Universidad de Valladolid

E.T.S Ingeniería Informática

Entrophy: guía de usuario

Autor:

D. David Marciel Pariente

Introducción

Entrophy es una aplicación diseñada para aumentar la seguridad de introducción de contraseña. Está inspirada en los principios del concepto de su mismo nombre presentados por David Marciel Pariente en su Proyecto final de Grado en Septiembre de 2015 (Universidad de Valladolid, Escuela de Ingeniería Informática).

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

Para su correcto funcionamiento ha de ser desplegada en un dispositivo Android táctil, las dimensiones de este dispositivo son de 720x1280 y su api mínima 17 (4.2.2). Estas especificaciones coinciden con las de Google Galaxy Nexus, por lo que, de no disponer de un terminal que coincida con las especificaciones, se recomienda usar una máquina virtual del dispositivo mencionado.

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.

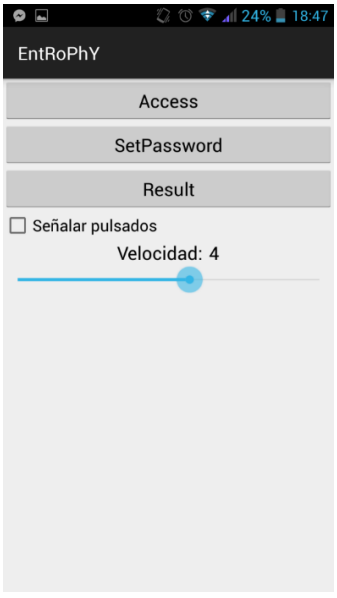
Aparte de lo ya dicho, conviene hacer una mención al primer uso. Es necesario establecer una contraseña antes de poder utilizar la aplicación.

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

Lanzador

Es la vista encargada del acceso al resto de vistas.

Consta de tres botones encargados de lanzar las otras vistas (acceso, la de cambio de contraseña y resultado), un checkbox que permite seleccionar si se quiere o no marcar las letras pulsadas en la vista de acceso y una barra que nos permite modificar la velocidad de movimiento de las letras en el resto de vistas.

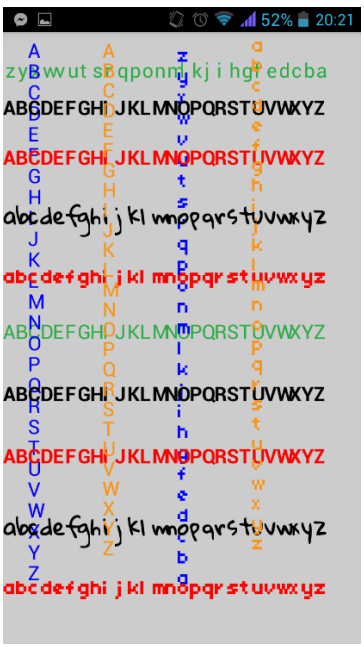


Aceso

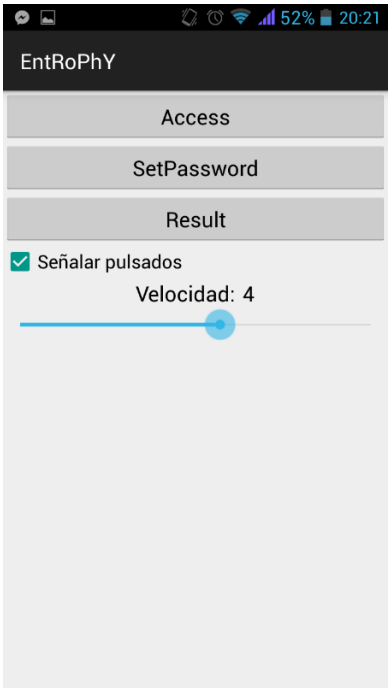
Es la vista principal, se encarga de mostrar la información correspondiente a la autentificación.

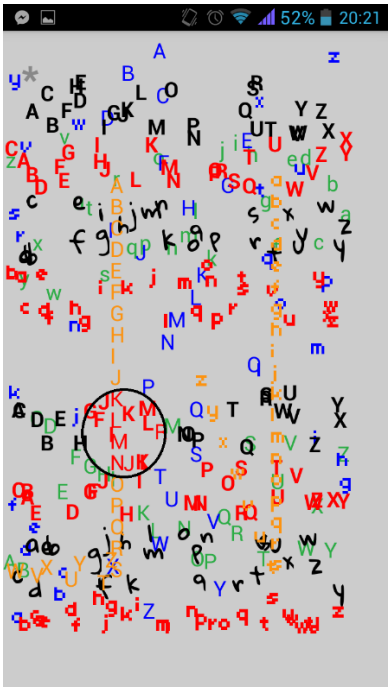
En ella podemos ver multitud de letras inmóviles. Una vez realicemos la primera pulsación empezarán a moverse, a partír de ese momento podremos pulsar sobre las letras.

Pulsaremos aquellas que formen nuestra contraseña. De esta forma demostraremos conocer la contraseña sin necesidad de revelarla.



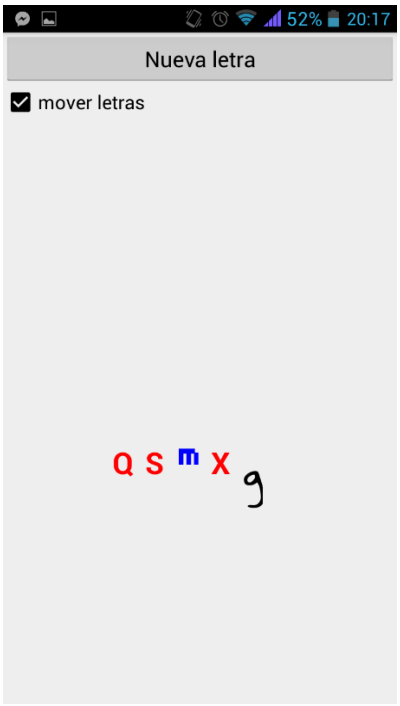
Todas las letras cercanas al punto en el que pulsemos serán válidas, no es necesario pulsar exactamente sobre la letra deseada, podemos pulsar cerca, de esta forma conseguimos que no sea posible conocer cuál de las pulsadas es la solución. Para ver mejor esto podemos activar la casilla señalar pulsados del lanzador. Así veremos marcadas en rojo las letras seleccionadas.

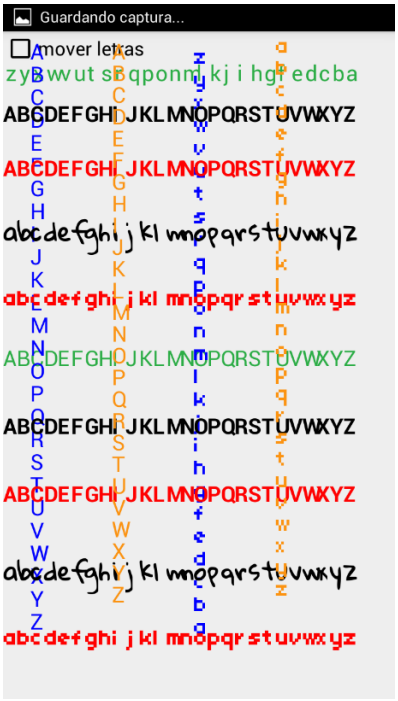




Cambiar contraseña

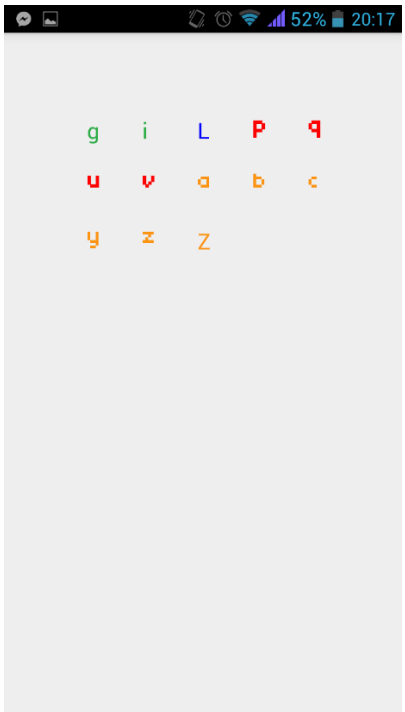
La vista de cambio de contraseña muestra la contraseña actual, un checkbox para permitir bloquear el movimiento de las letras al seleccionarlas y un botón que nos permite seleccionar una nueva letra para la contraseña.





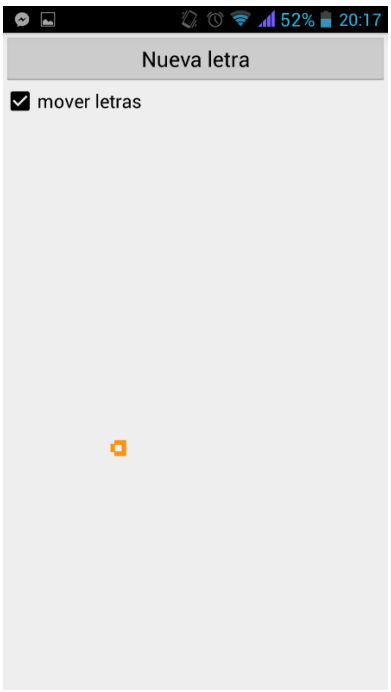
Tras pulsar sobre “Nueva letra” se nos muestra una pantalla similar a la de acceso, pero con un checkbox que nos permite parar o mover las letras de la pantalla.

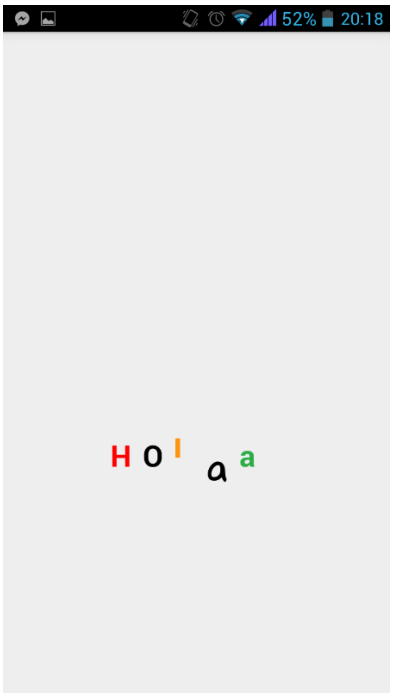
Tras pulsar sobre la pantalla se nos muestran las letras cercanas al punto seleccionado más dispersas. Con este selector logarítmico podemos seleccionar fácilmente la que deseemos.



Cuando hemos seleccionado la letra deseada se nos mostrará. Ahora podemos seleccionar una nueva letra pulsando sobre “Nueva letra”.

Las contraseñas utilizan cinco letras. Tras seleccionar las cinco letras nuestra contraseña estará establecida y no se mostrarán los botones para añadir nuevas letras.





Una vez está establecida la contraseña será la utilizada por la vista resultado para comprobar la validez de nuestros accesos.

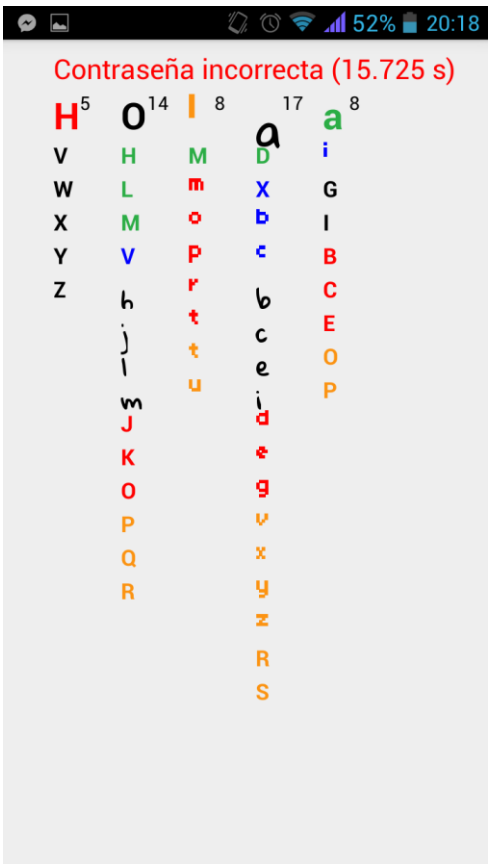
Resultado

En esta vista se nos muestra la información del último intento, podemos acceder a la pantalla de resultado desde el lanzador o automáticamente tras las 5 pulsaciones en la vista acceso.

En esta vista se nos muestra en primer lugar información sobre si la contraseña ha sido **acertada** o no junto con el **tiempo** (en segundos) que ha llevado el intento.

Además, se muestra la **contraseña** en letras grandes. Cada letra de la contraseña tiene como superíndice el **número de letras candidatas**, y si hubiera sido **acertada** tendría una A roja como subíndice.

Debajo de cada letra de la contraseña se muestran las **letras candidatas**, si la letra fuera **solución**, estaría además marcada como tal más grande junto a la letra candidata correcta.



Como es de esperar la vista resultado es propia de una prueba de concepto pero no de una aplicación final.

En una posible aplicación final esta vista constaría simplemente de un mensaje de información notificando la validez o no de la contraseña introducida. 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/tiempo en los que se ha pulsado en la pantalla corresponden con los lugares en los que se encontraban las letras de la contraseña.