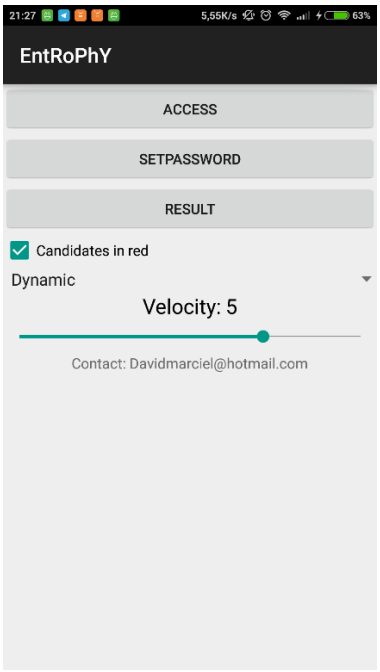
1. Lanzador.
2. Acceso.
3. Cambiar contraseña.
4. Resultado.

1. Lanzador

Es la vista encargada del acceso al resto de vistas. Consta de:

- Tres botones que nos *lanzan* a las otras vistas (“Acceso”, “Cambio de Contraseña” y “Resultado”)
- Un checkbox que ofrece la posibilidad de seleccionar las letras que se presentan en la vista.
- Un selector para los diferentes modos. Cada modo tiene un tipo de letras diferente, algo que habrá que tener en cuenta a la hora de elegir la contraseña.
- Una barra que permite modificar la velocidad de movimiento de las letras en el resto de vistas.

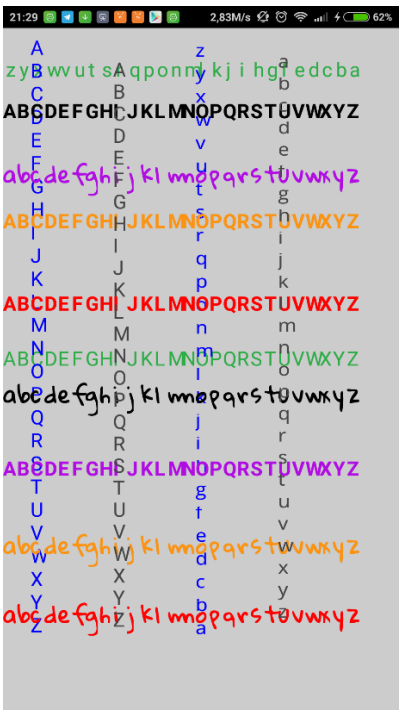


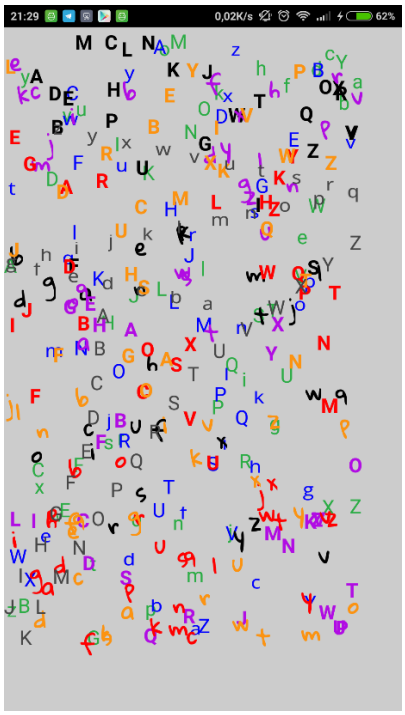


2. Acceso

Es la vista principal, encargada de mostrar la información correspondiente a la autentificación.

En ella podemos ver multitud de letras inmóviles. Una vez toquemos la pantalla, empezarán a moverse de forma caótica, y a partir de ese momento podremos seleccionar las letras.

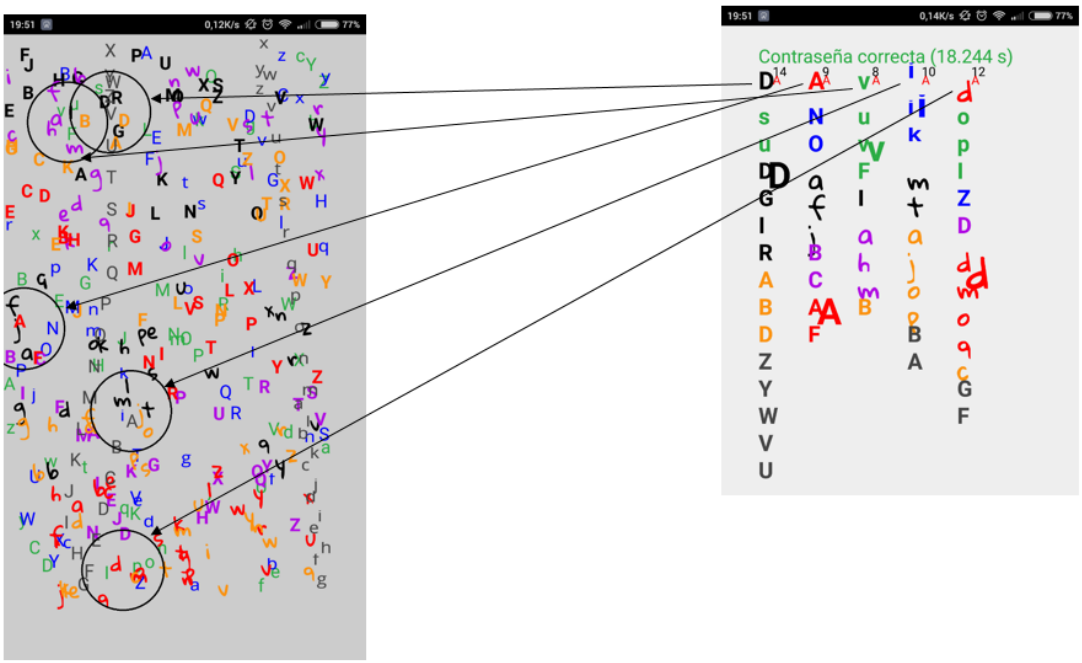




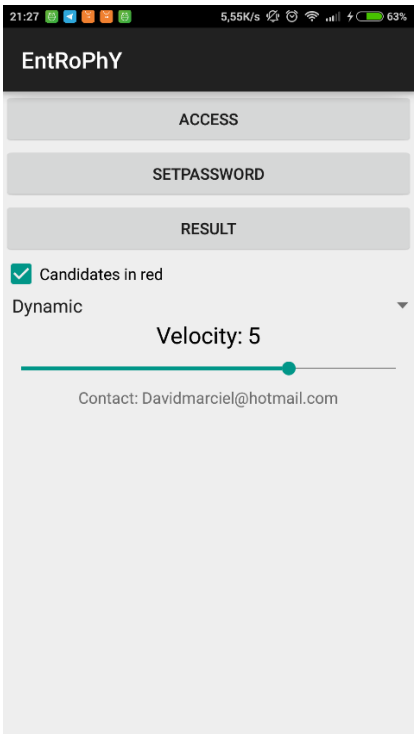
Pulsaremos en orden aquellas letras que formen nuestra contraseña, demostrando así que la conocemos. Todas las letras cercanas al punto en el que pulsemos serán “candidatas” a conformar la contraseña. Por eso no es necesario pulsar exactamente sobre la letra deseada, sino que podemos pulsar cerca.

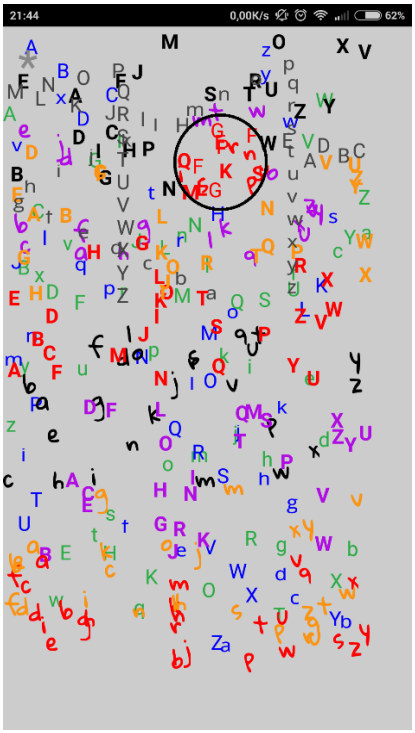
De esta forma conseguimos que no sea posible conocer cuál de todas las letras pulsadas es la solución. Nuestras pulsaciones no desvelarán la contraseña a un observador externo porque no podrá identificar qué letra de entre todas las “candidatas” es la que nosotros buscamos.

Es muy recomendable –al menos en los primeros usos- localizar las letras de nuestra contraseña antes de pulsar por primera vez y hacer que empiecen a moverse. De esta forma seremos capaces de encontrarlas rápidamente una vez estén en movimiento. Este sencillo funcionamiento nos permite localizar sólo aquellas letras que estemos buscando y cuya situación inicial conozcamos a la vez que nos protege de observadores indiscretos reduciendo el tiempo de exposición.



Si queremos ver mejor esto podemos activar la casilla “Señalar pulsados” en la vista “Lanzador”, lo que nos permitirá ver marcadas en rojo todas las letras seleccionadas como “candidatas” con nuestras pulsaciones de pantalla.



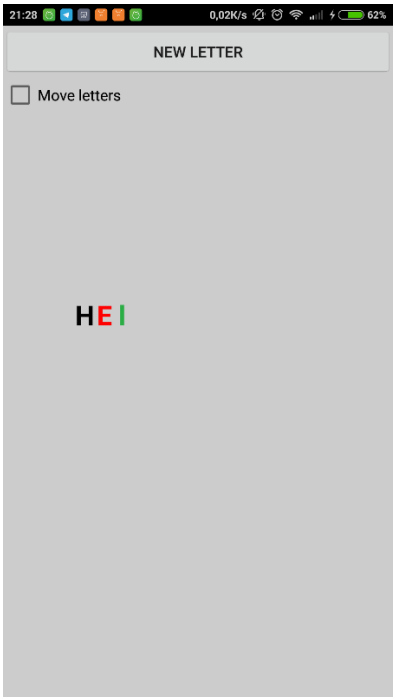


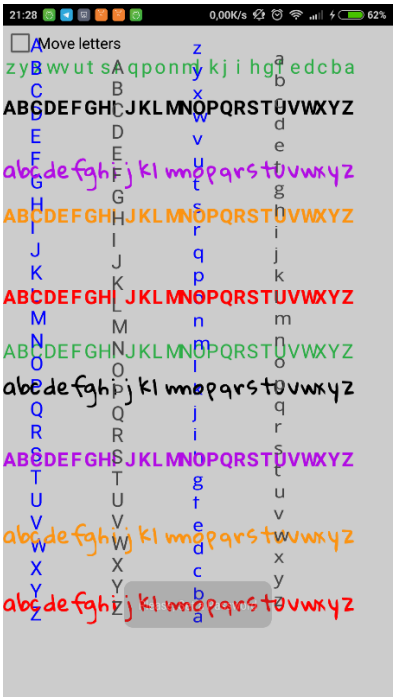
3. Cambiar contraseña

La vista “Cambio de contraseña” muestra:

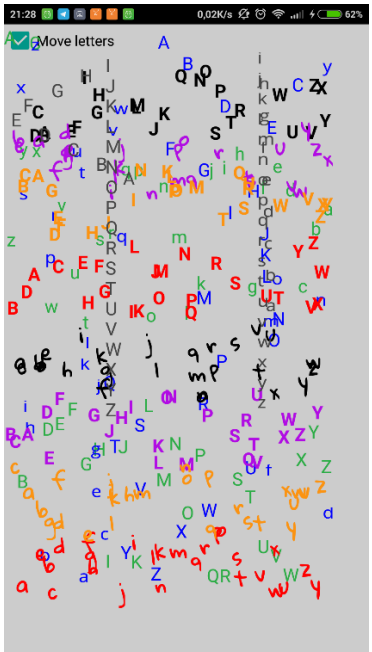
- La contraseña actual.
- Un checkbox que permite bloquear el movimiento de las letras al seleccionarlas.
- Un botón que nos permite seleccionar una nueva letra para la contraseña.

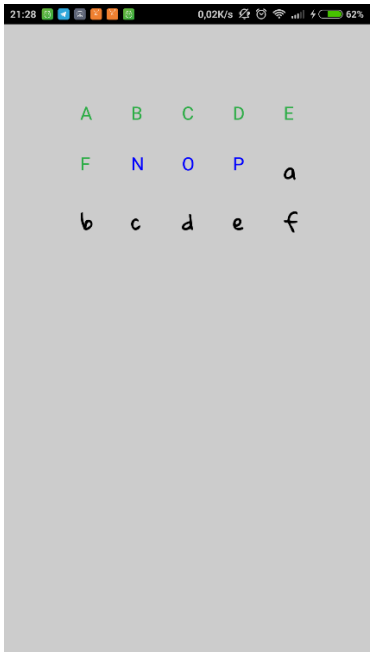
Al pulsar sobre “Nueva letra” se nos muestra una pantalla similar a la “Acceso”, pero con un checkbox que nos permite parar o reanudar el movimiento de las letras de la pantalla.





Tras pulsar sobre la pantalla, un selector logarítmico nos muestra las letras “candidatas” (aquellas más cercanas al punto seleccionado), permitiéndonos seleccionar fácilmente la que deseemos que sea parte de la nueva contraseña.

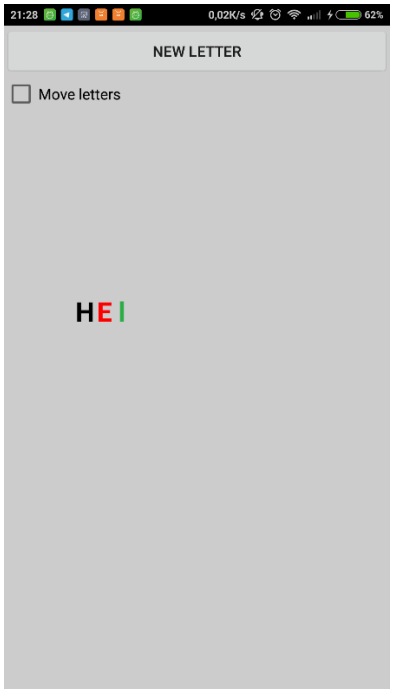


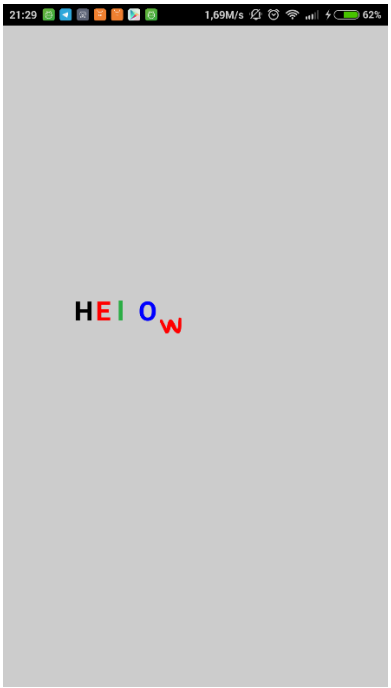


Cuando hemos seleccionado la letra deseada, ésta se nos muestra sola en la pantalla. Podremos seguir seleccionando nuevas letras pulsando sobre “Nueva letra”.

Cuando hayamos seleccionado las cinco letras para la contraseña actual, la contraseña se considerará establecida y ya no se mostrarán los botones para añadir nuevas letras.

A partir de ese momento la contraseña será la utilizada por la vista “Resultado” para comprobar la validez de los nuevos accesos.

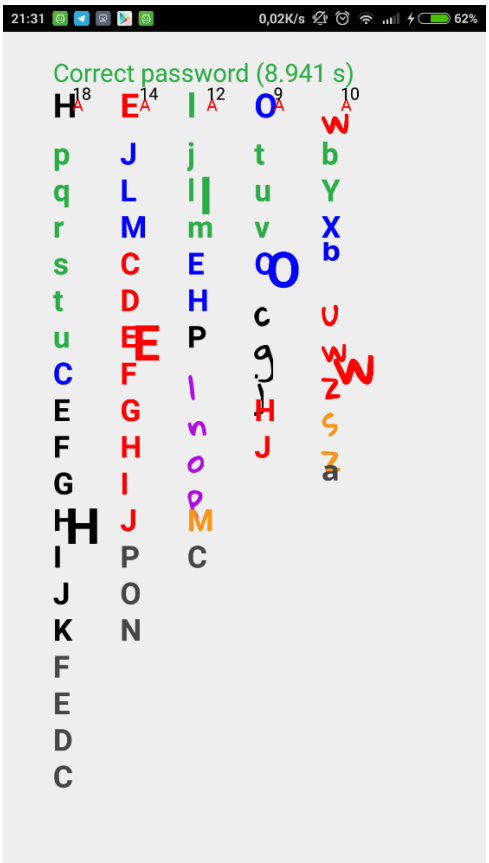




4. Resultado

Podemos acceder a la vista “Resultado” desde el lanzador. En esta vista se nos muestra la información del último intento. En esta vista se nos muestra:

- En primer lugar, información sobre si se ha acertado la contraseña (“Contraseña correcta” o “Contraseña incorrecta”) y el tiempo (en segundos) que ha llevado el intento.
- Debajo de esa información aparece la contraseña en letras grandes. Cada letra de la contraseña tiene como superíndice el número de letras “candidatas” que ha producido el intento de acceso. Si la letra correcta estuviera entre ese conjunto de letras candidatas, además tendría como subíndice una A (de “Acertada”) roja.
- Debajo de cada letra de la contraseña se muestran sus letras “candidatas” (las correspondientes a su pulsación). La letra correcta –si está entre las candidatas- tendrá una copia suya en grande al lado para indicarlo, al igual que arriba la letra de la contraseña lo indica con la A roja.



Como es de esperar, la vista “Resultado” es propia de una versión de prueba, pero no de una aplicación final. En una posible aplicación final no se mostraría esta vista, dado que la información relativa a la contraseña se almacenaría en el servidor y nunca sería conocida por el cliente.

De hecho, el dispositivo no conocería la contraseña en ningún momento; simplemente haría de transmisor de información entre el usuario y el servidor, quien se encargaría de validar si la

posición y el tiempo en los que se ha pulsado la pantalla corresponden con la posición y el tiempo en los que se encontraban las letras de la contraseña.

Así conseguimos seguridad incluso cuando nuestra comunicación es conocida. Dado que conocer la comunicación no implica conocer la contraseña, un observador externo únicamente puede saber que la primera letra de la contraseña está contenida en el primer conjunto, que la segunda está contenida en el segundo, y así sucesivamente.

En las últimas imágenes se muestra una contraseña aceptada. El primer conjunto de letras “candidatas” tiene 18 letras, el segundo otras 14, el tercero 12, el cuarto 9, y el quinto tiene 10. Esto significa que el número de combinaciones posibles con las letras “candidatas” es de 18*14*12*9*10 = 272160. De entre todas estas combinaciones sólo una (“HElOw”, con los colores correctos) es válida. Así, aunque alguien conozca la comunicación no podrá saber cuál de las 272160 contraseñas posibles es la correcta.

Además, dada la naturaleza pseudo-aleatoria de los movimientos de nuestras letras no existe la posibilidad de volver a pulsar los mismos conjuntos, por lo que seguiremos seguros ante ataques de fuerza bruta.