Mejoras de un sistema de contraseñas graficas

Autor: Jose Luis Brehcist Rodríguez
Responsable de la asignatura: Jordi Herrera Joancomartí
Universidad: Universitat Autònoma de Barcelona
Fecha: 03-01-2014

Máster interuniversitario de Seguridad de las tecnologías de la información y de las comunicaciones

Introducción

- Una de las grandes lacras del omnipresente sistema de autenticación basado en nombres de usuarios y contraseñas es la dificultad que tienen los usuarios para recordar contraseñas seguras.

- Las contraseñas alfanuméricas tradicionales pueden sustituirse por nuevos sistemas de autenticación gráfica.

- El objetivo de este trabajo es diseñar un mecanismo de autenticación gráfica.

Estado del arte de los sistemas de contraseñas gráficos

- Sistemas recall-based
- Sistemas recognition-based
- Sistemas Cued-recall

Elección del sistema con el que se trabajara

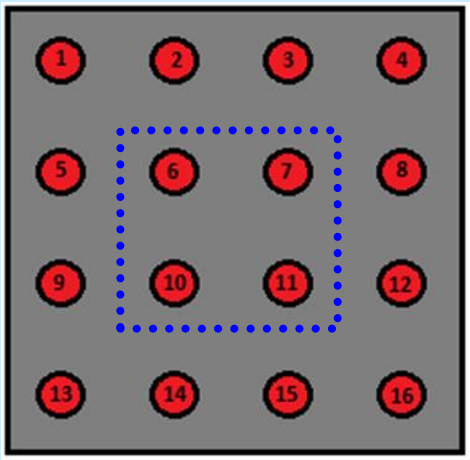
- El sistema elegido forma parte de los sistemas recall-based.
- Se diseñara un sistema para mejorar el sistema que ha sido desarrollado comercialmente para desbloquear la pantalla en los teléfonos móviles que llevan el sistema operativo de Google Android.
- Una de sus mayores vulnerabilidades de este sistema, ha sido probada por el estudio de Aviv et al. 2010 “Smudge Attacks on Smartphone Touch Screens”, donde se demuestra como un atacante puede determinar el patrón usado por el usuario, analizando los residuos de grasa que dejan los dedos en la pantalla.

Descripción general del nuevo sistema propuesto

- Problemas con el sistema actual.
  - Muy persistentes los residuos dejados en la pantalla
  - Difíciles de eliminar
  - Fácil de analizar para obtener el patrón utilizado
- Hay que tener en cuenta que siempre que se use un sistema de contraseña grafico para desbloquear la pantalla se dejaran residuos en ella.

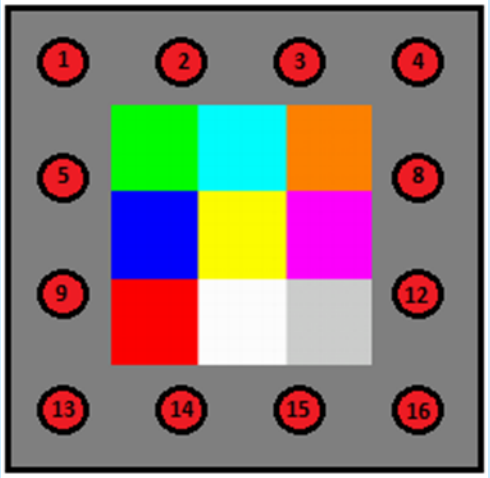
Descripción general del nuevo sistema propuesto

- El sistema propuesto consiste en aumentar el número de puntos en la cuadricula y añadir un nuevo factor, un color.
- La idea es usar en el patrón uno o más puntos situados en el centro de la cuadricula (6, 7, 10 y 11).
- Si no se pueden hacer desaparecer los residuos, se intenta camuflarlos.
- Para los casos en los que no se use los puntos centrales, el atacante aun tendrá que adivinar el color utilizado.



Descripción general del nuevo sistema propuesto

- El sistema propuesto aumenta la cuadricula de 3x3 a una de 4x4.
- El número mínimo de puntos a seleccionar pasa de 4 a 5.
- Se añade la elección de un color de nueve posibles, mostrados en una paleta que cambiara aleatoriamente su orden.



Funcionamiento del diseño

- La aplicación creada simula el comportamiento del sistema nuevo.

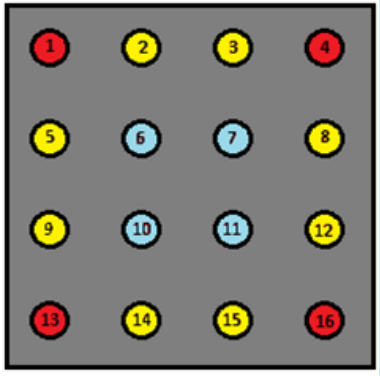
- Al ejecutar la aplicación podremos:
  - Registrar el patrón
  - Desbloquear la pantalla
  - Borrar el patrón registrado
  - salir de la aplicación

Análisis de la seguridad

- El espacio de contraseñas de la versión actual de 9 puntos:
  - La combinación más pequeña permitida es de 4 puntos y equivale a 1624 posibilidades permitidas.
  - La combinación más grande permitida es de 9 puntos y equivale a 140704 posibilidades permitidas.
- $C(m,n) = m! / (m – n)!$
- Con 9 puntos seleccionables, obtendremos $9! / (9 – 9)! = 9! = 362880$ combinaciones sin repetición, de las cuales solo 140704 están permitidas.
- Combinaciones posibles permitidas:
  - 4 puntos: 1624
  - 5 puntos: 7152
  - 6 puntos: 26016
  - 7 puntos: 72912
  - 8 puntos: 140704
  - 9 puntos: 140704
- Sumando un total de 389112 combinaciones permitidas, que equivalen al espacio total de contraseñas.

Análisis de la seguridad

- El espacio de contraseñas del sistema propuesto de 16 puntos:
  - La combinación más pequeña permitida es de 5 puntos y equivale a 154680 posibilidades permitidas.
  - La combinación más grande permitida es de 16 puntos y equivale a 1577602537520 posibilidades permitidas
- Con 16 puntos seleccionables, obtendremos 16! / (16 – 16)! = 16! = 20922789888000 combinaciones sin repetición.
- Para poder calcular las combinaciones permitidas hay que estudiar la simetría que hay en la cuadricula de 4*4. Porque analizar todas las combinaciones posibles es inviable en tiempos de computación.
- Con 16 puntos seleccionables, obtendremos 16! / (16 – 16)! = 16! = 20922789888000 combinaciones sin repetición.
- Para poder calcular las combinaciones permitidas hay que estudiar la simetría que hay en la cuadricula de 4*4. Porque analizar todas las combinaciones posibles es inviable en tiempos de computación.
- Combinaciones posibles permitidas:
  - 5 puntos: 154680
  - 6 puntos: 1331944
  - 7 puntos: 10690096
  - 8 puntos: 79137824
  - 9 puntos: 533427944
  - 10 puntos: 3221413136
  - 11 puntos: 17068504632
  - 12 puntos: 77129797424
  - 13 puntos: 285415667080
  - 14 puntos: 811404606344
  - 15 puntos: 1577602537520
  - 16 puntos: 1577602537520



- Sumando un total de 4350069806144 combinaciones permitidas, que multiplicadas por 9, el número de colores posibles para cada combinación obtenemos 39150628255296 combinaciones permitidas, que equivalen al espacio total de contraseñas.

Evaluación de usabilidad con usuarios reales

- Pruebas realizadas sin recomendar previamente al usuario el uso de los puntos centrales.
- Se les permite a los voluntarios familiarizarse brevemente con la aplicación antes de registrar el patrón.
- Las pruebas se basan en dos fases:
  - En la primera fase se busca obtener una idea de las preferencias de los voluntarios al elaborar su patrón.
  - En la segunda fase se pone a prueba el nivel de dificultad para recordar el patrón previamente elegido.

Evaluación de usabilidad con usuarios reales

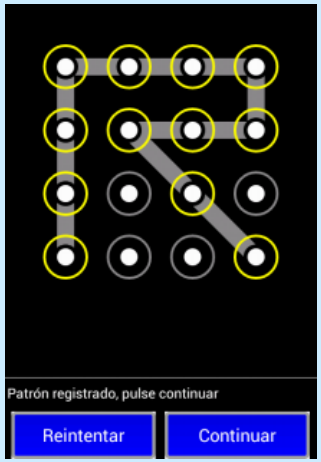
- Para comodidad en la realización y análisis de las pruebas se almacenan los resultados usando varios ficheros en la memoria interna.

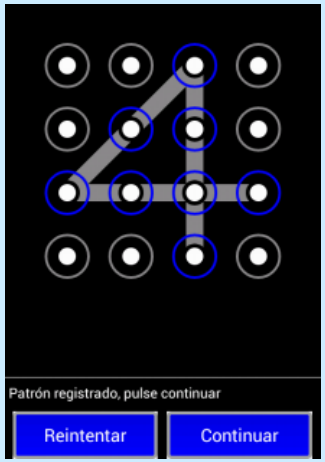
- Ejemplo de los datos obtenidos por un voluntario.

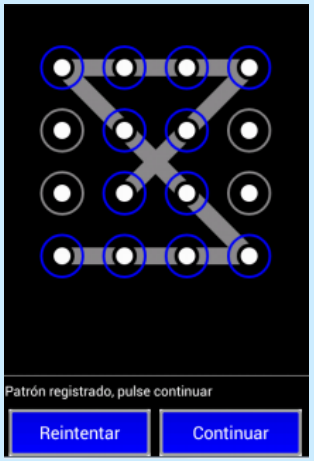
```
Pep registrando: Yellow 13 10 7 4 3 2 1 6 11 16 Sat Dec 07 20:49:21 2013
Pep confirmando: Yellow 13 10 7 4 3 2 1 6 11 16 Sat Dec 07 20:49:29 2013
## Patrón confirmado después de 1 intentos ##
Pep desbloquear: Yellow 13 10 7 4 3 2 1 6 11 16 Sat Dec 07 20:49:38 2013
## Pantalla desbloqueada después de 1 intentos ##
```

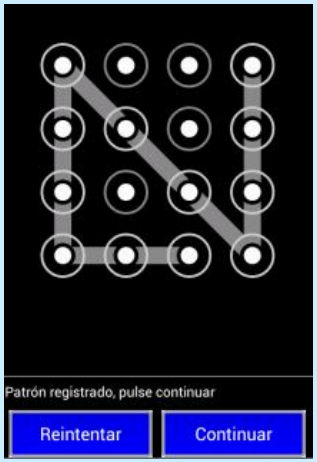
Análisis de los resultados obtenidos

- Más del 75% de los voluntarios usaron al menos 2 de los 4 puntos centrales de la cuadricula.


Patrón registrado, pulse continuar

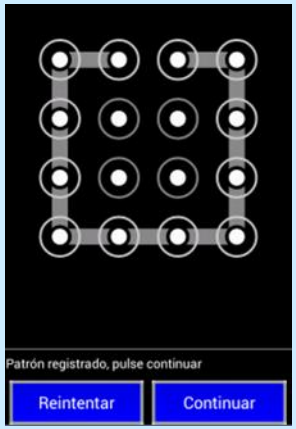

Patrón registrado, pulse continuar

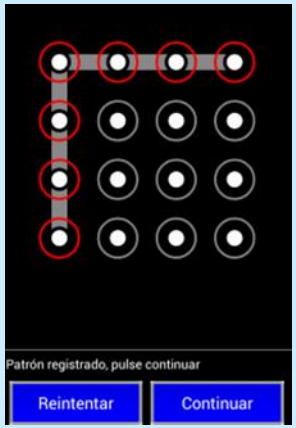

Patrón registrado, pulse continuar

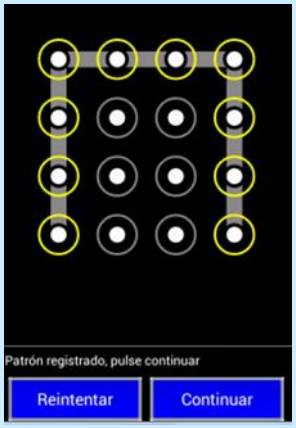

Patrón registrado, pulse continuar

Análisis de los resultados obtenidos

- A continuación se muestran algunos ejemplos de las combinaciones elegidas donde no se han usado los puntos centrales.







Análisis de los resultados obtenidos

- No hay problemas para recordar los colores.
- Al registrar el patrón, en algunos casos si la secuencia era muy larga, aparecieron algunos errores y se decidió por una secuencia más corta.
- Cuando el usuario ha seleccionado un patrón, salvo error de precisión en la selección, no ha habido errores.
- La secuencia más cortas seleccionada ha sido de 5 puntos.
- La longitud de la secuencias más frecuentes han sido de 6 y 12 puntos.
- Solo un usuario utilizo los 16 puntos disponibles en su patrón

Conclusiones

- Sin informar a los usuarios de la importancia de usar los puntos del medio, se han usado por encima del 75% de los casos.
- El incremento de seguridad en el sistema no ha supuesto un problema al usuario para recordar su contraseña.
- El sistema propuesto ayudaría a mejorar la seguridad en este tipo de dispositivos.