Disseny i anàlisi d'un sistema de contrasenyes gràfiques

Autor: Gregorio García Sancho

Enginyeria tècnica en informàtica de sistemes

Consultora: Cristina Pérez Solà

14 de juny de 2013

Obra sota llicència Creative Commons

Aquesta obra està subjecta a una llicència de
Reconeixement-NoComercial-CompartirIgual 3.0 No adaptada de Creative Commons

http://creativecommons.org/licenses/by-nc-sa/3.0/deed.ca

Resum

Les contrasenyes gràfiques existeixen des de fa gairebé vint anys, però ni són utilitzades abastament ni, de fet, són gaire conegudes. El present TFC consisteix en fer un estudi dels sistemes de contrasenya gràfica a tall de presentació per a donar a conèixer el seu funcionament. Primer de tot, es fa una explicació de què són i s'elabora una recopilació dels sistemes més significatius, tant comercials com experimentals, tot mostrant els trets més distintius així com els punts febles.

A continuació, el TFC adquireix un caire més pràctic. De tots els sistemes presentats anteriorment, es crea una evolució d'un d'ells que aporti millores a l'original, degudament justificades.

Finalment, es desenvolupa una aplicació real del sistema de contrasenya per poder fer proves amb usuaris que serviran per obtenir dades objectives. A l'apartat de conclusions, es fa una valoració de si s'han assolit les millores pressuposades inicialment.

Summary

Graphical passwords have existed for over twenty years but they are neither widely used nor actually known. This dissertation consists in developing a study about graphical password schemes as a presentation in order to show their performance. First of all, it explains what they are and includes a summary of the most representative schemes, both commercial ones and experimental ones. The aim of this essay is to show both the most distinctive features and the weak points.

After that, the dissertation becomes more practical. One of the former schemes presented above is chosen to create an evolution. It has to provide improvements to the original one, duly justified.

Finally, an application of the evolution is performed in order to be tested by users and to obtain objective data. In the conclusions chapter, an assessment is done in order to confirm the improvements.

Paraules clau

Contrasenya gràfica, seguretat, autenticació, pantalles tàctils.

Nom de l'àrea del TFC

Seguretat informàtica

Agraïments i dedicatòries

Vull agrair l'ajuda rebuda pels companys, consultors i tutor al llarg de tots aquests semestres. Sense aquest suport, no hagués estat possible arribar fins aquí.

També vull agrair als meus pares la seva insistència en que estudiés una carrera i, especialment, a la meva companya Dolors per la seva paciència al llarg de totes les hores dedicades a estudiar.

Índex de continguts

Índex de figures 9
1. Introducció 11
1.1. Objectius 13
1.2. Motivació per a l'ús de les contrasenyes gràfiques 13
1.3. Metodologia 15
1.4. Tasques 15
1.5. Planificació temporal 16
1.6. Recursos 17
1.7. Pressupost 18
1.8. Breu descripció dels altres capítols 19
2. Estat de l'art 20
2.1. Classificació dels sistemes de contrasenyes 20
2.2. Propietats de les contrasenyes 21
2.3. Contrasenyes gràfiques més característiques 22
2.3.1. Draw-A-Secret (DAS) [7] 22
2.3.2. Passdoodle [9] 24
2.3.3. Pass-Go [10] 25
2.3.4. GrIDsure [11] 26
2.3.5. PassFaces [12] 27
2.3.6. Déjà Vu [13] 28
2.3.7. Graphical password, G. Blonder [14] 30
2.3.8. PassPoints [15] 31
2.3.9. Cued Click Points [17] 32

2.3.10. Persuasive Cued Click-Points [18] 33
2.3.11. Inkblot Authentification [19] 34
2.4. Punts febles 35
2.4.1. Força bruta 36
2.4.2. Atacs de diccionari 36
2.4.3. Atacs de diccionari aplicats a sistemes gràfics 37
2.4.4. Shoulder surfing 37
2.4.5. Empremtes a la pantalla 38
2.4.6. Atacs amb programari 39
3. Elecció de sistema de contrasenya gràfica 40
3.1. Desbloqueigs d'Android 40
3.1.1. Lliscament del dit 40
3.1.2. PIN o contrasenya 41
3.1.3. Desbloqueig facial 42
3.1.4. Patró 42
4. Proposta de millora: l'aplicació TAP DOTS! 44
4.1. Justificació de la proposta 44
4.2. L'aplicació TAP DOTS! 45
4.2.1. Millores aportades 47
4.2.2. Disseny de l'aplicació 49
4.2.3. Desenvolupament de l'aplicació 51
4.3. Joc de proves amb usuaris 58
4.4. Resultats de les proves 60
5. Conclusions 62
5.1. Èxits 62

5.2. Problemàtiques 63

5.3. Millores de futur 65

Glossari 67

Bibliografia 69

Índex de figures

Figura 1: planificació temporal 16

Figura 2: diagrama de Gantt 17

Figura 3: Draw-a-secret 23

Figura 4: Passdoodle 24

Figura 5: Pass-Go 25

Figura 6: GrIdsure 27

Figura 7: PassFaces 28

Figura 8: Déjà Vu 29

Figura 9: Graphical password de Greg Blonder 30

Figura 10: PassPoints 31

Figura 11: Cued Click Points 32

Figura 12: Persuasive Cued Click-Points 33

Figura 13: hotspots de PCCP 34

Figura 14: Inkblot authentification 35

Figura 15: empremtes a la pantalla 39

Figura 16: lliscament de dit 41

Figura 17: PIN 42

Figura 18: desbloqueig facial 42

Figura 19: patró d'Android 43

Figura 20: teclat numèric 46

Figura 21: teclat TAP DOTS! 46

Figura 22: ditades sobre el fons de l'aplicació 48

Figura 23: ditades sobre la pantalla apagada 48

Figura 24: contrasenya correcta 50

Figura 25: contrasenya incorrecta 51

Figura 26: 10 pantalles de l'aplicació 51

Figura 27: pantalla principal de desenvolupament del MIT App Inventor 53

Figura 28: variable llista 55

Figura 29: accions de les tecles de l'1 al 9 55

Figura 30: acció tecla 10 57

Figura 31: instruccions finals pantalla 2 58

Figura 32: instruccions finals pantalla 10 58

Figura 33: taula de dades de les proves amb usuaris 60

Figura 34: taula de repeticions dels colors 61

Figura 35: signes en blanc i negre 65

1. Introducció

La seguretat informàtica té per objectiu protegir la integritat i privacitat de la informació que tenim en sistemes informàtics. Els mètodes més habituals per assegurar aquesta protecció són els sistemes d'accés amb contrasenya. La majoria dels que es fan servir avui dia no difereixen gaire de com eren en un inici: un nom d'usuari i un mot secret format per números, lletres, caràcters, o bé, un combinat de tots ells.

Aquests sistemes, tot i que no han sofert grans evolucions, són molt vàlids per a les necessitats actuals. Tanmateix, es comencen a utilitzar altres tipus que han sorgit per resoldre problemes concrets. Aquests són els sistemes de contrasenya gràfica.

El mètode més habitual per controlar l'accés a recursos és autenticar un usuari mitjançant un número (PIN, *Personal Identification Number*) o bé una cadena de text.

La contrasenya serà més o menys llarga en funció del grau de seguretat desitjat. És a dir, com més curta és, esdevé més fàcil que un tercer pugui esbrinar-la. Per tant, si volem protegir correctament els nostres recursos cal que la contrasenya sigui llarga.

Un altre factor que influeix en que la contrasenya sigui robusta i difícil d'esbrinar és el grau de complexitat. Números de telèfon, de matrícules, noms personals, dates d'aniversari, etc, són mots de pas a evitar ja que són molt previsibles per a atacants. Llavors s'ha de triar una combinació de lletres majúscules i minúscules, números i caràcters especials sense cap significat. Un exemple seria: a29Vc&D/

Segons la consultora *SplashData* [1] les 25 contrasenyes més utilitzades a Internet són les següents:

1. *password*
2. *123456*
3. *12345678*
4. *Qwerty*

5. *abc123*
6. *Monkey*
7. *1234567*
8. *Letmein*
9. *trustno1*
10. *Dragon*
11. *Baseball*
12. *111111*
13. *Iloveyou*
14. *Master*
15. *Sunshine*
16. *Ashley*
17. *Bailey*
18. *passw0rd*
19. *Shadow*
20. *123123*
21. *654321*
22. *Superman*
23. *Qazwsx*
24. *Michael*
25. *Football*

Com es pot comprovar són mots o números molt simples i fàcils de recordar. La mateixa consultora recomana utilitzar una contrasenya diferent per a cada servei o recurs al què s'ha d'accedir.

El fet d'haver d'emprar moltes contrasenyes llargues i complexes per a tenir una bona seguretat fa que els usuaris triïn entre dues opcions: o bé utilitzar la mateixa contrasenya per a tot, o bé fer servir diverses contrasenyes simples ja que esdevé molt difícil recordar vàries cadenes de text sense cap sentit i associar-les a diferents recursos.

Finalment, l'usuari vol eficiència en realitzar qualsevol comesa. Per tant, si recordar cadenes de text complexes implica massa esforç mental, no dubtarà en elegir-ne de més senzilles. Augmentar el grau de seguretat facilitant les tasques de recordar i reproduir esdevé el motiu de ser de les contrasenyes gràfiques. Es busca augmentar alhora la usabilitat i la seguretat.

1.1. Objectius

Aquesta proposta de treball fi de carrera té dos objectius bàsics. El primer és fer una presentació amb caràcter divulgatiu de les contrasenyes gràfiques per als usuaris neòfits. El segon objectiu és intentar crear un sistema nou a partir d'un existent millorant punts febles d'aquest.

Primer de tot es farà una breu anàlisi dels motius que han fet evolucionar les contrasenyes tradicionals de cadenes de caràcters a les gràfiques. Després, es farà una recopilació dels sistemes de contrasenyes gràfics que permeten autenticar a un usuari, enumerant els principals avantatges i desavantatges de cadascun.

A partir d'aquesta anàlisi es triarà un tipus de contrasenya gràfica i es farà una proposta de modificació per millorar-la. També es desenvoluparà una aplicació que permeti interaccionar amb el sistema de desbloqueig. El següent pas serà fer un estudi d'aquest nou sistema amb un grup d'usuaris per verificar si les modificacions suposen un avenç respecte el model anterior o per contra no s'experimenta una millora.

1.2. Motivació per a l'ús de les contrasenyes gràfiques

Quan s'implementa un sistema de protecció d'accés per contrasenya s'han de tenir en compte una sèrie de consideracions. La tria dependrà de les variables següents:

- Tipus d'usuari que accedirà al recurs: públic general, nens, adults, professionals, estudiants, etc.
- Freqüència d'ús: diverses vegades al dia, habitualment, esporàdicament, etc.
- Requeriments del sistema de contrasenyes o, dit d'una altra manera, recursos de maquinari que pot oferir l'aparell on s'ha de fer la connexió: ordinador, telèfon mòbil, telèfon intel·ligent, caixer automàtic, etc.
- Grau de seguretat necessari.

- Velocitat d'accés.

Aquestes característiques determinaran la viabilitat d'utilitzar els sistemes textuals clàssics o bé ponderar la possibilitat d'optar per una versió gràfica.

Si el motiu principal és la seguretat, llavors és necessari elevar el grau de complexitat. Si es tria el sistema alfanumèric tradicional, la contrasenya ha de ser complexa. Generar-ne de complexes per a dificultar atacs i mantenir segur l'accés als llocs que considerem sensibles no és complicat. Fins i tot existeix programari que pot fer aquesta feina per nosaltres [2]. El problema esdevé recordar-les. La problemàtica de les contrasenyes alfanumèriques es pot resumir en que les fàcils de recordar són fàcils d'endevinar i les difícils d'endevinar són difícils de recordar.

Diversos estudis, [3] [4] [5] et al., conclouen que és més fàcil recordar imatges que text. Aquests donen validesa a la dita popular xinesa 'una imatge val més que mil paraules'[1]. De fet moltes tècniques d'estudi es basen en ajudes visuals, mapes mentals o conceptuals, etc.

En conseqüència, resulta lògic que desenvolupar contrasenyes gràfiques podria ser útil per que els usuaris les recordin fàcilment. El primer en crear un sistema basat en imatges va ser Greg Blonder [6]. La seva proposta es basava en una imatge on s'havien de triar uns quants punts sobre determinades àrees preseleccionades. Llavors l'usuari havia de clickar sobre els punts triats anteriorment per ser autenticat.

Avui dia, les contrasenyes alfanumèriques tenen l'inconvenient que cada vegada hi ha programari més sofisticat per atacar-les amb els mètodes més habituals: atacs de diccionari i de força bruta que explicarem més endavant. Un exemple és el programari '*John the Ripper*'[2], que permet desxifrar diferents tipus d'algoritmes i és fins i tot personalitzable. Així doncs, trobar una alternativa a les contrasenyes alfanumèriques esdevé una tasca prioritària i les gràfiques semblen a priori una bona opció. En

[1] La traducció literal del proverbi xinés és: 'El significat d'una imatge pot expressar deu mil paraules'.

[2] http://es.wikipedia.org/wiki/John_the_Ripper

aquest treball fi de carrera farem una revisió del seu passat, present i futur.

1.3. Metodologia

Aquest treball fi de carrera és eminentment de recerca i per tant la major part de les tasques a realitzar seran d'obtenció d'informació per tenir una visió clara del tema a tractar, ja que és relativament nou, i poder-lo analitzar i desenvolupar adequadament. Les contrasenyes gràfiques existeixen des de fa uns vint anys però és des de fa poc temps que s'ha començat a popularitzar el seu ús a causa de la gran proliferació de dispositius mòbils amb pantalla tàctil, principalment telèfons mòbils i tauletes digitals. De totes maneres el TFC també té una part pràctica i una d'assaig 'en laboratori' amb el producte per observar les reaccions d'un grup d'usuaris.

1.4. Tasques

Les tasques a realitzar són les següents:

- Recerca de documentació relacionada amb el tema.
- Estudi de la documentació i elaboració d'una llista dels sistemes de contrasenya gràfica més característics.
- Recopilació de les característiques, punts forts, febles, especificacions, etc, de cada sistema per presentar-los.
- Triar un tipus de contrasenya gràfica i pensar possibles millores.
- Implementar una aplicació funcional.
- Dissenyar una bateria de tests que permeti comparar la nova aplicació amb un sistema tradicional.
- Fer proves amb usuaris per analitzar les seves reaccions en front del nou sistema.
- Analitzar les dades obtingudes dels tests reals.

- Extreure conclusions.
- Redactar la memòria
- Fer la presentació virtual en vídeo.

1.5. Planificació temporal

La planificació temporal està desglossada en 4 PACs en les quals s'han definit diverses fites i una estimació del temps necessari per assolir-les. Veure Figura 1.

TFC Primavera 2013

Tasks

Nombre	Fecha de inicio	Fecha de fin
PAC 1 - Pla de treball	27/02/13	18/03/13
Elecció proposta	27/02/13	6/03/13
Definir objectius	7/03/13	14/03/13
Elaborar temporalització	15/03/13	18/03/13
PAC 2	19/03/13	22/04/13
Recerca de documentació	19/03/13	3/04/13
Estudi i elaboració llista	4/04/13	10/04/13
Recopilar característiques	11/04/13	17/04/13
Triar sistema de contrasenya	18/04/13	18/04/13
Disseny nou sistema	19/04/13	22/04/13
PAC 3	23/04/13	31/05/13
Implementar aplicació	23/04/13	13/05/13
Dissenyar bateria de tests	14/05/13	17/05/13
Provar amb usuaris	20/05/13	23/05/13
Analitzar dades obtingudes	24/05/13	28/05/13
Extreure conclusions	29/05/13	31/05/13
PAC 4 - Memòria	3/06/13	14/06/13
Redactar memòria	3/06/13	14/06/13
Lliurament	17/06/13	21/06/13
Presentació virtual en vídeo	17/06/13	21/06/13

Figura 1

Gràficament es pot observar la temporalització amb un diagrama de Gantt. Veure Figura 2.

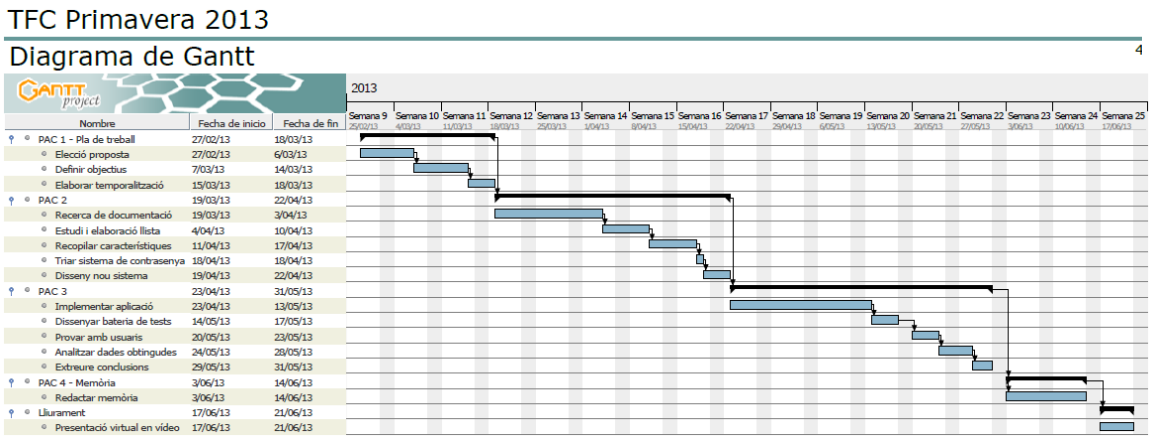

Figura 2

Finalment, el desenvolupament del projecte ha seguit la planificació inicial sense gaires desviacions. En quant a assolir fites, les dates de lliurament s'han respectat. Els desviaments s'han produït durant la implementació de l'aplicació ja que s'ha hagut de dedicar nombroses hores a la formació per utilitzar el programari MIT App Inventor.

La manera de solucionar la càrrega de feina ha sigut augmentant les hores de treball entre els dies 23/4 i 13/5.

1.6. Recursos

Per a dur a terme el TFC no són necessaris recursos amb grans prestacions, amb el punt de treball recomanat per la UOC i qualsevol telèfon Android n'hi ha prou.

Detall del maquinari i programari utilitzat:

- Ordinador amb les següents característiques:
  - CPU: Intel Pentium D 3 GHz
  - Memòria RAM: 2 GB
  - Resolució del monitor: 1.280 x 1.024 píxels
  - Unitat CD i DVD

- Sistema operatiu Windows 7 Professional N
- Connexió de banda ampla ADSL
- Telèfon mòbil:
  - Nexus 4 d'LG
  - SO Android 4.2.2 (Jelly bean)
- Càmera de vídeo Samsung Hyper DIS
- Programari:
  - Windows Office 2007: MS Word i MS Excel.
  - GanttProject 2.6.1 Brno
  - MIT App Inventor 2.07
  - Reproductor multimèdia VLC 2.0.6

1.7. Pressupost

El pressupost d'aquest projecte està basat únicament en hores de feina ja que no es necessari la compra de cap material ni s'ha d'elaborar cap producte físic.

El desglossament del pressupost és molt simple, es comptarà la quantitat d'hores projectada per finalitzar el TFC per un preu de 35€/hora. Les hores a facturar comptaran a partir de la fase PAC 2 ja que el pla de treball es considera com un pressupost sense compromís. L'estimació d'hores a invertir en aquest projecte és de 20 hores/setmana distribuïdes de la següent manera: 2 hores diàries de dilluns a divendres més 5 hores dissabte i 5 diumenge. Per tant, el cost total és de:

Març	40 hores
Abril	84 hores
Maig	86 hores
Juny	60 hores
Total	270 hores

Preu / hora	35 €

Total pressupost:	**35 € * 270 hores = 9450 €**

1.8. Breu descripció dels altres capítols

- Capítol 2. Estat de l'art: es fa una introducció als sistemes de contrasenya i a les diferents maneres que hi ha per classificar-los. S'introdueixen les raons per les quals són necessaris i es finalitza amb una revisió dels sistemes de contrasenya gràfica més representatius amb els seus punts forts i els febles.
- Capítol 3. Elecció de sistema de contrasenya gràfica: es mostren les diferents maneres amb les què es pot fer el desbloqueig de pantalla amb un telèfon Android ja que un d'ells és el triat com el sistema que es millorarà.
- Capítol 4. Proposta de millora: l'aplicació TAP DOTS!: es justifica l'elecció del sistema que es crearà així com els punts de millora. Es fa una descripció acurada de l'aplicació i el desenvolupament. També s'expliquen les proves que s'han fet amb usuaris i les conclusions a què s'ha arribat gràcies a elles.
- Capítol 5. Conclusions: es finalitza el treball explicant els èxits obtinguts respecte la hipòtesi inicial i els problemes detectats. Es proposen punts de millora per al futur.

2. Estat de l'art

Aquesta proposta de TFC es va oferir el semestre anterior, tardor 2012, però al repositori institucional de la UOC no s'hi pot trobar cap memòria. Per tant entenc que és la primera vegada que es fa un treball sobre aquesta matèria a la nostra universitat. Això suposa un nou repte ja que no hi ha cap document similar que pugui fer de referència per al desenvolupament. De fet, aquest va ser un dels motius en el moment de fer el triatge: treballar un tema nou amb marge per la creativitat.

A causa de que les contrasenyes gràfiques no són abastament utilitzades, gairebé no hi ha estudis que en facin referència en català o castellà. Afortunadament, en anglès hi ha molt material disponible a la xarxa que permet fer una revisió acurada de l'estat de l'art.

Aquest TFC pretén fer una anàlisi des de la creació fins l'actualitat d'aquests sistemes de protecció.

2.1. Classificació dels sistemes de contrasenyes

Les contrasenyes alfanumèriques són sempre cadenes de text que estan a la memòria i s'han de recordar en el moment d'autenticar l'accés a un recurs determinat. La manera en què el cervell actua amb una contrasenya gràfica pot diferir en funció de com s'ha dissenyat aquesta. Per tant, les podem classificar de tres maneres diferents segons l'acció que ha de fer l'usuari: recordar, reconèixer, o bé, recordar amb pistes.

Ja hem determinat que a la memòria humana li resulta més fàcil recordar imatges que text. Tal com passa amb les contrasenyes alfanumèriques, si una contrasenya gràfica és complexa, també serà difícil de recordar. En aquest cas, una persona ha de buscar la contrasenya a la memòria sense cap ajuda i introduir-la al dispositiu.

Una variant, recordar amb pistes, consisteix en que el sistema proporciona ajudes a l'usuari que estan relacionades amb la seva contrasenya i li permeten recordar-la més fàcilment.

Finalment, existeixen les contrasenyes que mostren imatges a la pantalla. La clau de pas hi és, i l'usuari només ha de reconèixer-la. Ha d'identificar unes característiques concretes entre allò que està veient.

Com es veurà més endavant, els sistemes de contrasenyes gràfiques poden ser molt variats uns respecte els altres tant en la presència física com en el funcionament ja que tenen la versatilitat de poder utilitzar diferents processos cognitius.

2.2. Propietats de les contrasenyes

Cada sistema de contrasenya té unes propietats que el diferencia dels altres. Per entendre millor què els caracteritza, farem una breu descripció dels factors que influeixen en les particularitats de cada sistema:

- Mida de l'espai de contrasenyes: determina la quantitat total de contrasenyes diferents que es poden formar.
- Temps de creació de la contrasenya: és el temps que es triga des de que l'usuari inicia el procés d'alta en un sistema de contrasenyes fins que el finalitza correctament. El procés inclou la creació d'un nom d'usuari, l'elecció d'una contrasenya, comprovació de la validesa i, finalment, ratificació de la contrasenya triada.
- Temps de login: és el temps que triga un usuari en autenticar-se fent servir un sistema de contrasenyes.
- Facilitat de recordar la contrasenya a llarg termini: és la capacitat de recordar una contrasenya passats uns dies des de la darrera vegada que es va aprendre i utilitzar.
- Resistència al '*shoulder surfing*': és el grau de dificultat que té un atacant en obtenir una contrasenya mitjançant l'observació, directa o indirecta, d'un usuari durant el procés d'autenticació.

2.3. Contrasenyes gràfiques més característiques

Com hem comentat, hi ha tres tipus de sistemes gràfics. Començarem amb el que té més similituds amb les alfanumèriques, el sistema basat en recordar la contrasenya tal com es fa amb les cadenes de text.

De sistemes de contrasenyes gràfics n'hi ha molts més dels aquí mostrats. Aquest llistat només pretén ser una mostra dels esquemes més representatius i d'altres que tenen algun tret característic que val la pena mencionar.

Sistemes basats en recordar: en aquest tipus de sistemes l'usuari ha de recordar i reproduir un gràfic només conegut per ell. Habitualment té la possibilitat de poder triar la seva contrasenya, cosa que en la majoria dels casos redueix el marge de seguretat. Això ho explicarem amb més detall al següent punt.

2.3.1. Draw-A-Secret (DAS) [7]

Aquest sistema consisteix en fer un dibuix a sobre una graella de NxN caselles amb un ratolí o un llapis òptic. Les caselles s'anomenen segons coordenades en dues dimensions (x,y) on $(x,y) \in [1, N] \times [1, N]$. La contrasenya en sí esdevé la seqüència de graelles per les quals ha passat el dibuix.

A l'exemple següent, veure Figura 3, la contrasenya seria la seqüència expressada en coordenades (x, y): (2,2), (2,3), (3,3), (3,2), (2,2), (1,2), (5,5) on (5,5) representa que s'aixeca el punter.

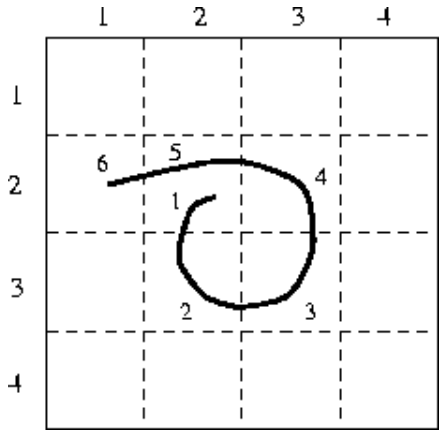

Figura 3

Un dels principals factors per determinar el grau de seguretat és l'espai mostral que pot oferir el sistema de contrasenyes. Aquest es determina sumant el total de combinacions possibles que es poden generar amb els elements disponibles. Una contrasenya alfanumèrica de 8 caràcters ASCII té un espai mostral de $95^8 \approx 2^{53}$ combinacions. En el sistema DAS, amb una graella de 5x5 fa falta una contrasenya de 12 caselles per superar l'exemple anterior: 2^{58} combinacions.

Aquestes xifres fan referència al total de combinacions en ambdós sistemes. Per fer més entenedora la robustesa del sistema DAS, comparem contrasenyes més simples. Un estudi [8] fet sobre 14.000 contrasenyes conclou que el 25% d'elles es poden trobar en un diccionari de només $3x10^6$ paraules de 8 lletres minúscules quan l'espai mostral és de $2x10^{14}$. Una contrasenya DAS simple pot ser el dibuix de un rectangle: aquest està format per dos línies verticals i dos horitzontals. Sobre una graella de 5x5 caselles es poden formar $2.56x10^6$ rectangles diferents. Aquesta xifra ja és gairebé igual al diccionari de 8 paraules anterior i es tracta només d'un tipus de dibuix simple. Es podrien trobar d'altres exemples de gràfics senzills i d'aquesta manera la quantitat de combinacions creix sense complicar la contrasenya.

En comparació al sistema alfanumèric, el sistema DAS té aproximadament el mateix espai mostral amb les particularitats que la

quantitat de contrasenyes simples o predictibles és més gran i que el format gràfic és més fàcil de memoritzar.

Variants d'aquest sistema són BDAS (*Background Draw a Secret*) i R-DAS (*Rotational Draw a Secret*). BDAS introdueix una imatge al fons de la graella. D'aquesta manera els usuaris tenen una ajuda visual que els permet fer dibuixos més complexes. R-DAS manté el mateix format que el disseny original però l'usuari pot girar la graella mentre està introduint la contrasenya. Aquests moviments incrementen la seguretat.

2.3.2. Passdoodle [9]

Aquest sistema és similar al DAS però té diversos trets diferencials. Es tracta de dibuixar un gargot amb el ratolí o llapis òptic sobre una àrea delimitada de la pantalla però sense tenir un fons en forma de graella, veure Figura 4. Aquest traç ha de coincidir amb l'emmagatzemat prèviament com a contrasenya secreta. La creació del traç original no és trivial. L'usuari ha d'enregistrar diverses proves com a entrenament i finalment el sistema de *Passdoodles* fa un contorn gaussià que és el que es compararà amb l'intent de l'usuari per autenticar.

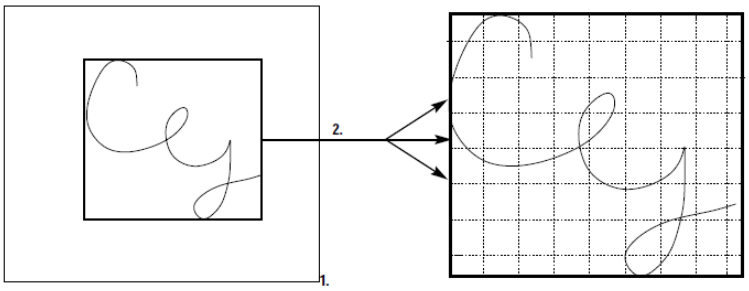

Figura 4

Per afegir seguretat la velocitat del traç també és una variable que forma part de l'autenticació. Així doncs, dos traços idèntics executats a velocitats diferents també seran diferents pel sistema que denegarà l'accés a aquell que no coincideix amb el patró que té per comparar.

Tot i que no és visible, el sistema fa servir una graella de 100x100 caselles per enregistrar els traços. Aquest esquema dóna un espai mostral teòric de 10^{400} *doodles* diferents sense tenir en compte la velocitat. En realitat l'espai és menor a causa de que traços que difereixen en poques graelles poden ser considerats iguals si coincideixen amb el contorn gaussià. Així doncs, l'espai mostral estarà limitat pel grau de precisió humana que es requereixi per autenticar.

Val a dir com a consideració final, que *Passdoodles* no és un sistema del tipus habitual on primer es demana un nom d'usuari que després s'autentica amb la contrasenya. En aquest cas, el *doodle* identifica i valida directament.

2.3.3. Pass-Go [10]

És un sistema que millora el DAS afegint seguretat fent la graella més gran i simplificant-ne l'ús. Està inspirat en el joc xinès *Go* i el principi de funcionament és l'elecció d'interseccions a una graella per part de l'usuari. Veure exemples a la Figura 5.

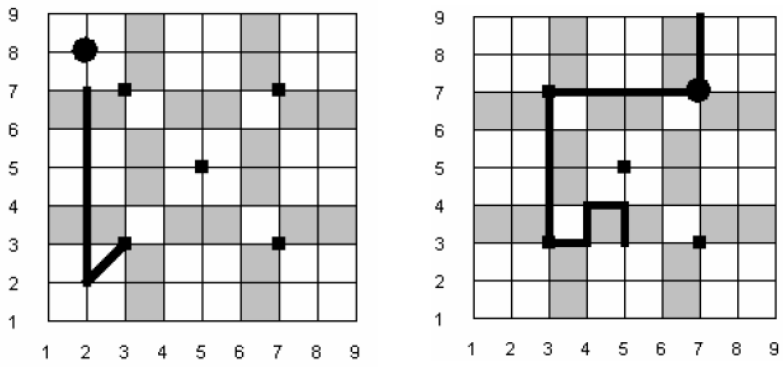

Figura 5

La diferència respecte DAS és que s'han de seleccionar interseccions de la graella en lloc de les caselles que la formen. Els dos avantatges que se'n deriven directament són que es poden dibuixar diagonals, cosa que és impossible seleccionant caselles, i que l'espai mostral augmenta amb

una graella de la mateixa mida. Una graella de NxN caselles té un espai de (N+1)x(N+1) interseccions.

Per fer l'espai mostral encara més gran, a la implementació final la graella té una mida de 9x9 caselles. Per tal evitar confusions de files i columnes en fer els traços, es van introduir unes ajudes referencials ombrejant caselles tal com es pot observar a la Figura 5. D'aquesta manera es minimitza la possibilitat que l'usuari cometi errades en el moment d'autenticar-se.

Cal destacar d'aquest sistema que la introducció de les ajudes referencials fa que els usuaris dissenyin contrasenyes més llargues cosa que dificulta els possibles atacs tant per força bruta com per *shoulder surfing*.

2.3.4. GrIDsure [11]

Aquest sistema és un producte comercial[3] i consisteix en introduir un PIN d'un sol ús. És a dir, cada vegada que un usuari s'ha d'autenticar el sistema genera un PIN nou que ha de ser teclejat. A la persona que ha d'introduir-lo se li mostra una graella de 5x5 caselles amb un número a cadascuna. El sistema es basa en que el que s'ha de recordar és un patró de 4 caselles de la graella i no en una seqüència de números. Aquests apareixeran aleatòriament a la graella.

A la Figura 6 es pot observar un exemple: la imatge de l'esquerra té el patró que ha de recordar l'usuari i la de la dreta mostra la graella que veuria en el moment d'intentar accedir al recurs. Seguint el patró a la graella amb números, el PIN per aquesta sessió seria *0 6 4 9*. L'usuari pot triar el patró a voluntat d'entre les 25 caselles de la graella.

[3] http://www.gridsure-security.co.uk/

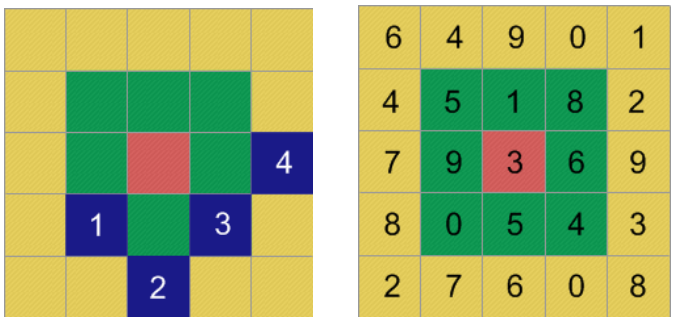

Figura 6

GrIDsure va ser concebut com una millora als PINs habituals de 4 xifres. En aquest sentit els supera àmpliament ja que soluciona els següents problemes: atacs de força bruta, *shoulder surfing*, captura de teclat i empremtes a la pantalla.

Sistemes basats en reconeixement: Estan basats en la memorització d'unes imatges que seran la contrasenya seleccionades d'entre totes les d'un catàleg. Posteriorment es presenten a l'usuari barrejades amb d'altres i es demana que les reconegui. Es pot utilitzar qualsevol tipus d'imatges com ara cares, figures polinòmiques, objectes, abstractes, etc. Són sistemes vàlids com a substituts de PIN numèrics ja que tenen un espai mostral similar.

2.3.5. PassFaces [12]

PassFaces és un producte comercial[4] i el mètode de funcionament consisteix en triar 4 o 5 cares d'una biblioteca d'imatges que s'han de recordar. Durant el procés d'autenticació es presenta una graella amb 9 cares on hi ha una de les que formen la contrasenya i s'ha de tocar. Veure Figura 7. Després apareix una segona graella similar a l'anterior amb una altra cara de les memoritzades que també s'ha de tocar i així successivament fins completar les identificacions de les 4 o 5 cares que formen la contrasenya. Per augmentar la seguretat respecte el *shoulder*

[4] http://www.passfaces.com/index.htm

surfing, totes les cares que apareixen són diferents i la seva posició es aleatòria cada vegada que s'executa el programa.

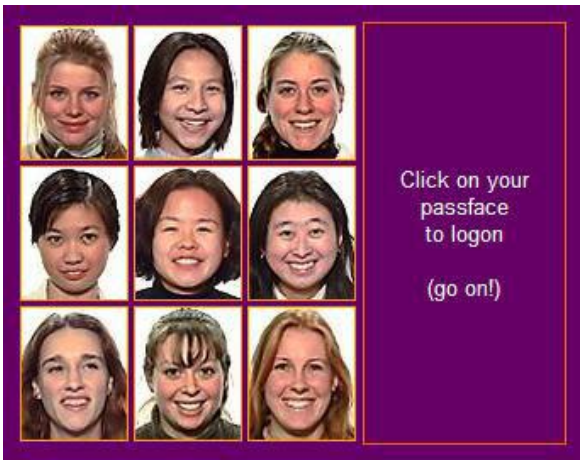

Figura 7

El principal avantatge de *PassFaces* és la facilitat que té l'ésser humà per recordar cares en comparació a text o fins i tot d'altres tipus d'imatges. Per contra, el sistema té un espai mostral molt similar al del sistema PIN, necessita recursos d'emmagatzemament per a les imatges i, el pitjor de tot, el procés d'autenticar és lent ja que requereix una mitja de 20 segons per completar-lo en el cas d'una seqüència de 5 graelles.

Estudis realitzats [7] sobre aquesta aplicació demostren que és un bon sistema per a connexions esporàdiques ja que la contrasenya és recordada més fàcilment que les alfanumèriques a l'utilitzar-la espaiada en el temps.

2.3.6. Déjà Vu [13]

És un sistema similar a *PassFaces* amb la particularitat que hi ha 10.000 imatges que formen la biblioteca i són abstractes. Veure Figura 8. Per a fer la contrasenya se n'han de triar 5. L'aparença de l'aplicació és una graella on es mostren 25 imatges on hi ha les 5 que l'usuari ha

d'identificar. L'espai mostral no és gaire extens ja que les combinacions de triar 5 elements d'entre 25 són $\binom{25}{5} = 53.130 \approx 2^{16}$.

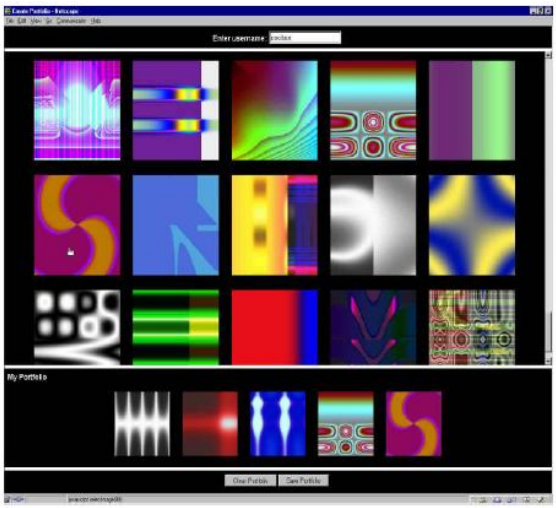

Figura 8

El punt fort del *Déjà Vu* consisteix en que és efectiu als atacs tipus diccionari. Això és així a causa de les imatges que formen la biblioteca són força homogènies i es fa difícil trobar un subconjunt que sigui el favorit dels usuaris com passa amb les paraules. De la mateixa manera també es fa difícil que un usuari pugui descriure amb exactitud les imatges de la seva contrasenya a un tercer i que aquest les identifiqui correctament a causa de les diferents percepcions que té la gent davant d'una mateixa descripció.

Sistemes basats en pistes: Recordar és un exercici que requereix esforç i estímul. Per tant, també és aplicable a la utilització de sistemes d'autenticació mitjançant contrasenyes. Per conseqüent, és lògic que si hi afegim pistes, llavors és més fàcil recordar-les i fins i tot complicar-les.

2.3.7. Graphical password, G. Blonder [14]

Greg Blonder va ser la primera persona en patentar una contrasenya gràfica. Es va adonar que els atacs a les contrasenyes alfanumèriques esdevenien cada vegada més ràpids i efectius a mesura que augmentava la potència dels ordinadors, així que va pensar la manera de crear un format nou més resistent als atacs.

El sistema és molt simple i consisteix en una imatge predeterminada que alhora té unes àrees també predeterminades on l'usuari ha de tocar en una seqüència concreta. Veure Figura 9.

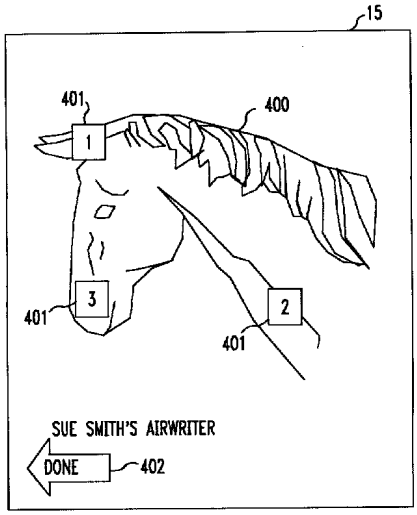

Figura 9

Blonder el va crear l'any 1995 quan les contrasenyes més habituals eren en format PIN. Per tant, a la patent, considera una gran millora augmentar de les 10.000 combinacions que té un PIN de 4 dígits o les 17.000 d'un de 3 lletres a les 13.6 milions que es poden aconseguir amb una graella de 7.5x12.5cm que conté caselles de 6x6mm.

Greg Blonder no va fer cap modificació al seu invent. Simplement el va patentar i no va tenir interès en desenvolupar-lo més enllà de disseny inicial.

2.3.8. PassPoints [15]

És una evolució del sistema anterior ja que soluciona les seves limitacions. L'esquema consisteix en una imatge, oferta pel sistema o del propi usuari, amb gran quantitat de detalls. Veure Figura 10.

Figura 10

Per crear la contrasenya s'han de seleccionar 5 punts qualsevol dins de tota l'àrea de la imatge sense limitacions de zones predefinides. Aquests punts s'han de reproduir en el mateix ordre que es van triar per autenticar la sessió al recurs. L'espai mostral depèn del nivell de tolerància aplicada a la zona on s'ha de picar amb el ratolí o llapis digital. Això crea un problema en generar el *hash* de la contrasenya, ja que si es seleccionen dos píxels diferents, el codi *hash* no serà el mateix. Per solucionar-ho s'utilitzen tres graelles de discretització simultàniament. Les graelles no són visibles per a no influir en l'elecció del punt.

L'espai mostral, una vegada més, és superior al d'una contrasenya alfanumèrica de 8 caràcters [16] amb només una seqüència de 5 clicks a sobre de la imatge.

2.3.9. Cued Click Points [17]

És un sistema evolucionat del proposat per *PassPoints*. El mètode per autenticar és idèntic: s'han de reconèixer 5 punts però no d'una única fotografia sinó en aquest cas en 5 fotografies diferents a raó d'un únic punt per imatge. Es deixa a l'usuari l'opció de triar les 5 fotografies que serviran per la seva contrasenya. El sistema està pensat per a tenir les imatges a una base de dades al servidor i autenticar des del costat client mitjançant una connexió segura SSL/TLS.

El funcionament és el següent: apareix la primera imatge i l'usuari ha de tocar el punt que forma part de la seva contrasenya. Si ho fa correctament apareix la segona imatge, es repeteix el procés amb la resta d'imatges i si els punts tocats són els correctes es fa la validació. En cas que no s'hagi encertat al tocar algun dels punts, apareix una imatge, com si continues l'autenticació, però és una de diferent a l'esperada. Dit d'una altra manera, el punt tocat determina la següent imatge. Així, la persona sap que s'ha equivocat però no es mostra cap missatge d'error fins al final del procés. Veure Figura 11. La quantitat de fotografies és de 1.200, que correspon amb la de caselles per imatge que defineixen la tolerància del punt a tocar.

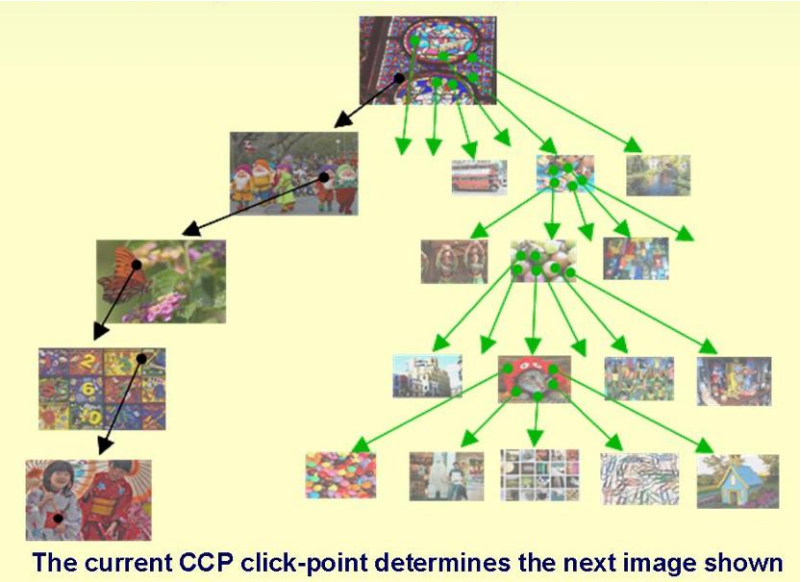

Figura 11

La millora que aporta aquest esquema és que a l'única imatge de *PassPoints* es poden identificar *punts favorits* on hi ha més probabilitat que les persones triïn com a part de la contrasenya. En el cas de *Cued Click Points* un atacant hauria de buscar aquestes zones a 1.200 imatges.

2.3.10. Persuasive Cued Click-Points [18]

Persuasive Cued Click-Points, o PCCP, és una proposta de millora a *PassPoints* i al mètode anterior o CCP. Un dels problemes associat a ambdós sistemes és la tendència dels usuaris a triar els punts favorits coneguts com a *hotspots*. PCCP intenta solucionar-ho delimitant la zona on s'han de triar els punts de la contrasenya a una finestra de reduïdes dimensions posada sobre la imatge aleatòriament. Veure Figura 12.

Figura 12

La intenció és persuadir als usuaris a triar punts localitzats més a l'atzar durant la creació de la contrasenya. Un estudi [18] fet comparant els dos sistemes, CCP i PCCP, revela que efectivament els punts triats amb PCCP estan distribuïts més aleatòriament. A la Figura 13 es pot observar aquest fet: les zones en colors groc, taronja i vermell corresponen als *hotspots* de la imatge de la Figura 12 i els cercles de color blau corresponen als punts triats com a part de la contrasenya. És evident

que en el sistema PCCP n'hi ha més fora dels *hotspots* que en el CCP. Per contra, utilitzant PCCP, la taxa d'encert a l'hora de tocar els punts en el moment de reproduir la contrasenya disminueix lleugerament a causa que aquests no són tant evidents com els *hotspots*.

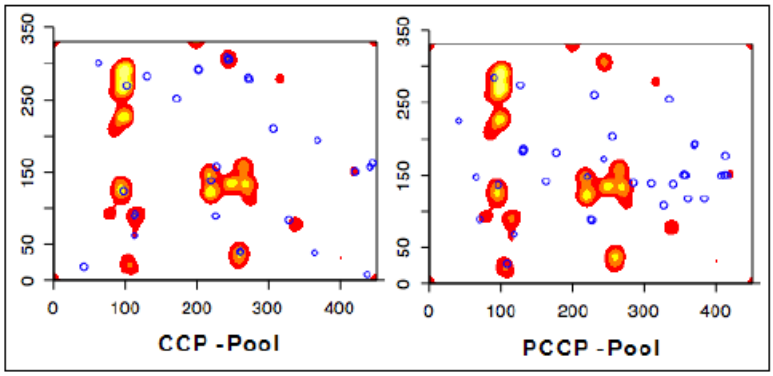

Figura 13

2.3.11. Inkblot Authentification [19]

Aquest sistema és una patent de *Microsoft Corporation*® i està basat en les taques de tinta del test de *Rorschach*[5] tot i que no s'utilitzen les mateixes taques ja que són massa ambigües per a l'objectiu que es fan servir. Per aquest motiu, les taques són generades automàticament per un algoritme. D'aquesta manera és possible generar taques diferents per a cada usuari.

Inkblot Authentification no és rigorosament un sistema de contrasenyes gràfiques. La manera d'autenticar és mitjançant una cadena alfanumèrica introduïda pel teclat amb l'ajuda de les taques com a pistes per recordar els caràcters a introduir. Els creadors estaven interessats en els mètodes gràfics però consideraven que són útils per a dispositius mòbils. No obstant, en altres situacions, una tercera persona pot observar la contrasenya fent el que coneixem com *shoulder surfing*. El *shoulder surfing* es descriurà amb detall més endavant.

[5] http://es.wikipedia.org/wiki/Test_de_Rorschach

El funcionament és el següent: es mostren 10 taques de tinta a l'usuari d'una en una. Per a cada taca s'ha introduir la primera i la darrera lletra de la descripció que aquesta suggereix. Per exemple, a la taca central superior de la Figura 14 algú pot veure una 'mosca obesa', llavors s'han d'introduir les lletres 'ma' com part de la contrasenya.

Figura 14

L'objectiu de l'esquema és crear una contrasenya alfanumèrica complexa amb l'ajuda de les taques i que amb l'ús continuat no faci falta utilitzar-les cada vegada per autenticar. De tota manera, en cas d'oblidar la seqüència de caràcters sempre es podria disposar de les 10 taques per recordar-la.

2.4. Punts febles

Tot i que la raó de ser de les contrasenyes gràfiques és millorar les alfanumèriques en quant a experiència d'ús i seguretat, no estan exemptes de vulnerabilitats. Són aquestes les que els atacants intenten aprofitar per trencar les contrasenyes, suplantar al propietari i accedir a un recurs determinat.

Per punts febles considerem aquelles característiques que permeten a una persona obtenir la contrasenya d'algú altre sense el seu permís. Hi ha dues maneres d'obtenir-la il·lícitament: endevinant-la o bé captant-la.

Mètodes endevinatoris: L'atacant intenta obtenir la contrasenya utilitzant mètodes repetitius fins que l'aconsegueix.

2.4.1. Força bruta

És la manera més senzilla d'obtenir una contrasenya. Consisteix simplement en provar totes les que formen part de l'espai mostral fins que es descobreix la que funciona. La defensa contra aquest atacs esdevé immediata: augmentar l'espai mostral fins que es fa inviable provar totes les alternatives en termes de temps.

Com a exemple es pot fer la següent comparació. Per un costat, un sistema de PIN de 4 xifres que es pot endevinar manualment amb una mica de paciència ja que consta de 10.000 combinacions. Per una altra banda, una contrasenya de longitud 8 d'un alfabet de 86 caràcters té un espai mostral de $86^8 \approx 2^{51}$. Per a comprovar totes les possibles combinacions, provant-ne un milió cada segon, necessitaríem 94 anys[6]. Evidentment, no té sentit realitzar aquest esforç.

2.4.2. Atacs de diccionari

És la versió reduïda i optimitzada dels atacs per força bruta. La sistemàtica és la mateixa però s'inicia l'atac per les opcions més probables. En el cas de les cadenes de text, es proven paraules conegudes que hom pot trobar a un diccionari, d'aquí el nom del tipus d'atac, i en el cas de números es proven telèfons, matrícules, dates d'aniversaris, etc.

Amb una mostra reduïda de l'espai mostral s'aconsegueix un índex elevat d'encert com ara la llista presentada a la introducció. Per protegir-se dels atacs de diccionari s'han de triar contrasenyes formades per una successió de caràcters sense sentit en cap llengua. Una tècnica per fer-ho és utilitzar la primera lletra de cada paraula

[6] http://www.lockdown.co.uk/?pg=combi

d'una frase fàcil de recordar. Un exemple seria: *L'any 2013 vaig fer el TFC a la UOC*. I la contrasenya seria: *La13vfeTalU*.

2.4.3. Atacs de diccionari aplicats a sistemes gràfics

En sistemes on l'usuari ha de dibuixar la seva contrasenya hi ha la tendència de fer gràfics simples, figures geomètriques senzilles (cercles, quadrats, triangles, rectangles, etc) o, fins i tot, es dibuixen lletres com ara la inicial del propi nom.

Un atac que conté aquestes formes geomètriques en una base de dades i comença per elles per minimitzar els intents de trencar la contrasenya és considerat un atac de diccionari equivalent als alfanumèrics.

També es poden incloure en aquest grup els *hotspots* dels sistemes gràfics basats en imatges. La tendència a triar unes zones de la imatge respecte la resta perquè destaquen més o són més atractives també és explotat en aquest tipus d'atac.

En definitiva són trets predictibles de les preferències humanes tot i que els atacs de diccionari en sistemes gràfics són més complicats de portar a terme, ja que s'ha de fer una anàlisi prèvia de cada imatge utilitzada pel sistema o de les diferents variants que s'utilitzi per crear un patró propi.

Mètodes de captura: L'atacant intenta obtenir la contrasenya d'una altra persona en el moment d'utilitzar-la a l'autenticar, ja sigui mitjançant observació visual directa o amb càmeres, amb software, etc. També és possible obtenir-la posteriorment o forçar a revelar-la amb enganys.

2.4.4. Shoulder surfing

Shoulder surfing es podria traduir per '*observar per sobre de l'espatlla*'. Tal com indica la traducció, es tracta d'observar directament com algú introdueix la seva contrasenya. Una manera més sofisticada de fer-ho

és utilitzant prismàtics o càmeres de vídeo. És relativament fàcil obtenir el PIN d'una targeta de crèdit del client precedent a un comerç o a un caixer automàtic mirant directament al teclat ja que acostumen a estar poc protegits de les mirades alienes. De fet molt sovint no és necessari ni veure les tecles ja que amb el gest del moviment del dit n'hi ha prou per endevinar la clau.

Així doncs, un sistema de contrasenyes molt resistent a atacs de força bruta i de diccionari no és robust utilitzat a un cibercafè o a la biblioteca, on qualsevol persona pot estar observant sense adonar-nos-en.

Hi ha diverses propostes [20][21] de sistemes que són resistents a l'observació directa de la introducció de la contrasenya fins i tot gravant el procés en vídeo. Una opció intermèdia que resisteix moderadament el *shoulder surfing* és el sistema *GrIDsure* presentat anteriorment, veure punt 2.3.4. Per obtenir el patró que fa realment de contrasenya és necessari observar diversos accessos al recurs gravats en vídeo ja que difícilment es pot arribar a deduir només amb observació visual.

2.4.5. Empremtes a la pantalla

Hi ha sistemes de contrasenya gràfica que requereixen dibuixar un patró amb el dit a una pantalla tàctil. Un exemple és el desbloqueig de pantalla dels mòbils Android. El sistema consta de nou punts que s'han d'unir seguint un patró establert prèviament per l'usuari. Cada vegada que es vol accedir al telèfon cal repetir aquest patró. Els dits de les mans, encara que estiguin netes, tenen restes de greix que es queda adherit a la pantalla en tocar-la.

Especialment interessant és l'estudi '*Smudge attacks on smartphone touch screens*'[7] [22]. En ell es fan diversos assajos per avaluar la capacitat d'obtenir una patró fet sobre una pantalla tàctil mitjançant

[7] *Smudge attacks on smartphone touch screens':* Atacs de taques sobre pantalles tàctils de telèfons intel·ligents.

fotografies fetes sota diferents angles i en diverses condicions de la pantalla. Els autors revelen que les taques que es deixen amb els dits poden ser captades fins i tot amb restes d'altres ditades a sobre del patró i amb la pantalla parcialment neta de treure i guardar el mòbil a la butxaca. Veure Figura 15.

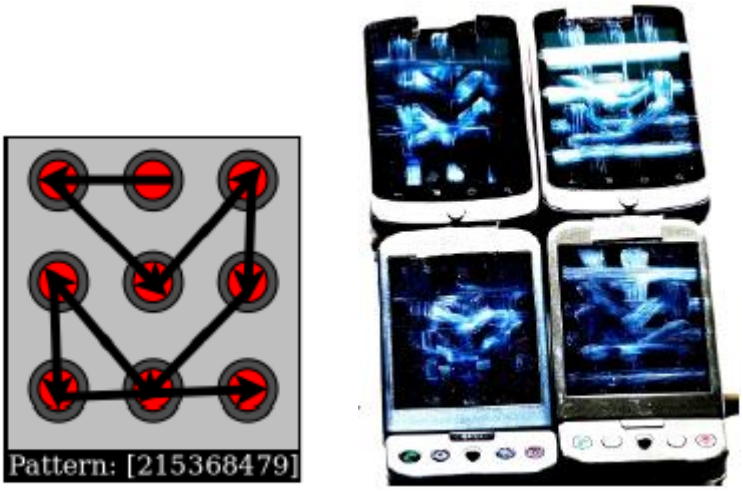

Figura 15

2.4.6. Atacs amb programari

Les tècniques habituals són introduir programari dins d'un equip sense consentiment del propietari que sigui capaç de captar les seves contrasenyes. També són habituals els mètodes que imiten amb tot detall una pàgina d'Internet que hom utilitza com a client i sol·licita el nom d'usuari i la contrasenya.

En el cas dels sistemes gràfics, aquests atacs són més difícils de reproduir ja que l'atacant ha de conèixer quines imatges són utilitzades en sistemes tipus *PassFaces*, *PassPoints*, CCP, etc.

3. Elecció de sistema de contrasenya gràfica

Actualment els sistemes de contrasenya gràfica encara no són abastament utilitzats. A nivell personal sempre que m'he registrat com a usuari a diferents serveis oferts a Internet, sempre se m'ha demanat una contrasenya alfanumèrica amb diferents graus de complexitat. De fet, l'únic sistema gràfic que conec és el desbloqueig de pantalla per patró dels telèfons que utilitzen el sistema operatiu Android.

Així doncs, l'elecció consisteix a crear un sistema gràfic nou que és una variació del sistema PIN amb l'estètica del patró Android. A continuació es fa una descripció dels sistemes de desbloqueig de pantalla als telèfons Android i la justificació de la proposta es farà al següent capítol.

3.1. Desbloqueigs d'Android

El sistema operatiu Android utilitza el bloqueig de pantalla per dos motius. El primer és per protegir el telèfon d'accessos involuntaris. El telèfon en repòs té la pantalla apagada per estalviar bateria. Com a norma general, per encendre-la s'utilitza un botó. Per evitar que si es prem aquest botó accidentalment, la pantalla estigui constantment encesa, que s'activin aplicacions o, fins i tot, que es facin trucades tenint el telèfon a la butxaca, s'ofereix la possibilitat d'incorporar un segon pas per fer la pantalla accessible. El segon motiu és per evitar accessos no autoritzats de terceres persones. Els diferents desbloqueigs són els següents:

3.1.1. Lliscament del dit

Després de prémer el botó d'encesa de la pantalla apareix un cercle amb un cadenat al centre que s'ha de lliscar en qualsevol direcció. Veure Figura 16.

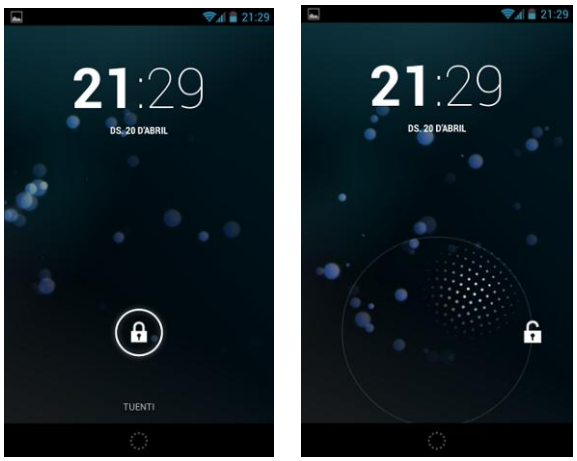

Figura 16

Aquest mètode no aporta cap seguretat extra tret dels motius comentats anteriorment per evitar els accessos involuntaris.

3.1.2. PIN o contrasenya

Mètode tradicional alfanumèric que està disponible en les dos versions: PIN de mínim 4 dígits i contrasenya alfanumèrica. El mètode més utilitzat és el PIN ja que encara que només té un espai mostral de 10.000 possibles combinacions és suficient ja que no és possible un atac per força bruta. Després de 3 intents erronis el terminal queda bloquejat. Veure Figura 17.

Figura 17

És el favorit dels usuaris per la velocitat amb què es pot introduir la contrasenya.

3.1.3. Desbloqueig facial

Des de la versió 4.0 d'Android, coneguda com Ice Cream Sandwich, s'incorpora com a novetat el desbloqueig de la pantalla utilitzant la càmera frontal del telèfon i enfocant la cara del propietari. Com a concepte és molt original però realment poc segur, amb una simple fotografia es pot enganyar al sistema. Veure Figura 18.

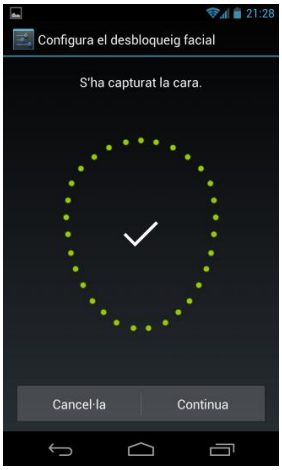

Figura 18

3.1.4. Patró

Es tracta d'un sistema de contrasenya gràfica introduït al sistema operatiu Android a partir de la versió 2.2 més coneguda com Froyo. Consisteix en crear un patró gràfic unint els nou punts distribuïts a la pantalla formant una graella. No és necessari utilitzar-los tots però el mínim per a que el patró sigui vàlid és de 4 unitats. Veure Figura 19.

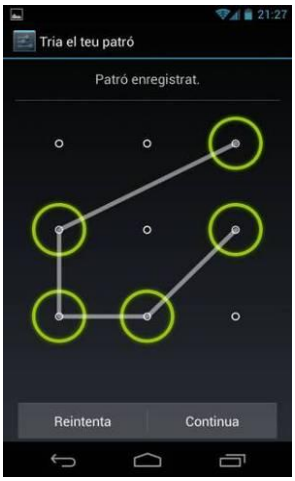

Figura 19

Aquest sistema s'ha popularitzat a causa de l'originalitat i a que, com el mètode PIN, també és força ràpid.

4. Proposta de millora: l'aplicació TAP DOTS!

Com es va indicar a l'inici de la memòria, el TFC té dos objectius. El primer consisteix a fer una presentació de les contrasenyes gràfiques més representatives que existeixen actualment. Aquesta tasca s'ha portat a terme al llarg dels capítols 2 i 3. El segon objectiu és desenvolupar un sistema nou, a partir d'un d'existent, millorant punts febles d'aquest.

4.1. Justificació de la proposta

Al desembre de 2012 vaig decidir fer el meu TFC en l'àrea de seguretat informàtica en llegir la proposta que s'oferia sobre les contrasenyes gràfiques. Em va semblar força interessant tot i no tenir cap coneixement relacionat amb el tema. L'únic sistema que coneixia d'aquest tipus era el sistema de desbloqueig de pantalla per patró d'Android. També coneixia el sistema basat en PIN que també fan servir als sistemes operatius per a telèfons mòbils, caixers automàtics, compres en comerços, etc. però no es tracta d'un sistema gràfic.

Una vegada vaig tenir decidit que demanaria aquesta proposta concreta de TFC, vaig començar a pensar com podria ser el nou sistema i com podria millorar els que jo ja coneixia. Només tenia la informació que hi ha al pla docent en relació a les contrasenyes gràfiques i a les característiques de s'havien de millorar, que són les següents:

- La mida teòrica de l'espai de contrasenyes
- La mida real (pràctica) de l'espai de contrasenyes
- La dificultat de fer "shoulder surfing" de l'esquema proposat
- La dificultat de recuperar la contrasenya a partir de la informació residual d'una autenticació satisfactòria (per exemple, les ditades deixades a la pantalla)
- La capacitat d'emmagatzemament necessària per implementar el sistema
- La facilitat de recordar la contrasenya

- El temps necessari per introduir la contrasenya

Així doncs, la meva idea girava al voltant d'aquestes especificacions.

Se'm va acudir fer un combinat dels dos sistemes més populars als telèfons Android: PIN i patró. M'agradava el format del sistema patró i la senzillesa del PIN. Bàsicament, el nou sistema consisteix a canviar els números del sistema PIN per imatges simples, tot imitant l'estètica del sistema patró però evitant que la seva funcionalitat fos la mateixa per evitar el punt feble de les ditades a la pantalla. Després de valorar diverses opcions, em vaig decidir per cercles de colors. Com a curiositat, en ple procés de pluja d'idees, vaig tenir la pensada de substituir els cercles de colors per fotografies de cares dels contactes de l'agenda o de Facebook en una graella 3x3. La meva sorpresa va ser molt gran, mentre recopilava informació de contrasenyes gràfiques, ja que vaig descobrir que aquest sistema ja existeix: el PassFaces.

Més tard, mentre anava coneixent més i més sistemes de contrasenya gràfica, em vaig adonar que aquests, per aportar millores i/o diferenciar-se de la resta, creixen en complexitat. Cada vegada que analitzava un nou sistema, es feia més difícil triar-ne un per veure què es podia millorar. Així doncs, la meva elecció va ser quedar-me amb la idea original.

4.2. L'aplicació TAP DOTS!

Aquesta segona part del TFC requereix dissenyar un sistema de contrasenya gràfica i desenvolupar una aplicació que l'implementi. Més endavant, es faran proves amb usuaris reals per observar les seves reaccions i analitzar si realment hi ha millores respecte al model original modificat.

El disseny proposat consisteix en substituir el números d'un teclat per introduir PINs (figura 20) per cercles de color (figura 21).

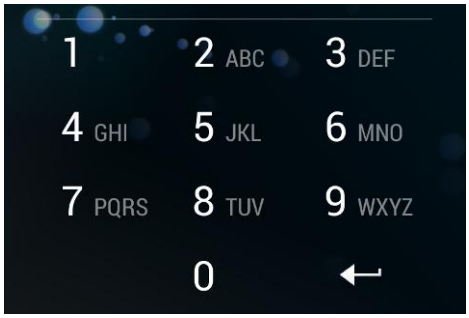

Figura 20

Figura 21

L'especificació de funcionament és la següent:

- La contrasenya la formen 4 colors a triar per l'usuari d'entre un conjunt de 12 elements amb possibilitat de repetició. Quan s'utilitzi el sistema de contrasenya, aquests 4 colors s'hauran d'introduir sempre en el mateix ordre.
- El conjunt està format pels 12 colors següents:
  - Blanc
  - Groc
  - Taronja
  - Vermell
  - Blau clar
  - Blau fosc
  - Verd clar
  - Verd fosc
  - Lila
  - Violeta
  - Rosa
  - Negre

- A la pantalla es mostra una graella de 3 x 3 colors on hi haurà sempre els 4 que formen part de la contrasenya de l'usuari més 5 triats aleatòriament de la resta del conjunt de colors.
- La posició dels colors a la graella no és fixa. Cada vegada que apareixen per pantalla per tal de desbloquejar el dispositiu, es mostren distribuïts a l'atzar.
- Es permeten 3 intents de validació. En cas d'errar 3 vegades consecutives, l'aparell es bloqueja i caldrà un mètode alternatiu per alliberar-lo.

4.2.1. Millores aportades

La finalitat del nou sistema gràfic és millorar les característiques del sistema PIN. Per tant, compararem les peculiaritats de tots dos tot justificant les millores.

- Mida teòrica i real de l'espai de contrasenyes: En tots dos casos, tant la mida teòrica com la real coincideix, ja que és factible utilitzar totes les contrasenyes de l'espai mostral.

  Sistema PIN: s'utilitzen 4 elements d'un conjunt de 10. Per tant, la mida de l'espai mostral és de 10^4 = 10.000 elements.

  Sistema TAP DOTS!: també es fan servir 4 elements, però d'un conjunt de 12 elements. D'aquesta manera l'espai mostral és de 12^4 = 20.736 elements.

  Només afegint 2 elements nous, l'espai mostral ha augmentat significativament i passa a ser més del doble. Per fer-lo créixer encara més, es podrien incorporar més elements com ara colors tipus fosforescents per diferenciar-los de la resta. Altres tonalitats de colors no són aconsellables ja que podrien generar confusió i provocar errades en el moment d'autenticar.

- Dificultat de fer 'shoulder surfing': aquest punt no és fàcil de quantificar, però s'intenta dificultar el 'shoulder surfing' afegint

la posició aleatòria dels elements en el moment de mostrar-los per introduir la contrasenya. En el sistema PIN els números estan sempre en la mateixa posició, així doncs, és possible obtenir la contrasenya d'algú només observant el patró utilitzat a sobre del teclat encara que no es tingui visió directa dels números.

Amb el sistema TAP DOTS! s'ha de tenir visió directa dels cercles de colors per poder obtenir la contrasenya, no n'hi ha prou amb observar el patró fet pel dit de l'usuari.

- La dificultat de recuperar la contrasenya a partir de la informació residual d'una autenticació satisfactòria (per exemple, les ditades deixades a la pantalla): el fet que els cercles de color apareguin de forma aleatòria a la pantalla fa que les ditades que queden sobre ella també siguin uniformes sobre els 9 elements tàctils, com es pot observar a les figures següents.

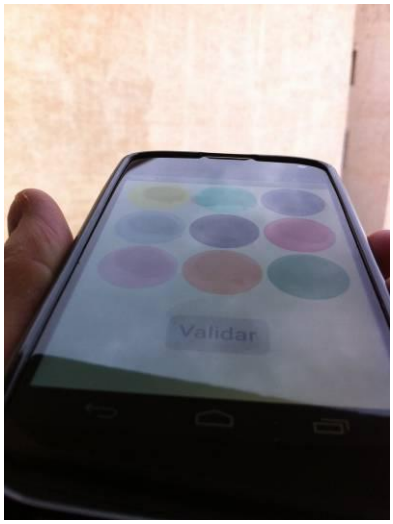

Figura 22

Figura 23

- La capacitat d'emmagatzemament necessària per implementar el sistema: en aquest punt el sistema TAP DOTS! no millora les característiques del PIN ja que requereix tenir emmagatzemats els elements gràfics per funcionar. De tota manera, els recursos necessaris són mínims i assumibles per qualsevol dispositiu

actual. Cada cercle de color és un fitxer d'imatge amb extensió JPG d'entre 3 i 4 KBytes.

En qualsevol cas, difícilment un sistema gràfic pot reduir la capacitat d'emmagatzemament d'un sistema PIN.

- Facilitat de recordar la contrasenya: una de les característiques dels sistemes de contrasenya gràfica és que són, o haurien de ser, més fàcils de recordar. En el cas particular de l'aplicació TAP DOTS! no s'observa gran diferència respecte el sistema PIN. De les proves realitzades amb usuaris se'n desprèn que la contrasenya utilitzada formada per 4 colors es recorda amb facilitat. La posició aleatòria dels cercles de colors en el moment d'autenticar té una doble missió: dificultar el 'shoulder surfing' i forçar a recordar la contrasenya en lloc d'un patró sobre una pantalla.
- Temps necessari per introduir la contrasenya: més endavant s'explicarà amb detall com s'han dut a terme les proves amb usuaris, on es podrà veure que els temps d'introducció de la contrasenya, tot i ser superiors, són propers als del sistema PIN. De fet, amb pràctica, es poden igualar.

4.2.2. Disseny de l'aplicació

El disseny de l'aplicació real que s'ha utilitzat per implementar el sistema TAP DOTS! difereix lleugerament de l'especificació. S'han simplificat certes característiques que han permès reduir el temps de desenvolupament i ajustar-lo al previst a la planificació temporal del pla de treball.

L'aplicació no implementa un sistema real de desbloqueig d'un dispositiu mòbil. Com s'indica al pla docent del TFC, es tracta només d'un prototip per poder experimentar amb usuaris. Així doncs, s'ha creat una aplicació per a telèfon amb SO Android que simula la interacció amb el sistema dissenyat.

Al disseny original, el sistema consta d'un conjunt de 12 colors on n'apareixen només 9 a la pantalla escollits a l'atzar, però que inclou sempre els 4 que formen la contrasenya. A l'aplicació s'ha reduït el conjunt als 9 elements que surten a la pantalla, que són: groc, taronja, vermell, verd, blau clar, blau fosc, rosa, lila i negre.

L'aplicació mostra en pantalla els 9 cercles de color en una graella de 3 x 3 i un botó per validar la contrasenya introduïda. Si l'usuari l'encerta, apareix el missatge 'Contrasenya correcta' en color verd i 'Contrasenya incorrecta' en color vermell en cas contrari. Veure Figures 24 i 25.

Figura 24

Figura 25

Cada vegada que apareixen els cercles de colors a la pantalla per introduir la contrasenya ho han de fer en posicions diferents respecte a la darrera vegada que es va fer una autenticació. Per simular aquesta posició aleatòria s'han creat 10 pantalles amb els cercles en diferents disposicions. Veure figura 26.

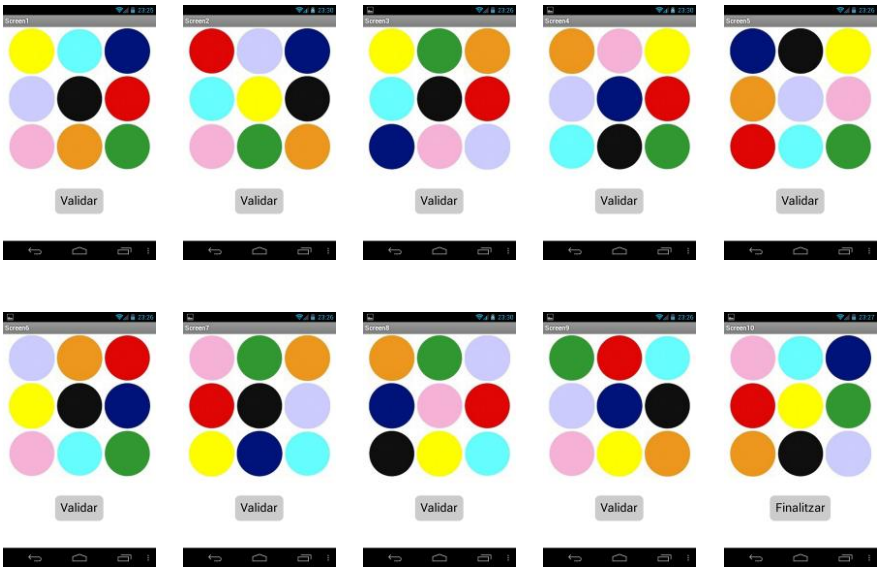

Figura 26

Finalment, en una aplicació real, l'usuari podria triar la seva contrasenya. En aquest cas, novament per simplificar el desenvolupament, l'aplicació funciona només amb una contrasenya predeterminada que és: blau clar, vermell, verd i groc, en aquest ordre.

El funcionament és, doncs, intuïtiu. En engegar l'aplicació, apareix la primera pantalla i l'usuari ha d'introduir la contrasenya descrita abans i prémer la tecla 'Validar'. A continuació, es mostra la pantalla 2 que té els cercles de colors en posicions diferents a les de la primera. L'usuari ha de repetir la contrasenya i prémer una altra vegada la tecla 'Validar'. S'ha de repetir aquestes operacions fins completar les 10 pantalles.

L'aplicació s'ha implementat amb 10 pantalles diferents per poder obtenir dades de la interacció dels usuaris amb ella. El sistema real només constaria d'una única pantalla que donaria accés al recurs en cas d'introduir la contrasenya correcta.

4.2.3. Desenvolupament de l'aplicació

Per a fer proves amb el disseny de sistema gràfic de contrasenyes, es fa necessària una petita aplicació però que sigui el més real possible. El

sistema de contrasenyes està pensat per a un dispositiu mòbil com ara un telèfon o tauleta digital. Per aquest motiu, s'ha decidit fer una aplicació basada en el sistema operatiu Android. Desenvolupar-la des de zero programant amb l'SDK propi d'Android hagués necessitat més temps del disponible segons la planificació temporal del pla de treball. Per aquest motiu, l'aplicació s'ha desenvolupat amb el software MIT App Inventor [23], fet que ha permès reduir el temps de desenvolupament i depuració.

L'App Inventor for Android és un programari inicialment desenvolupat com un dels molts projectes de recerca de l'empresa Google. Es va posar a disposició del públic al juliol de 2010 però al desembre de 2011 Google va deixar de donar-hi suport. En lloc de desaparèixer, el Massachusetts Institute of Technology, més conegut com MIT, va decidir continuar el seu manteniment. El nom actual és MIT App Inventor.

El MIT App Inventor permet desenvolupar aplicacions Android simples a persones amb coneixements bàsics de programació [24][25]. El seu funcionament està basat en web i consisteix en dues interfícies gràfiques. Una on es distribueixen els elements visibles i invisibles, que formaran part de la interacció amb l'usuari, dins d'una àrea que simula la pantalla. L'altra és on es programa el codi amb l'ajuda de sentències senzilles en forma de blocs que encaixen uns amb els altres com si es tractés d'un trencaclosques.

Tot i que el MIT App Inventor fa més simple la programació, és necessari un aprenentatge del programari per poder executar correctament allò que es vol implementar. També cal un període d'adaptació a aquesta nova forma de programar ja que el concepte és totalment diferent i s'han de assimilar les diferències respecte a fer-ho en Java amb un IDE.

Primer de tot cal crear la distribució dels elements que hi formaran part a l'àrea de la pantalla. A la vista principal del programari MIT App Inventor tenim totes les eines que ho permeten. Veure figura 27.

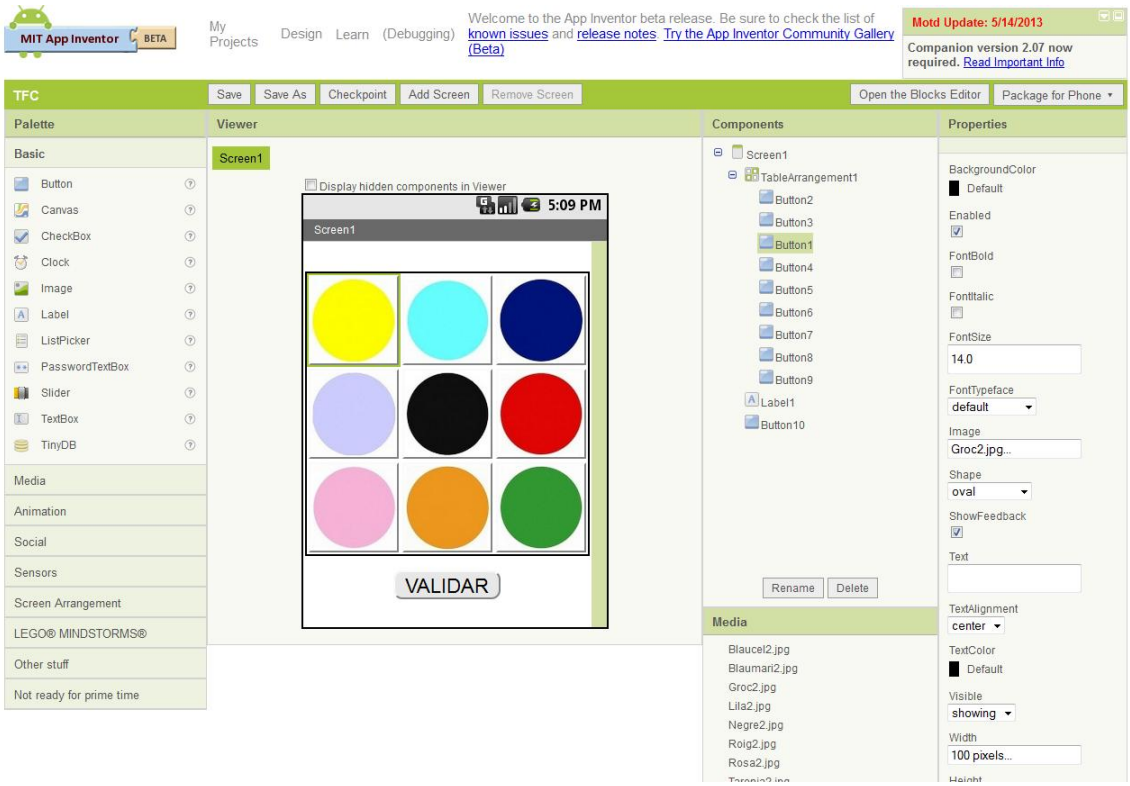

Figura 27

Aquesta part és molt simple. S'arrossega sobre l'àrea de la pantalla un element del tipus 'TableArrangement' que distribuirà 9 tecles en una graella de 3 x 3. Així doncs, sobre la taula de distribució, s'afegeixen 9 tecles. Després, a cadascuna se li assigna una imatge que és un cercle de color. Prèviament, haurem importat els 9 fitxers JPG amb les imatges dels cercles de colors.

Les tecles estan numerades de l'1 al 9 i cadascuna li correspon un únic color. La distribució és la següent:

- Tecla 1 – color groc
- Tecla 2 – color blau clar
- Tecla 3 – color blau fosc
- Tecla 4 – color lila
- Tecla 5 – color negre
- Tecla 6 – color vermell

- Tecla 7 – color rosa
- Tecla 8 – color taronja
- Tecla 9 – color verd

S'afegeixen dos elements més: una etiqueta que mostrarà el missatge 'Contrasenya correcta' o 'Contrasenya incorrecta' segons convingui i una desena tecla amb la llegenda 'VALIDAR' que servirà per confirmar la contrasenya introduïda i passar a la següent pantalla. Aquest procés s'ha de repetir per a les 10 pantalles que formen part de l'aplicació. Com s'ha explicat al punt 5.2.2., és en aquesta seqüència de pantalles on es col·loquen els cercles de colors en diferents posicions a cadascuna per simular l'aleatorietat.

Una vegada es tenen les pantalles definides s'ha de generar el codi per dotar de funcionalitat cada pantalla. En aquest punt s'obre l'editor de blocs del MIT App Inventor. S'anomena editor de blocs perquè totes les sentències, variables, etc. que s'utilitzaran per a programar són blocs en forma de peça de trencaclosques. Es tracta d'una finestra on s'editen els elements que hem afegit a la pantalla. És aquí on se'ls dotarà de funcionalitat per a quan l'usuari interactuï amb el dispositiu.

Aquesta tasca m'ha resultat complexa d'entendre pel costum de programar seguint un fil argumental lògic amb ajuda de procediments, típic de la programació estructurada o orientada a objectes. Més encara quan els blocs que formen el codi del programa es poden deixar escampats per l'editor sense ordre i barrejats. El resultat final és d'una simplicitat tal que pensava que no podria funcionar d'aquesta manera.

Primer exposarem la funcionalitat de cara a l'usuari i després explicarem la manera com s'ha solucionat. L'usuari ha de introduir la contrasenya, recordem que és la seqüència de colors blau clar, vermell, verd i groc, i després l'ha de validar prement la tecla 'VALIDAR' que ens dirà si és correcta o no i passarà a la següent pantalla.

Programant amb blocs s'ha solucionat creant una variable de tipus llista segons la figura 28 on s'hi guardaran els números que corresponen a les tecles quan aquestes siguin premudes.

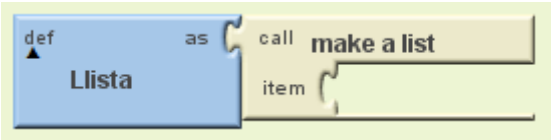

Figura 28

Prémer una tecla és un esdeveniment que genera una acció. En el cas de les tecles de l'1 al 9 que corresponen als cercles de colors, l'acció a realitzar és que s'introdueixi el número relacionat amb el color a la llista. Això es fa amb els blocs de la figura 29.

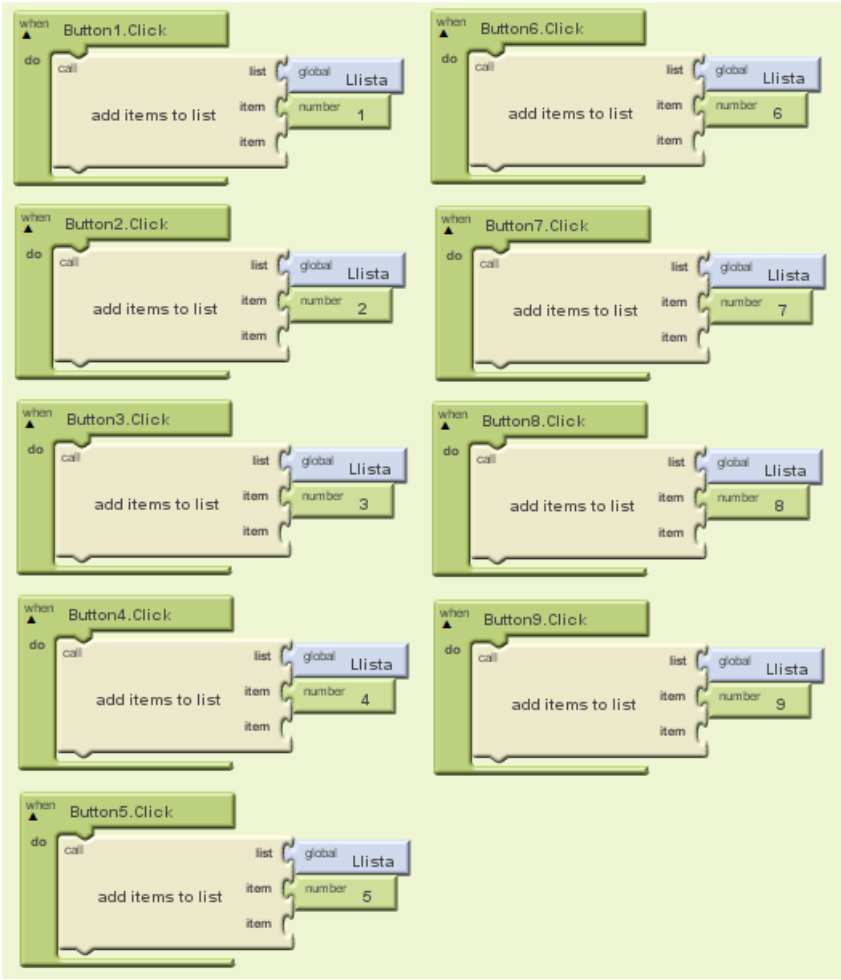

Figura 29

Finalment, després d'introduir la contrasenya, l'usuari ha de prémer la tecla 10. L'esdeveniment generat per l'acció d'aquesta tecla és el que validarà l'autenticació o no (veure Figura 30). El procés de comprovació és el següent:

- Es verifica si el nombre d'elements a la llista és igual a 4. Si a la llista hi ha més o menys elements, llavors la contrasenya no pot ser correcta ja que està formada per 4 colors.
- Seguidament es verifica si el primer element és el número 2 (= color blau clar). En cas contrari, la contrasenya és incorrecta.
- Després es verifica si el segon element és el número 6 (= color vermell). En cas contrari, la contrasenya és incorrecta.
- La tercera verificació és comparar el tercer element amb el número 9 (= color verd). En cas contrari, la contrasenya és incorrecta.
- La darrera verificació és comparar si el quart element és el número 1 (= color groc). En cas contrari, la contrasenya és incorrecta.
- Si les 4 verificacions són positives es mostra a l'etiqueta el missatge 'Contrasenya correcta' en color verd. Qualsevol altre resultat significarà que la contrasenya és incorrecta i l'etiqueta mostrarà el missatge 'Contrasenya incorrecta' en color vermell.
- El següent pas és buidar la llista. Aquesta acció no és estrictament necessària ja que cada pantalla crea la seva pròpia llista. Aquestes són totalment independents encara que s'anomenin de la mateixa manera. Per evitar possibles problemes de sobrecàrrega a la memòria o desbordaments de pila, que segurament no es produiran, he preferit afegir aquest pas.
- La darrera acció és passar a la següent pantalla.

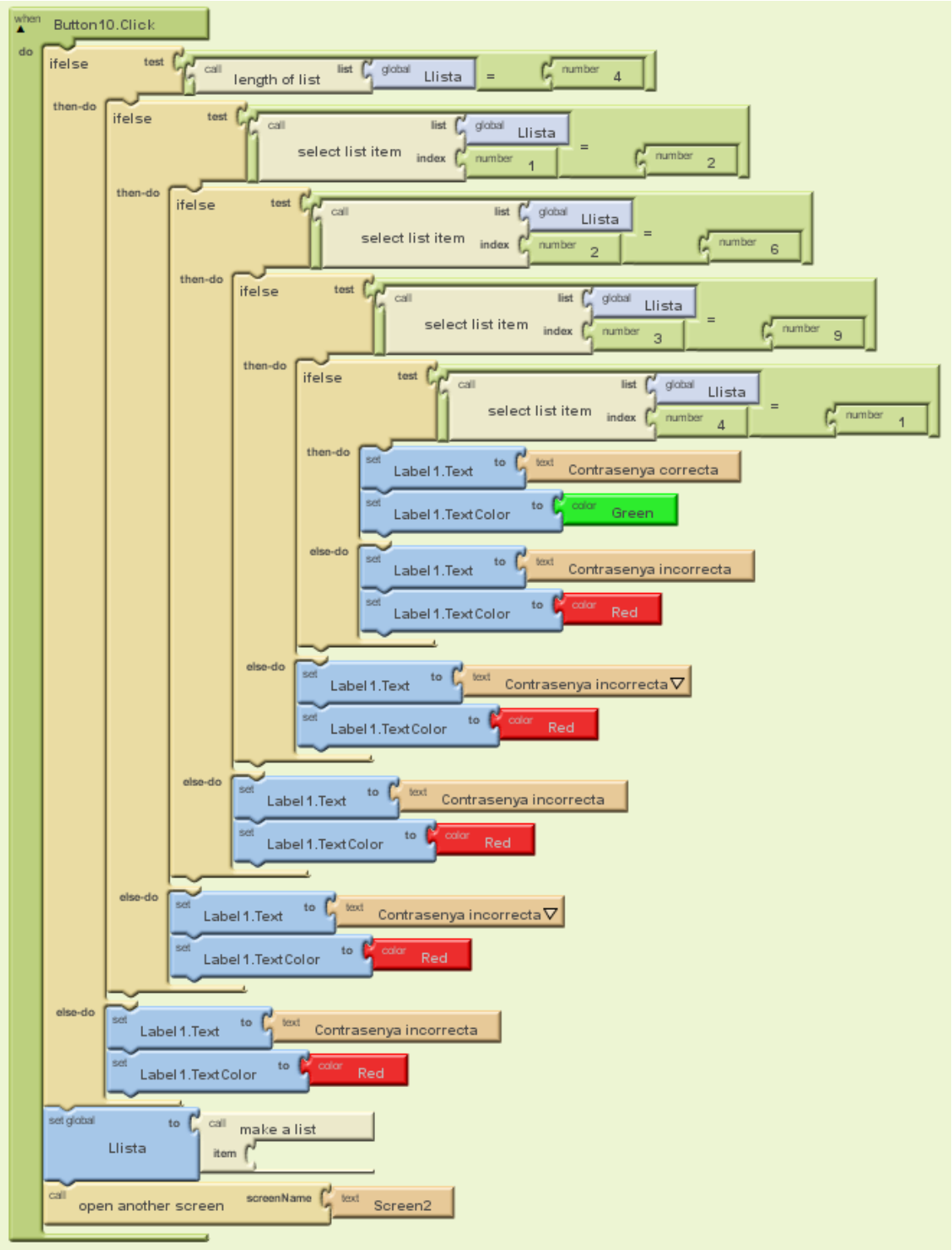

Figura 30

Les 9 primeres pantalles són idèntiques, només canvia el número que hi ha a la darrera acció que és obrir la pantalla

següent. La figura anterior correspon a la pantalla 1, que obre la pantalla 2. Anàlogament, la pantalla 2 obre la 3 segons la instrucció de la Figura 31 i així successivament.

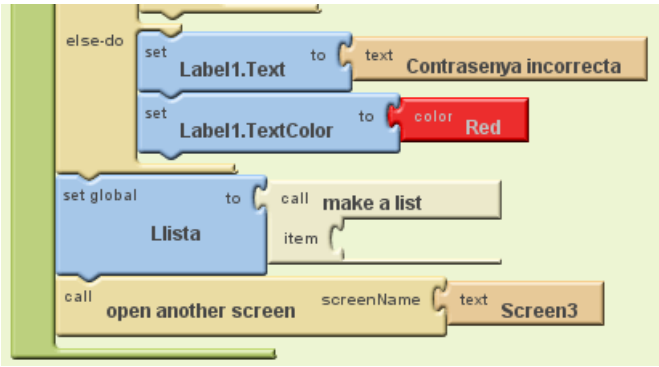

Figura 31

Finalment, la darrera instrucció de la pantalla 10 és tancar l'aplicació. Veure Figura 32.

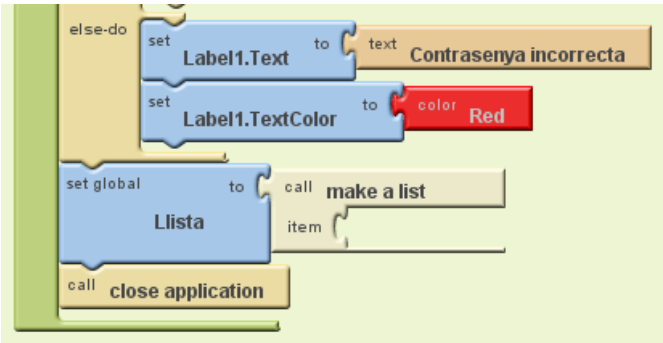

Figura 32

4.3. Joc de proves amb usuaris

Una vegada es disposa de l'aplicació depurada d'errors, es procedeix a crear un joc de proves que permetran avaluar diferents aspectes del nou sistema de contrasenya gràfica.

Amb el joc de proves es pretén obtenir dades objectives que permetin comparar l'aplicació TAP DOTS! amb el sistema PIN i certificar si les

hipòtesis de millora són correctes o no. Els principals aspectes que es volen avaluar són:

- Capacitat per recordar la contrasenya
- Temps d'introducció de la contrasenya
- Preferències en cas d'haver de triar una contrasenya

Per a obtenir dades representatives, s'han realitzat les proves a un grup de 15 persones. Aquestes proves, s'han portat a terme sempre en les mateixes condicions per tal de no desvirtuar l'estudi.

El procediment emprat amb cada usuari ha estat el següent:

- Breu introducció al motiu de la prova: explicació de la tasca realitzada com a TFC de l'enginyeria tècnica informàtica i de la importància de tenir exemples de la reacció amb usuaris reals.
- Explicació del sistema de contrasenya gràfica: es mostra com funciona el sistema i com reacciona al maneig.
- Una vegada l'usuari ha entès la mecànica del sistema, se li demana que triï els colors que faria servir com a contrasenya. Això es fa abans de mostrar-li la que serà la contrasenya amb la que farà les proves per no coaccionar-lo.
- S'explica que l'usuari ha d'introduir la contrasenya predeterminada 'blau clar, vermell, verd, groc' i que l'aplicació només reconeix com a correcta aquesta combinació mostrant per pantalla el missatge 'Contrasenya correcta' en color verd. Qualsevol altre cas mostra el missatge 'Contrasenya incorrecta' en vermell.
- Es deixa a l'usuari practicar amb l'aplicació per familiaritzar-s'hi.
- Es demana fer la seqüència de 10 pantalles amb una ajuda visual.
- Es repeteix la seqüència de 10 pantalles sense ajuda visual. Es cronometra i contabilitzen el nombre d'errades només durant aquesta darrera seqüència.

Sempre que ha sigut possible (10 persones), s'ha gravat en vídeo la darrera part de l'assaig per tenir evidències i facilitar la presa de les dades.

Els paràmetres que s'han enregistrat de cada usuari són:

- Nom
- Edat
- Sexe
- Colors de la contrasenya triada
- Temps total en introduir la contrasenya a les 10 pantalles diferents
- Nombre d'errades

Amb aquestes dades n'hi ha hagut prou per extreure conclusions.

4.4. Resultats de les proves

Les proves s'han realitzat entre els dies 19 i 25 de maig de 2013 a 15 persones (familiars, amics i companys de feina). Els resultats de totes elles són a la taula de la figura 33. Per tal de protegir la identitat dels enquestats segons la Llei 15/99, de 13 de desembre, de protecció de dades, només s'han indicat les inicials dels noms.

	Nom	Edat (anys)	Sexe	Contrasenya triada				Temps (m:s)	Errades
1	M P	39	Home	Blau fosc	Negre	Vermell	Groc	00:59	0
2	MJ M	38	Dona	Vermell	Blau fosc	Negre	Groc	00:45	0
3	A F	47	Home	Vermell	Groc	Verd	Blau fosc	00:42	0
4	J M	46	Home	Blau fosc	Groc	Vermell	Verd	01:21	2
5	D M	39	Dona	Blau fosc	Groc	Vermell	Taronja	00:44	0
6	M F	32	Dona	Taronja	Lila	Taronja	Vermell	00:39	3
7	P G	48	Dona	Verd	Rosa	Lila	Blau clar	00:48	1
8	B H	47	Home	Blau fosc	Groc	Vermell	Negre	00:43	0
9	J P	35	Home	Verd	Vermell	Blau fosc	Taronja	00:42	0
10	X F	36	Home	Vermell	Verd	Groc	Blau clar	00:38	0
11	A A	30	Home	Groc	Blau fosc	Negre	Vermell	00:44	0
12	J P	46	Home	Blau fosc	Vermell	Verd	Taronja	00:45	2
13	A M	36	Home	Groc	Negre	Vermell	Verd	01:11	2
14	E E	49	Home	Verd	Vermell	Vermell	Blau fosc	00:34	0
15	C A	47	Dona	Lila	Rosa	Blau clar	Groc	00:38	1

Figura 33

D'aquests resultats s'extreuen les següents dades:

- Han participat 10 homes i 5 dones

- La mitjana d'edat és de 41 anys
- El temps mig en completar les 10 pantalles és de 48 segons
- La mitja d'errades és de 0.73
- Cada color ha sigut triat la quantitat de vegades que es pot veure a la Figura 34

Color	Repeticions
Vermell	14
Groc	10
Blau fosc	10
Verd	8
Negre	5
Taronja	5
Blau clar	3
Lila	3
Rosa	2

Figura 34

5. Conclusions

Per finalitzar l'exercici amb el nou sistema de contrasenya gràfica, extraurem conclusions de les dades que ens ha subministrat l'experiment realitzat. Aquestes i les especificacions pròpies de l'aplicació TAP DOTS! ens ajudaran a determinar la millora respecte el sistema PIN.

5.1. Èxits

El primer èxit és el grau d'adaptació dels usuaris a l'aplicació. Les explicacions sobre el funcionament van ser mínimes. En comparar-lo amb el sistema PIN que tothom utilitza als caixers automàtics, el concepte es va entendre a la primera. A partir d'aquí, els usuaris dedicaven només uns segons per practicar amb el telèfon mòbil. Immediatament, es passava a realitzar la prova. L'adaptació està justificada pel nombre d'errades:

- El 60% (9 de 15) comet 0 errades
- El 13.3% (2 de 15) comet 1 errada
- El 20% (3 de 15) comet 2 errades
- El 6.6% (1 de 15) comet 3 errades

La facilitat per recordar la contrasenya queda en part justificada amb les dades anteriors. Tres quartes parts dels enquestats finalitza la prova sense errades o només una. El test de memòria a llarg termini no s'ha pogut realitzar per falta de temps. Com a curiositat, s'ha preguntat la contrasenya als 6 companys de feina una setmana després de fer la prova i 5 l'han recordat, 3 persones sense ajuda i 2 persones donant el primer color com a pista.

El temps en introduir la contrasenya també és un èxit. La mitja en fer les 10 pantalles és de 48 segons, o sigui, 4.8 segons fer una autenticació. Si eliminen els dos millors i els dos pitjors temps, tenim una mitja de 44 segons, 4.4 per pantalla. El temps en introduir 4 números en un sistema

PIN està al voltant de 2 segons[8]. Tenint en compte que l'aplicació TAP DOTS! és totalment nova per als usuaris i que només l'han utilitzat 20 vegades, el temps s'acosta molt al que fa anys que utilitzen a diari als caixers automàtics i d'altres aparells. Durant les proves que he fet jo mateix per testejar l'aplicació, he assolit mitjanes de 23 segons sense errades, 2.3 segons per pantalla.

Es pot afirmar també que l'edat no sembla ser un factor que influeixi negativament. No s'observa una relació directa entre edat i augment de temps o errades. Cal destacar que la persona de major edat ha completat l'exercici en el menor temps i sense errades.

5.2. Problemàtiques

Tot i que l'objectiu del nou sistema de contrasenya gràfica és millorar el precedent, hem d'identificar els possibles punts febles. Hi ha aspectes que depenen de la subjectivitat dels usuaris, com ara la preferència personal per canviar el sistema PIN pel nou. En converses posteriors a les proves, els usuaris es mostren dividits respecte el nou sistema: uns afirmen que estarien oberts a adoptar-lo, almenys temporalment, i d'altres serien reticents a fer el canvi.

Per contra, sí podem afirmar que és un punt feble allò que ens evidencien les dades dels tests. Aquestes ens revelen que els usuaris mostren preferència per uns determinats colors per formar la seva contrasenya personal. Això crea una debilitat en el sistema de contrasenya ja que permet realitzar atacs de diccionari. Com es pot observar a la Figura 34, hi ha 4 colors que han sigut triats moltes més vegades que la resta.

Destaca especialment el color vermell, que ha sigut triat un 23.3% de les vegades. De fet, és present en totes les contrasenyes menys en dues.

[8]Temps obtingut en proves fetes per mi en les mateixes condicions que amb l'aplicació: temps total de 10 autenticacions seguides dividit entre 10.

Els quatre colors són:

- Vermell: 23.3% (14 de 60)
- Groc: 16.6% (10 de 60)
- Blau fosc: 16.6% (10 de 60)
- Verd: 13.3% (8 de 60)

La conseqüència immediata és que hi ha d'altres colors que no són atractius per a gairebé ningú. El menys triat és el rosa amb només un 3.3% (2 de 60).

Per contra, s'observa que en només dues contrasenyes es repeteix un color. Això aporta diversitat en la seva formació i ajuda a minimitzar els atacs per diccionari. Aquestes són:

- Taronja, lila, taronja i vermell
- verd, vermell, vermell i blau fosc

Com era de preveure, el color vermell és un dels dos que es repeteix.

Finalment, hi ha una altra problemàtica relacionada que no es pot detectar amb el prototip de l'aplicació. Si el conjunt de colors és 12 com està definit al disseny, llavors, fent '*shoulder surfing*', es pot arribar a deduir la contrasenya, en el pitjor dels casos, amb només 3 vegades que s'observi la pantalla d'autenticació simplement anotant els colors que no es repeteixen. Aquest problema es pot solucionar posant tots els colors a la graella, fent-la de 4 x 3, o bé reduint el conjunt de colors a només 9 mantenint la graella de 3 x 3, tal com està feta l'aplicació.

Respecte a la metodologia utilitzada en fer les proves amb usuaris, també es detecten inconvenients. A causa de la impossibilitat d'enregistrar en vídeo tots els usuaris, com ja s'ha comentat, cinc proves es van realitzar cronòmetre en mà per registrar els temps utilitzats en fer-les. Els usuaris que eren enregistrats en vídeo no sabien per endavant que el temps era una variable a estudiar, però alguns dels que veien que la prova es cronometrava la feien en mode 'competició contrarellotge'. Aquesta situació

pot generar major nombre d'errades i, per tant, totes les proves s'haurien d'haver fet exactament en les mateixes condicions.

Que l'aplicació no permetés que els usuaris poguessin triar la seva contrasenya també ha sigut un altre inconvenient. S'ha de tenir en compte que abans d'iniciar la part d'interacció amb l'aplicació, a l'usuari se li preguntava quina seria la seva contrasenya personal amb aquest sistema. Per tant, ja estava predisposat a uns colors diferents als que després hauria d'utilitzar.

5.3. Millores de futur

El sistema de contrasenyes creat és funcional, com podem comprovar amb l'aplicació Android generada a tal efecte. El disseny és eminentment pràctic i està pensat per a superar els requisits bàsics exigits sense tenir en compte necessitats especials dels usuaris que pateixen daltonisme o ceguera. Així doncs, els aspectes a millorar poden ser adaptar l'aplicació a aquests col·lectius:

- Els daltonians tenen problemes per distingir els colors, especialment certs matisos de vermells i verds. L'aplicació, tal com està dissenyada, no és apta per aquest col·lectiu ja que el seu funcionament està basat únicament en colors. Per solucionar aquest problema, es poden substituir els cercles de colors per gràfics simples en blanc i negre. Per exemple: un cercle, una creu, un signe menys, una estrella, un quadrat, etc. Veure Figura 35.

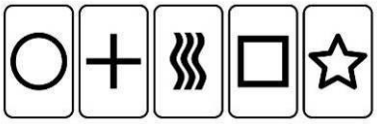

Figura 35

- Els sistemes de contrasenya gràfica són inservibles per als cecs. La solució consisteix en generar gràfics tàctils a la pantalla del dispositiu que puguin reconèixer com fan per llegir amb el sistema

Braille. Actualment hi ha una empresa, Tactus Technology[9], que ha aconseguit generar protuberàncies sobre la superfície plana d'una pantalla tàctil simulant tecles. En un futur, aquesta tecnologia pot evolucionar i millorar per permetre relleus més definits que els cecs puguin reconèixer com caràcters o símbols.

- Una aplicació destinada al públic ha de tenir opcions de configuració. Per exemple: afegir so a les tecles, oferir personalitzacions com ara longitud de contrasenya, fons de pantalla, missatges, etc.

Com a conclusió, podem dir que les contrasenyes gràfiques en general tenen un gran marge de millora i que hi ha encara moltes possibilitats de desenvolupament dels punts més febles.

[9] http://www.tactustechnology.com/

Glossari

Android: sistema operatiu basat en Linux per a dispositius mòbils amb pantalla tàctil

ASCII: American Standard Code for Information Interchange, codi estàndard americà per a l'intercanvi d'informació

BDAS: Background Draw A Secret, dibuixa un secret amb imatge de fons

Cued Click Points (CCP): clickar punts amb pista

DAS: Draw A Secret, dibuixa un secret

Déjà Vu: expressió francesa que vol dir 'ja vist'. Descriu l'experiència de sentir que s'ha estat testimoni o s'ha experimentat prèviament una situació nova

Doodle: gargot

Faces: cares

Froyo (frozen yoghurt, gelat de iogurt), Ice cream sandwich (gelat de sandvitx de nata) i Jelly bean (llaminadura): sistema per anomenar les diferents versions del SO Android. Corresponen a postres en anglès i a cada versió nova del SO se li assigna un nom que comença per una lletra diferent que avança seguint un ordre alfabètic

Go: joc d'estratègia de tauler

Google: empresa propietaria del SO Android

Hotspot: punt calent, lloc de moda

IDE: Integrated Development Environment, entorn de desenvolupament integrat

Inkblot: taca de tinta

Java: principal llenguatge de programació utilitzat en aplicacions per a Android

MIT: Massachussets Institute of Technology

Persuasive Cued Click-Points (PCCP): clickar punts amb pista de manera persuasiva

PIN: Personal Identification Number

R-DAS: Rotational Draw A Secret, dibuixa un secret giratori

SDK: Software Development Kit , kit de desenvolupament de programari

Shoulder surfing: observar per sobre de la espatlla

SO: sistema operatiu

SSL/TLS: Secure Sockets Layer (capa de connexió segura) / Transport Layer Security (seguretat de la capa de transport)

TAP DOTS!: colpejar punts

Bibliografia

[1] SplashData, Inc. [Data de consulta: 21/3/2013]. www.splashdata.com/press/PR111121.htm

[2] [Data de consulta: 21/3/2013]. www.password.es, www.clavesegura.org, www.generadordecontraseñas.com

[3] Baron, Robert A (2005).'Fundamentos de psicología'. Pearson educación.

[4] [Data de consulta: 21/3/2013]. http://en.wikipedia.org/wiki/Picture_superiority_effect

[5] Paivio, Allan (1971). *'Imagery and verbal processes'.* New York: Holt, Rinehart & Winston.

[6] Blonder, Greg. '*Graphical passwords*'. United States Patent 5559961 (25/9/1996)

[7] Jermyn, Ian; Mayer, Alain; Monrose, Fabian; Reiter, Michael K.; Rubin, Aviel D (1999). '*The Design and Analysis of Graphical Passwords'*. Berkeley: USENIX Association Berkeley.

[8] Klein, Daniel V (1990). '*Foiling the cracker: A survey of, and improvements to, password security'*. Portland: USENIX.

[9] Varenhorst, Christopher (2004).'*Passdoodles; a Lightweight Authentication Method'*. Massachussets: Massachusetts Institute of Technology.

[10] TAO, HAI (2006). '*Pass-Go, a New Graphical Password Scheme'*. International Journal of Network Security (Volumen 7, No 2, Pàgines 273–292).

[11] Bond, Mike (2008). '*Comments on Gridsure Authentication*'. Cambridge: University of Cambridge.

[12] Brostoff, Sacha; Sasse, M. Angela (1998). '*Are Passfaces More Usable Than Passwords? A Field Trial Investigation*' (Pàgines 405-424). People and Computers XIV — Usability or Else! London: Springer London.

[13] Olanrewaju O., Ayannuga; Olusegun, Folorunso; Adio T, Akinwale (2011). '*Evaluation of a Usable Hybrid Authentication System*'. International Journal of Computer Applications (Volumen 17, No. 8, Pàgines 27-31).

[14] Blonder, Greg (1995). '*Graphical password'*. U.S. patent 5,559,961. Nova York.

[15] Emir Dirik, Ahmet; Memon, Nasir; Birget, Jean-Camille (2007). '*Modeling user choice in the PassPoints graphical password scheme*'. Pittsburg: Symposium On Usable Privacy and Security (SOUPS).

[16] Wiedenbecka, Susan; Watersa, Jim; Birgetb, Jean-Camille; Brodskiyc, Alex; Memonc, Nasir (2005). '*PassPoints: Design and longitudinal evaluation of a graphical password system*'. International Journal of Human-Computer Studies (No. 63, pàg. 102–127). Filadèlfia: Elsevier Inc.
[17] Chiasson, Sonia; van Oorschot, Paul C.; Biddle, Robert (2007). '*Graphical Password Authentication Using Cued Click Points*'. Dresden: 12 th European Symposium On Research In Computer Security (ESORICS).
[18] Chiasson, Sonia; Forget, Alain; Biddle, Robert; van Oorschot, Paul C (2008).'*Influencing Users Towards Better Passwords: Persuasive Cued Click-Points*'. Swinton: British Computer Society Swinton.
[19] Stubblefield, Adam; Simon, Daniel R (2004). '*Inkblot Authentication*'. Redmond: Microsoft Research.
[20] Wiedenbeck, Susan; Waters, Jim; Sobrado, Leonardo; Birget, Jean-Camille (2006). '*Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme'*. Nova York: ACM New York.
[21] Man, Shushuang; Hong, Dawei; Matthews, Manton (2003). '*A Shoulder-Surfing Resistant Graphical Password Scheme – WIW*'. Las Vegas: Proceedings of the International Conference on Security and Management, SAM '03.
[22] Aviv, Adam J.; Gibson, Katherine; Mossop, Evan; Blaze, Matt; Smith, Jonathan M (2010). '*Smudge Attacks on Smartphone Touch Screens'*. Berkeley: USENIX Association Berkeley.
[23] Massachusetts Institute of Technology. [Data de consulta: 24/3/2013]. http://appinventor.mit.edu/
[24] Massachusetts Institute of Technology. [Data de consulta: 24/3/2013]. http://beta.appinventor.mit.edu/learn/reference/index.html
[25] Villalpando, Juan Antonio. [Data de consulta: 24/3/2013]. http://www.iesromerovargas.net/android/
[26] Hong, Dawei; Ma, Shushuang; Hawes, Barbra; Matthews, Manton (2004). '*A password scheme strongly resistant to spyware'*. Las Vegas: Proceedings of the International Conference on Security and Management, SAM '04.
[27] Biddle, Robert; Chiasson, Sonia; van Oorschot, Paul C (2012). '*Graphical Passwords: Learning from the First Twelve Years*'. Ottawa: ACM Computing Surveys.
[28] Wiedenbeck, Susan; Waters, Jim; Birget, Jean-Camille; Brodskiy, Alex (2005). '*Authentication Using Graphical Passwords:Effects of Tolerance and*

Image Choice'. Pittsburg: Symposium on Usable Privacy and Security, SOUPS'05.