D@NGEROUS WEB: PROTEGEIX-TE

Pseudònim: Cinc segons

Saber trencar mesures de seguretat no et converteix en hacker, així com saber fer un pont a un cotxe no et converteix en un enginyer d'automoció.

ERIC RAYMOND

AGRAÏMENTS

Al meu tutor del treball, per la seva paciència, suport i orientacions; a la meva tutora de 2n de Batxillerat, als professors que m'han encaminat i als meus pares, pel seu suport durant l'elaboració del treball.

ÍNDEX

ÍNDEX DE FONTS DE LES IMATGES

Fig 1.: https://tinyurl.com/ycnxuntz (3 de juliol)

Fig 2.: https://tinyurl.com/yb5w8tjv (3 de juliol)

Fig 3.: https://tinyurl.com/ybqn67yt (6 de juliol)

Fig 4.: https://tinyurl.com/yambkrol (6 de juliol)

Fig 5.: https://tinyurl.com/y8rzdzmt (12 de juliol)

Fig 6.: https://tinyurl.com/ycp7sufz (12 de juliol)

Fig 7.: https://tinyurl.com/y892akmw (21 de juliol)

Fig 8.: https://tinyurl.com/h7c5ox4 (21 de juliol)

Fig 9.: https://tinyurl.com/y9mtt2dv (12 d'agost)

Fig 10.: https://tinyurl.com/y7e37k9b (12 d'agost)

Fig 11.: https://tinyurl.com/y6vtbbmp (12 d'agost)

Fig 12.: https://tinyurl.com/y8pqconh (12 d'agost)

Fig 13.: https://tinyurl.com/y7h747dg (12 d'agost)

Fig 14.: https://tinyurl.com/y7v4tss8 (28 d'agost)

Fig 15.: https://tinyurl.com/yb6u3gy4 (28 d'agost)

Fig 16.: https://tinyurl.com/ycgzo4hc (28 d'agost)

Fig 17.: https://tinyurl.com/yc7t8dgz (1 de setembre)

Fig 18.: https://tinyurl.com/yb52wc72 (1 de setembre)

Fig 19.: https://tinyurl.com/y9w58gxy (1 de setembre)

Fig 20.: https://tinyurl.com/ydxtqdmw (7 de setembre)

Fig 21.: https://tinyurl.com/yar7t6uq (7 de setembre)

Fig 22.: https://tinyurl.com/yczkqs8n (22 de setembre)

Fig 23.: https://tinyurl.com/y9qhj28m (22 de setembre)

Fig 24.: https://tinyurl.com/y8kzhdo3 (24 de setembre)

Fig 25.: https://tinyurl.com/y8s23ayj (24 de setembre)

Fig 26.: https://tinyurl.com/yc2yv55f (25 de setembre)

Fig 27.: https://tinyurl.com/ycpqbxja (2 d'octubre)

Fig 28.: https://tinyurl.com/ycc9n77y (3 d'octubre)

Fig 29.: https://tinyurl.com/y94vcylp (7 d'octubre)

Fig 30.: https://tinyurl.com/yajhmgxj (7 d'octubre)

Fig 31.: https://tinyurl.com/yb8nqxdm (11 d'octubre)

Fig 32.: https://tinyurl.com/y92u5gqf (12 d'octubre)

Fig 33.: https://tinyurl.com/yanepgfx (12 d'octubre)

Fig 34.: https://tinyurl.com/y7v4f9do (12 d'octubre)

Fig 35.: https://tinyurl.com/ydzxbmcr (17 d'octubre)

Fig 36.: https://tinyurl.com/y9us5yka (17 d'octubre)

Fig 37.: https://tinyurl.com/y8ukp3po (19 d'octubre)

Fig 38.: https://tinyurl.com/y8w7qqzz (20 d'octubre)

Fig 39.: https://tinyurl.com/y9zablu4 (23 d'octubre)

Fig 40.: https://tinyurl.com/ybouggu8 (23 d'octubre)

Fig 41.: https://tinyurl.com/ybd4f3ru (2 de novembre)

Fig 42.: https://tinyurl.com/ydgwhk7u (4 de novembre)

Fig 43.: http://appinventor.mit.edu/explore/ (5 de novembre)

Fig 44.: Font pròpia (10 de novembre)

Fig 45.: Font pròpia (10 de novembre)

Fig 46.: Font pròpia (10 de novembre)

Fig 47.: Font pròpia (12 de novembre)

Fig 48.: Font pròpia (12 de novembre)

Fig 49.: Font pròpia (21 de novembre)

Fig 50.: Font pròpia (21 de novembre)

Fig 51.: Font pròpia (21 de novembre)

Fig 52.: Font pròpia (21 de novembre)

Fig 137.: https://tinyurl.com/ycxpntlp (1 de gener)

Fig 138.: https://tinyurl.com/ydhm2lm6 (1 de gener)

Fig 139.: https://tinyurl.com/yd9a726o (1 de gener)

Fig 140.: https://tinyurl.com/y7vx8mob (2 de gener)

Fig 141.: https://tinyurl.com/ya9cq8as (2 de gener)

Fig 142.: https://tinyurl.com/ybg4yfuq (2 de gener)

Fig 143.: https://tinyurl.com/y8dh6s2t (2 de gener)

Fig 144.: https://tinyurl.com/y8hn4lak (2 de gener)

Fig 145.: https://tinyurl.com/yc3cg5wn (3 de gener)

Fig 146.: https://tinyurl.com/yay5bz8z (3 de gener)

Fig 147.: https://tinyurl.com/y7azkoh7 (3 de gener)

Fig 148.: https://tinyurl.com/y88vtzho (3 de gener)

Fig 149.: https://tinyurl.com/ycoxaccy (3 de gener)

Fig 150.: https://tinyurl.com/y99dhcvc (3 de gener)

Fig 151.: https://tinyurl.com/yccw6efc (3 de gener)

Fig 152.: https://tinyurl.com/y9knlj65 (3 de gener)

Fig 153.: https://tinyurl.com/ydg8cmjd (3 de gener)

Fig 154.: https://tinyurl.com/ydypy9mx (3 de gener)

Resum

Aquest treball pretén fer un estudi del món de la seguretat informàtica i del hacking.

A la part teòrica se centra principalment en els malwares: tipus, procedència, finalitat i manera d'evitar-los. També fa un incís sobre els grups més famosos en aquest àmbit, coneguts com a hackers, i una introducció a la criptografia.

Respecte la part pràctica, podreu veure el procés de creació d'una aplicació per a Android que permet emmagatzemar contrasenyes. Aquesta aplicació està pensada especialment per al professorat de l'institut de Flix, però el seu ús es pot fer extensiu a tots els professors en general.

Com a curiositat, als annexos hi trobareu entrevistes a experts en seguretat informàtica fetes i publicades per diferents mitjans digitals.

Abstract

This project aims to study the Computer security and Hacking world.

In the theoretical section, I mainly focused on Malware: types, origin, purpose and how to avoid them. I made an incision as well about the most famous groups in this scope, known as hackers, and an introduction to the cryptography.

Regarding to the practical section, you will see how I managed to develop an Android's application that allows us to keep our passwords safe. This application was made especially for the INS Flix's teachers, but its use can be extended to any teacher.

As a curiosity, you can find some interviews to Computer security experts, done and published by many digital media, in the annex.

1. INTRODUCCIÓ

La informàtica sempre ha estat un tema que m'ha resultat interessant, des de ben petit que m'ha apassionat.

Fins que no vaig fer la meva primera comunió, no vaig disposar d'un ordinador, el qual anhelava des de feia temps. Encara que no tingués ni deu anys, sempre que tenia possibilitat d'utilitzar-ne algun, ho feia, ja que la sensació d'estar davant d'un teclat, una pantalla i un ratolí m'agradava.

A part de la passió que tenia pel món de la computació, també tenia una destresa natural per a aquesta. Encara que desconec si era motivada pel meu interès o per simple casualitat, utilitzar un ordinador em reconfortava. Tot va començar a l'escola en la qual vaig cursar l'Educació Primària, a Llardecans, on alguns cops els professors ens deixaven utilitzar els ordinadors que hi havia a la biblioteca. Allí va ser on vaig descobrir realment l'interès que tenia per ells i vaig decidir estalviar per poder comprar-me'n un.

Fins que no vaig començar a l'institut bàsicament l'utilitzava per jugar. En aquesta etapa de la meva vida, a poc a poc, vaig anar descobrint les dimensions del món cibernètic. L'evolució en aquest camp era lenta i els descobriments que me l'anaven facilitant eren petits, un exemple podria ser les ganes de saber quina era la finalitat dels famosos virus dels quals tothom parlava amb temor. Durant l'ESO, cada cop les noves tecnologies em semblaven més i més fascinant, ja que les possibilitats englobades en l'àmbit general informàtic eren immenses. Va ser al començament de l'últim curs d'aquest període educatiu quan vaig decidir que enfocaria els meus estudis universitaris cap a aquest àmbit.

Un cop a primer de batxillerat, va arribar el moment de decidir el tema del treball de recerca. Abans d'elegir-lo, vaig dubtar molt perquè tot i que em feia gràcia aprofundir en la seguretat informàtica, tenia clar que era difícil i, a més, el meu tutor també m'ho havia advertit. Finalment, vaig decidir tirar-lo endavant, superar les dificultats seria un repte per a mi.

Al llarg d'aquest treball parlaré sobre els aspectes que desconeixem del hacking i de la seguretat informàtica en el tema de malware, per així poder mantenir-la als nostres dispositius.

La part teòrica m'ha resultat de gran ajuda per conèixer millor en què consisteix aquest món tan complex i per desmentir estereotips i conceptes que acostumem a confondre. Respecte a la part pràctica, m'ha costat molt concretar-la, ja que fer un treball sobre seguretat informàtica requereix un coneixement previ que s'adquireix al llarg d'anys d'estudi especialitzat en aquest àmbit. Malgrat tot, l'he pogut adaptar i fer una aplicació per a Android de manera que sigui útil per a determinats usuaris.

Encara que per fer la part pràctica també he hagut d'aprendre com utilitzar el software de manera autodidacta, he pogut assolir els coneixements necessaris per desenvolupar-la amb ajuda i consells del tutor.

Al principi, vaig decidir que aquesta part seria sobre prevenció de malware, però després de perdre unes dades sobre un compte de correu electrònic que tenia emmagatzemades en una aplicació de notes al meu telèfon mòbil, vaig canviar-ne el rumb orientant-la cap una aplicació de seguretat i utilitzar uns criptogrames, encara que no estiguessin al nivell que m'agradaria de la criptografia moderna.

Els objectius que em plantejo assolir amb la realització d'aquest treball són:

1. Aprofundir en els tipus de malware i el seu origen.
2. Desmentir els mites sobre hackers.
3. Crear una aplicació útil per al professorat.

2. SEGURETAT INFORMÀTICA I HACKING

Encara que quan sentim a parlar del concepte de hacking o d'una persona que és denominada hacker pensem que és algú que atempta contra la seguretat d'algun sistema informàtic, no sempre és així, ja que molts cops té la finalitat de descobrir les vulnerabilitats existents i així poder millorar-ne la seguretat. Aquesta branca s'anomena ethical hacking o hacking ètic.

Fig 1. Xarxa de seguretat informàtica

D'altra banda, la seguretat informàtica, encara que tingui una relació propera amb el hacking ètic, és un concepte diferent.

La seguretat informàtica, també coneguda com ciberseguretat, és l'àrea relacionada amb la informàtica i la telemàtica que se centra en la protecció de la infraestructura computacional, que és fonamental per a l'emmagatzematge i la gestió de la informació i el seu funcionament, com també els seus usuaris.

Fig 2. Protecció d'un equip

Per això, existeixen uns estàndards, protocols, mètodes, regles, eines i lleis que pretenen minimitzar els riscos a aquesta infraestructura o a la informació que hi ha en un ordinador o que circula a través de les xarxes d'ordinadors.

No només s'han de tenir en compte les amenaces que sorgeixen de la programació i el funcionament, també hi ha altres amenaces que poden venir d'aspectes molt diferents i que són tant o més perilloses que les anteriors.

Poden ser causades per:

- **Usuaris:** En alguns casos les seves accions poden causar problemes de seguretat, ja que pot ser que no se'ls hagi restringit accions innecessàries o perquè tinguin molts permisos.

- **Programes maliciosos (malware):** Són programes que estan destinats a perjudicar o fer un mal ús dels recursos del sistema. Aquests són instal·lats a l'ordinador, modificant les dades o obrint portes a intrusos.
- **Errors de programació**
- **Intrusos:** Persones que poden accedir a informació o programes als quals no estan autoritzats.

Personal intern: Ja sigui per problemes laborals, interessos econòmics, espionatge.

Fig 3. Intrús informàtic

2.1 HISTÒRIA DEL HACKING

2.1.1 INTRODUCCIÓ

L'anomenat "hacking" no va néixer amb l'objectiu de ser una amenaça i ser negatiu, es va crear com un estat de diversió i satisfacció personal en relació amb el món de la informàtica. Encara que la idea que té gairebé tothom sobre aquest concepte o món és acusador o negatiu, el problema no està en el fet de fer hacking, sinó en com s'utilitza i quin ús se'n fa.

Fig 4. Hacker

La paraula "hacker" s'ha anat revestint al llarg dels anys i és pràcticament intraduïble, ja que està vinculada amb els "hacks", que eren els cops secs que aplicaven els tècnics de telefonia quan intentaven arreglar un dels seus aparells o, un exemple més familiar, quan se li donava un cop a una televisió antiga que no funcionava perquè tornés al seu estat de funcionament.

Aquest fenomen es remunta a molt temps enrere, des que s'utilitzaven coloms missatgers. En aquella època, hi havien persones que desxifraven missatges dels enemics, però no van ser anomenats hackers fins l'arribada de l'ordinador.

Encara que anteriorment no estava penalitzat, a mesura que la tecnologia ha anat avançant, els hackers han hagut de limitar les seves actuacions, ja que actes com descodificar un canal de pagament, són considerats delictes informàtics i, per consegüent, estan penats.

Això sí, davant aquesta situació és obvi que sempre hi haurà curiositat per estudiar aquests codis i tecnologies.

2.1.2 PRÒLEG: ELS AUTÈNTICS PROGRAMADORS

En un principi, els encarregats del món del hacking eren els anomenats Autèntics Programadors, encara que fins l'any 1980, no rebrien aquest sobrenom.

Des de meitats del segle XX, concretament l'any 1945, tota la tecnologia relacionada amb la computació havia atret moltes de les persones més brillants i creatives del món.

```
-u 100 1a
0CFD:0100 BA0B01      MOV     DX,010B
0CFD:0103 B409        MOV     AH,09
0CFD:0105 CD21        INT     21
0CFD:0107 B400        MOV     AH,00
0CFD:0109 CD21        INT     21
-d 10b 13f
0CFD:0100                                       48 6F 6C 61 2C
0CFD:0110  20 65 73 74 65 20 65 73-20 75 6E 20 70 72 6F 67
0CFD:0120  72 61 6D 61 20 68 65 63-68 6F 20 65 6E 20 61 73
0CFD:0130  73 65 6D 62 6C 65 72 20-70 61 72 61 20 6C 61 20
0CFD:0140  57 69 6B 69 70 65 64 69-61 24
```

Fig 5. Llenguatge assemblador

El primer ordinador, anomenat ENIAC (Electronic Numerical Integrator And Computer) va ser creat per Eckert i Mauchly i va impulsar l'existència d'una comunitat composta per programadors que creaven i modificaven software per diversió.

Els Autèntics Programadors normalment eren enginyers o físics i hi havia un estereotip establert sobre la seva aparença. Eren coneguts per dur mitjons blancs, camises amb corbata i ulleres gruixudes, i programaven en llenguatges arcaics que ja estan força oblidats, com el codi màquina, el llenguatge assemblador i el FORTRAN.

2.1.3 ELS PRIMERS HACKERS

El principi de la cultura hacker es pot datar el 1961, l'any en que el MIT (Institut Tecnològic de Massachusetts) va adquirir el primer ordinador PDP-1.

Fig 6. PDP-1

Llavors, el comitè de Senyals i Energia del TMRC (Tech Model Railroad Club) va mostrar una preferència en l'interès del PDP-1 dins el panorama tecnològic i va inventar eines de

programació, un argot i una cultura entorn la computació.

Els hackers del TMRC es van convertir en el nucli del laboratori d'Intel·ligència Artificial del MIT, el centre més destacat d'investigació en aquest camp a nivell mundial al principi dels anys 80.

Aquest centre va tenir una gran influència i es va estendre per tot arreu a partir de l'any 1969, quan es creà ARPANET, la primera xarxa intercontinental d'alta velocitat, construïda pel Departament de Defensa dels EEUU com a experiment, però que va créixer fins a interconnectar centenars d'universitats i centres d'investigació. Per tant, això va permetre a investigadors intercanviar informació amb una gran rapidesa i flexibilitat, impulsant la col·laboració i augmentant exponencialment el creixement de la tecnologia.

Fig 7. Mapa de la xarxa d'ARPANET

El desenvolupament de la cultura hacker va sorgir arran dels departaments d'informàtica de les universitats, en els quals es duia a terme una exhaustiva investigació sobre la Intel·ligència Artificial i va atreure gent brillant que van fer magnífiques aportacions a aquesta cultura.

Fig 8. PDP-10

Els sistemes de temps compartit van ser el medi en el qual va créixer la cultura hacker i, durant la major part de la seva existència, ARPANET va ser una xarxa d'ordinadors, i la PDP-10, apareguda el 1967, en va ser la més important. També va ser considerada la preferida pels hackers durant 15 anys i utilitzava el sistema operatiu TOPS-10 i el llenguatge assemblador MACRO-10.

2.1.4 L'APARICIÓ DE L'UNIX

El 1969, l'any en que va néixer ARPANET, Ken Thompson, un hacker de Laboratoris Bell, va inventar Unix.

Ken Thompson havia participat en el desenvolupament d'un sistema operatiu de temps compartit anomenat "Multics", el qual va ser un bon camp de proves sobre com amagar les dificultats d'un sistema operatiu, i la idea que es tenia era fer l'ús de Multics més fàcil.

Fig 9. DEC PDP-7

En el moment en que Multics va tornar-se inútil, els Laboratoris Bell van decidir abandonar el projecte i Ken Thompson va començar a fer proves,

implementant una barreja de les característiques de Multics i idees pròpies en una antiga DEC PDP-7.

Un temps després, un altre hacker anomenat Dennis Ritchie, va inventar un nou llenguatge que va denominar com a "C" per utilitzar-lo en el projecte Unix de Thompson, amb la intenció que fos un llenguatge flexible i sense límits.

Fig 10. Llenguatge C

L'interès per aquestes eines es va anar estenent pels Laboratoris Bell i va tenir un gran impuls el 1971 i els dos hackers van rebre una oferta per crear un sistema d'automatització d'oficines per un ús intern dels laboratoris.

Abans els sistemes operatius s'escrivien completament en llenguatge assemblador per obtenir la màxima eficiència, però Thompson i Ritchie van ser dels primers en adonar-se que la tecnologia del hardware i els compiladors havia avançat suficientment com per poder crear un sistema operatiu utilitzant únicament llenguatge C, el qual tindria un gran èxit a partir del 1978.

Aquest avenç seria realment útil perquè gràcies a aquesta innovació, es va poder utilitzar aquest sistema operatiu en diferents tipus d'ordinador, el qual significa que podria servir d'entorn de software comú per a ells i els usuaris no haurien de pagar per un nou disseny de software cada cop que una màquina es quedés obsoleta.

Fig 11. UNIX

A part de l'excel·lent portabilitat que oferia, també va servir per crear la filosofia de "fes-ho senzill", perquè no fes falta haver de consultar els manuals constantment, només calgués memoritzar el seu funcionament.

Les màquines habituals al principi de la cultura Unix eren les PDP-11 i la VAX, encara que gràcies a la seva nova portabilitat, es podia executar, pràcticament de la mateixa manera, en màquines diverses d'ARPANET.


Fig 12. PDP-11

En aquell moment ja no s'utilitzava el llenguatge assemblador, puix els programes en C eren molt més portables. Fins i tot, UNIX tenia el seu propi sistema de xarxes, de tipus UUCP: de baixa velocitat i poc fiables en la transmissió, però de baix cost.

Utilitzant línies telefòniques, qualsevol parell de màquines Unix podia enviar i rebre correus electrònics, i el 1980 es van començar a intercanviar notícies, creant un tauler d'anuncis que resultaria ser més gran que ARPANET.

Fig 13. VAX 11/780

El primer ordinador que va sortir a la venda va ser el 1975 i l'empresa Apple es va fundar el 1977. Amb intenció comercial, va sorgir la idea dels microordinadors, que va atreure una altra generació de joves hackers. S'utilitzava el llenguatge BASIC, que es considerava primitiu.

2.1.5 EL FINAL DELS VELLS TEMPS

L'any 1980, hi havia tres cultures en aquest món que semblaven semblants però estaven agrupades en tecnologies molt diferents.

La cultura del PDP-10 i l'ARPANET estava lligada a LISP, MACRO, TOPS-10, ITS i SAIL. La comunitat d'Unix i C ho estava amb els PDP-11 i els VAX, les connexions telefòniques i una gran quantitat d'entusiastes dels microordinadors, que tenien intenció d'oferir el potencial d'aquests ordinadors al poble.

2.1.6 ARRIBADA DEL HACKING ÈTIC

Amb l'arribada dels accessos no autoritzats, les vulnerabilitats i totes les amenaces que eren dirigides a la informació, va aparèixer el concepte d'ethical hacking, o sigui, hacking "ètic".

La idea també inclou les denominacions vulnerability scanning (un escaneig de les vulnerabilitats) i penetration test, també anomenat network security assessment, que consistia en comprovar la vulnerabilitat del sistema en el que s'estava treballant.

Fig 14. Escaneig de vulnerabilitats

Per tant, a mesura que cada cop més empreses o institucions digitalitzaven la seva informació, la demanda de seguretat en els seus sistemes creixia i, per consegüent, es necessitava oferta.

Fig 15. Comerç electrònic

Tot això succeïa sobre els anys 90. Fou quan va aparèixer l'e-commerce, format per la integració de les empreses al món de les xarxes.

Aquesta integració va resultar de molta utilitat ja que era un sistema molt pràctic. Però també hi havia inconvenients, ja que apareixia cada cop malware més sofisticat i es publicaven tècniques d'intrusió o explotació de les vulnerabilitats d'aquests sistemes.

Malware: És l'abreviació de malicious software (programes maliciosos) i engloba tots els programes i codis informàtics que s'han creat o manipulat amb intenció de causar un mal funcionament o sabotejar un sistema.

2.2 QUÈ ÉS UN HACKER? DE QUINS TIPUS N'HI HA?

En l'àmbit de la informàtica, un hacker és una persona apassionada, curiosa i dedicada a programar. Comunment, aquest terme és associat a un expert informàtic que utilitza els seus coneixements tècnics per superar un problema, normalment associat a la seguretat.

S'utilitza per a denominar informàtics amb grans coneixements en seguretat i amb la capacitat de detectar errors en sistemes informàtics per després reportar-los als desenvolupadors d'aquest software.

Hi ha una gran diferència entre hacker i cracker, ja que, encara que ambdós són experts en entrar en sistemes aliens, el segon ho fa amb un propòsit il·lícit. A més, el terme hacker no es limita a la seguretat informàtica, sinó que està associat a la resolució de qualsevol problema.

Fig 16. Diferència entre hacker i cracker

Normalment, es classifiquen associant-los amb el color d'un barret:

- **Hacker white hat (de barret blanc):** Són aquells que penetren la seguretat del sistema, i solen treballar per companyies en l'àrea de la seguretat informàtica per protegir el sistema de qualsevol alerta.
- **Hacker black hat (de barret negre):** També són coneguts com crackers. Mostren les seves habilitats informàtiques trencant sistemes de seguretat, col·lapsant servidors, entrant a zones restringides, infectant xarxes...
- **Hacker grey hat (de barret gris):** Tenen un coneixement similar als de barret negre. Se centren en penetrar sistemes i buscar problemes, per després cobrar per la reparació dels danys.
- **Hacker gold hat (de barret dorat):** És aquell que viola els sistemes informàtics amb la intenció de notificar la vulnerabilitat del sistema a l'administrador o col·lapsar ordinadors i servidors o entrar a zones restringides. Trenca la seguretat informàtica per posar a prova el seu propi sistema o el de la companyia on treballa.

Fig 17. Tipus de hackers segons el color del barret

- **Altres:**
  - **Phreaker:** Són persones amb grans coneixements en telèfons mòbils i modulars i tenen com a objectiu superar reptes intelectuals complexos que els permetin obtenir privilegis no accessibles de forma legal.
  - **Lammer o script-kiddie:** És un terme col·loquial associat a la manca d'habilitats tècniques. Són normalment adolescents que ells mateixos es denominen hackers o crackers sense tenir les habilitats necessàries. El seu abast es limita en buscar i descarregar programes i eines d'intrusió informàtica, cibervandalisme, i propagació de malware.

2.3 MALWARE I TIPUS DE MALWARE

Com abans he explicat, és un terme anglès que prové de la unió de les paraules "malicious software" o software maliciós.

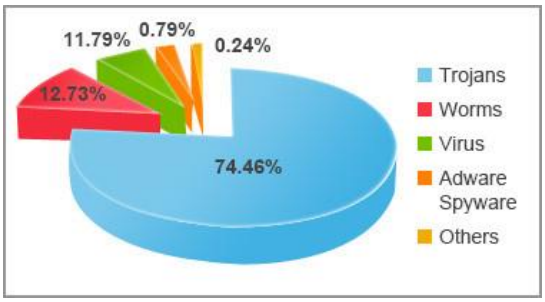

Fig 18. Gràfica dels tipus de malware

És un tipus de software que té com a objectiu infiltrar-se o causar danys a un ordinador sense el consentiment del seu propietari.

Per tant, el malware és el terme principal que s'utilitza per parlar de totes les amenaces informàtiques. Dins aquesta categoria, hi ha classificacions més específiques, com els troians, els cucs, els virus informàtics, els adwares, els spywares, ransomwares, hijackers...

Però, no sempre són malware els programes que posen en perill la nostra informació, sinó que poden ser simples programes amb errors de programació sense intenció però que són molt vulnerables a certs atacs o usurpació de dades.

2.3.1 D'ON PROVENEN?

Freqüentment, el malware accedeix al dispositiu a través d'Internet i del correu electrònic, encara que també pot aconseguir accedir a través de pàgines web hackejades, demos de videojocs, arxius de música, software, suscripcions gratuïtes o qualsevol cosa que sigui descarregada d'Internet.

2.3.2 PROPÒSIT

Encara que alguns dels primers programes infecciosos, com el Morris Worm i alguns virus com l'MS-DOS, van ser elaborats com a experiments, com a bromes o per molestar, no per causar danys a ordinadors, les intencions amb que es creava aquest programari van canviar. Començant pel 1999, en el que el virus Melissa (un macrovirus que infectava els documents de Microsoft Office) va tenir un impacte de nivell mundial, amb la simple intenció de molestar a companyies com Microsoft o Intel, arribant al punt de forçar-les a bloquejar les seves connexions a Internet.

També, a causa de l'augment d'usuaris a Internet, el malware ha arribat a ser dissenyat per treure'n benefici, ja sigui legalment o il·legal. Des de l'any 2003, la majoria dels virus i cucs han estat dissenyats per controlar ordinadors i explotar-los al mercat negre**.** Aquests ordinadors infectats, anomenats "zombis", són utilitzats per fer spam (enviament massiu) per correu electrònic,

per emmagatzemar contingut ilegal com pornografia infantil o, per exemple, unir-se a atacs DDoS.

Atac DDoS: És un atac de denegació de servei, que consisteix en atacar un sistema o xarxa d'ordinadors de manera que el servei sigui denegat als seus usuaris.

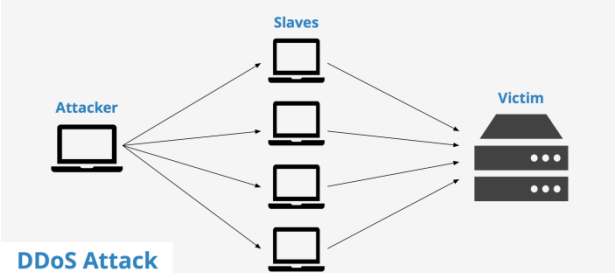

Fig 19. Representació gràfica d'un atac DDOS

2.3.3 MALWARE INFECCIÓS: VIRUS I CUCS

Els virus i els cucs (o "worms" en anglès i "gusanos" en castellà) són els tipus de malware més coneguts, bàsicament per la manera en què es propaguen.

Un virus informàtic és un programa que, en executar-se, es propaga infectant altres softwares executables dins del mateix ordinador. També poden tenir un payload**,** que duu a terme accions malicioses com esborrar arxius.

D'altra banda, un cuc és un programa que es transmet a si mateix, aprofitant-se de les vulnerabilitats en una xarxa d'ordinadors per infectar altres dispositius. El seu principal objectiu és infectar la major quantitat possible d'usuaris, encara que també poden contenir accions amb intencions nocives.

2.3.4 MALWARE OCULT

Perquè l'objectiu d'un malware pugui ser complert, és essencial que romangui ocult en el sistema. Si no, si l'usuari el detectés, simplement l'eliminaria i l'amenaça desapareixeria i, per tant, el malware hauria resultat inútil.

2.3.4.1 Backdoors

Els backdoors, o també coneguts com "portes posteriors", són un mètode per evitar els procediments habituals d'autentificació en connectar-se a un ordinador. Si ja s'ha accedit a l'ordinador desitjat anteriorment, es pot instal·lar

Fig 20. Representació gràfica d'un backdoor

aquest tipus de malware per a un futur accés simplificat, encara que també pot instal·lar-se abans d'infectar el sistema, per permetre l'entrada a aquest.

Ara bé, no sempre els backdoors són maliciosos, alguns cops venen integrats amb alguns programes per mantenir tasques de manteniment.

2.3.4.2 Drive-by downloads

Aquest terme es refereix als llocs web que duen a terme descàrregues de malware sense el consentiment de l'usuari, infectant així el sistema amb facilitat.

Els casos més freqüents d'aquests malware són en visitar una pàgina web, en llegir un correu electrònic o en entrar en una finestra pop-up, pot sortir un missatge d'error i l'usuari, en voler tancar-lo, descarregar un arxiu maliciós sense ser-ne conscient.

El procés d'atac d'aquest tipus de malware es fa automàticament mitjançant eines que busquen al lloc web alguna vulnerabilitat. Un cop l'han trobada, insereixen un script maliciós al codi HTML, de manera que quan un usuari visiti el lloc infectat, descarregarà aquest script al seu sistema i després es comprovarà si l'equip de l'usuari té alguna vulnerabilitat que pugui ser explotada posteriorment amb més scripts.

Ara bé, en la majoria de navegadors s'estan afegint bloquejadors antiphishing i antimalware que alerten l'usuari quan vol accedir a una pàgina web infectada, encara que no sempre ofereixen una protecció total.

2.3.4.3 Rootkits

Són una tècnica que modifica el sistema operatiu d'un ordinador per permetre que el malware que l'ha infectat romangui ocult. Per exemple, eviten que un procés maliciós sigui visible en la llista de processos del sistema o que els seus fitxers puguin ser buscats a l'explorador d'arxius.

Originalment, un rootkit era un conjunt d'eines instal·lades per un atacant a un sistema Unix, on l'atacant havia obtingut accés d'administrador (accés **root**).

També existeixen programes maliciosos que contenen rutines per evitar ser esborrats.

Fig 21. Representació gràfica d'un rootkit

Un exemple pot ser: “Existeixen dos processos fantasma que funcionen al mateix temps. Cada procés detecta quan l’altre ha acabat i comença una nova instància en qüestió de mil·lisegons, de manera que l’única manera d’eliminar els dos processos seria fer-ho simultàniament, la qual cosa és molt difícil i pot provocar un error al sistema.”

2.3.4.4 Troians

El terme **troià** sol ser utilitzat per anomenar un malware que permet un control remot d’un ordinador, de forma oculta i sense el consentiment del propietari, per part d’un usuari no autoritzat. Aquest tipus de malware és un híbrid entre un troià i un backdoor, no un troià segons la seva definició.

Hi ha diferents tipus de troians : backdoors, bankers, botnets, dialers, droppers, downloaders, keyloggers, password stealers, proxies.

Les formes més comunes de distribuir-lo és adjuntar-los a software descarregable d’Internet, de manera que quan l’usuari instal·la el software, també introdueix el troià dins el seu sistema.

Fig 22. Representació gràfica d’un troià

2.3.5 MALWARE PER OBTENIR BENEFICIS

2.3.5.1 Malware de distribució de publicitat

Spyware

Aquests programes són creats per obtenir informació sobre l'activitat d'un usuari i distribuir-la a agències de publicitat o organitzacions interessades.

Normalment, acostumen a enviar spam a les direccions de correu electrònic amb les quals s'ha interactuat. La informació s'obté a partir de spyware que s'ha instal·lat de manera legal junt amb altre software (segurament a causa de que l'usuari no ha llegit els termes d'ús i condicions abans d'instal·lar-lo).

Ara bé, també hi ha spyware il·legal i que pot comportar greus problemes, ja que poden robar informació d'índole personal fins dades bancàries.

Fig 23. Representació gràfica d'un spyware

Adware

Són programes que mostren publicitat intrusiva a un usuari, principalment en forma de finestra emergent (pop-up). És molt molest, ja que apareix de forma inesperada i constantment.

També existeixen els programes shareware, els quals són molt semblants als adware, però amb la diferència que en aquests els usuaris accepten veure publicitat a canvi d'un ús gratuït del software.

Hijackers

Són un tipus de malware que modifiquen la configuració del navegador web. Alguns canvien la pàgina d'inici del navegador per pàgines web de publicitat o pornogràfiques i uns altres redireccionen les recerques de l'usuari a anuncis de cost o pàgines phishing bancàries (pàgines falses que imiten les reals).

2.3.5.2 Malware per robar informació personal

Keylogger

És un tipus de malware que s'encarrega de registrar les pulsacions que es realitzen en el teclat, per emmagatzemar-les posteriorment en un arxiu o enviar-les a través d'Internet.

Solen funcionar en segon pla i són ocultes a l'usuari, de manera que es pugui conèixer contrasenyes importants, el número d'una targeta de crèdit, informació privada...

El registre de les pulsacions pot fer-se tant amb mitjans de hardware com de software.

Amb hardware, es pot fer mitjançant adaptadors que s'interposen en la connexió del teclat, amb l'avantatge que poden ser instal·lats instantàniament. No obstant, amb una revisió visual detallada, poden ser advertits fàcilment.

Fig 24. Hardware d'un keylogger

També, es pot fer mitjançant dispositius que es poden instal·lar dins els teclats, però es requereix habilitat per soldar i tenir accés al teclat. Són indetectables si no s'obre el cos del teclat.

Amb software, n'hi ha tres tipus:

- Es pot fer amb software basat en nucli (és el procés més difícil), que enderroquen el nucli del sistema operatiu, així allotjant-los-hi i fent-los pràcticament invisibles. Un exemple seria un driver del teclat, que accediria a tota la informació registrada en aquest.
- **Enganxats**: Aquests keyloggers registren les pulsacions de les tecles del teclat amb les seves respectives funcions. El sistema operatiu activa el keylogger quan es pressiona una tecla, i es fa el registre.
- **Mètodes creatius**: Són els més fàcils de programar, però poden augmentar l'ús de la CPU (unitat central de processament) i deixar escapar algunes pulsacions del teclat.

Per protegir-nos d'aquest tipus de malware, podem fer ús de programes anti-spyware, d'un firewall (un tallafocs que també pot prevenir la descàrrega d'arxius maliciosos), de monitors de xarxa (evitarien que l'informació robada s'enviés a través d'internet) o, amb un software més concret per a l'ocasió, software anti-keylogging, que conté una llista de tots els keyloggers coneguts i busca els seus arxius al disc dur, però amb el desavantatge que és vulnerable a keyloggers nous o desconeguts.

Stealers

Aquest tipus de malware també roba l'informació privada, però només la que està emmagatzemada a l'equip, per exemple, les contrasenyes recordades en programes o navegadors web.

Fig 25. Representació gràfica d'un stealer

2.3.5.3 Malware per realitzar trucades telefòniques

Dialers

Són programes maliciosos que prenen el control del mòdem dial-up (connexió que utilitza un mitjà telefònic analògic), fan una trucada a un número de telèfon de tarifació especial i deixen la línia oberta carregant el cost de la trucada a l'usuari infectat.

La forma més habitual de distribuir aquest malware és a través de pàgines web que ofereixen contingut gratuït només a través de connexió telefònica. Solen utilitzar com esquer videojocs o pornografia.

Actualment ja no són tan populars, ja que la majoria de connexions a Internet són mitjançant ADSL i no mitjançant un mòdem.

2.3.5.4 Realització d'atacs distribuïts

Botnet

Són xarxes d'ordinadors infectats, també anomenats "zombis", que poden ser controlats per un sol usuari a la vegada i fan diverses feines.

Aquestes xarxes són utilitzades per enviar spam massivament o per executar atacs DDoS contra organitzacions en forma d'extorsió o per impedir el seu correcte funcionament.

L'ús d'ordinadors infectats permet als spammers romandre en l'anonimat, el qual els protegeix de la persecució policial.

Fig 26. Representació gràfica d'una botnet

2.3.5.5 Altres tipus

Rogue software

Fa creure a l'usuari que està infectat per algun tipus de virus o de software maliciós, induint-lo a pagar per poder instal·lar un software maliciós que suposadament elimina les infeccions, però l'usuari no el necessita, ja que no està infectat.

Ransomware

També anomenat com "malware segrestador", és un tipus de malware que xifra els arxius importants de l'usuari, fent-los inaccessibles, i demanant que es pagui un rescat per rebre la contrasenya que els permet recuperar.

S'ha informat que a partir del 2012, hi ha hagut dues variants del "virus de la policia", produït pel troià Ransom.ab que, amb el pretext que l'usuari havia entrat a pàgines amb pornografia infantil, es fa pagar una multa per desbloquejar l'equip, adjuntant suposades preses de vídeo utilitzant la pròpia càmera web de l'ordinador, o la versió falsa de l'antivirus Microsoft Security Essentials, que ens notifica "bloquejar l'equip per seguretat" i que perquè es pugui tornar a utilitzar s'ha de pagar un mòdul especial.

Fig 27. Representació gràfica d'un ransomware

2.4 PREVENCIÓ DE MALWARE

2.4.1 COM DETECTAR UN MALWARE?

Per a un usuari comú, detectar qualsevol tipus de malware és bastant complicat si no es disposa de les eines adequades, perquè la majoria de codis maliciosos passen inadvertits, ocultant qualsevol comportament que pugui resultar estrany a l'usuari.

Ara bé, hi ha alguns tipus de malware, com els adware, els rogue software o els ransomware, que són fàcilment detectables.

Per exemple, si observem que la pàgina d'inici o de cerca d'un navegador web ha canviat o redirigeix els resultats de Google cap a altres llocs web, si s'emeten falsos missatges d'alertes o infeccions al nostre sistema, si s'impedeix la instal·lació o execució de programes o l'actualització de software de seguretat o antivirus, si llocs web de seguretat o fòrums on s'explica com eliminar les amenaces es troben bloquejats, o si hi ha un bloqueig total de l'ordinador, com en el cas dels ransomware.

2.4.2 QUÈ CAL FER?

Primerament, cal evitar-ne la propagació. Si analitzem bé un correu electrònic, podrem saber si és perillós o no. Per això, cal fixar-nos en alguns punts clau, com l'assumpte (o títol) del correu, observant si està en un altre idioma o si la traducció al nostre idioma és errònia i, per tant, deduïm que s'ha utilitzat un traductor online. Si el remitent és una empresa, cal que comprovem si la direcció de correu electrònic coincideix amb l'original (podem buscar-ho a la seva pàgina web o anteriors correus dels quals tinguem constància que són segurs).

Sobretot, si hi han arxius adjunts amb extensions desconegudes, com XLSM o DOCM, hem d'evitar executar-los, ja que el resultat podria ser la pèrdua dels teus documents i la sol·licitud d'una recompensa econòmica per poder recuperar-los. Així doncs, cal remarcar que qualsevol dada personal com contrasenyes no s'han de donar sota cap circumstància, especialment si és de caire bancari.

Si resulta que el nostre sistema ha estat infectat, és molt recomanable demanar ajuda a una persona especialitzada en la seguretat informàtica perquè, si per exemple accedíssim a pagar l'extorsió, aquesta no cessaria, i cada cop aniria augmentant.

En acabat, si descobrim que el nostre ordinador està infectat, és molt important mirar si hi ha algun dispositiu de memòria USB ja que si és el cas, abans de retirar-lo, hem de netejar-lo de malware, ja que possiblement els seus arxius també han estat infectats i així previndrem la infecció dels ordinadors als quals el connectem posteriorment.

3. GRUPS DE HACKERS: SÓN TOTS DOLENTS?

De la mateixa manera que els animals, els hackers que lluiten per un objectiu comú també acostumen a atacar en grup. En alguns casos, aquests grups arriben a fer-se famosos per un bon motiu, com quan aconsegueixen enderrocar pàgines web de grups terroristes, però, en altres casos, actuen al marge de la llei.

En la majoria de casos, els hackers de barret negre o també anomenats crackers, són considerats dolents, ja que malmeten o perjudiquen persones alienes amb la intenció d'aconseguir beneficis per a ells mateixos. Acostumen a actuar en solitari o en petits grups que aspiren a la discreció màxima, ja que no els interessa ser famosos i ser descoberts per les institucions policials; només volen aconseguir el seu objectiu (sol ser d'àmbit econòmic) i romandre en l'anonimat.

D'altra banda, hi ha agrupacions que vetllen pel bé comú de la societat, com bé podria ser eliminant llocs web de pornografia infantil i de phishing, i que accepten ser reconegudes encara que actuïn anònimament. No tenen cap intenció lucrativa ni de benefici propi, sols busquen millorar el món que ens envolta. En aquest sentit, podem citar Anonymous.

També, per necessitat dels governs de combatre els ciberterroristes, que en els darrers anys han incrementat dràsticament, financen grups de hackers per poder mantenir una seguretat òptima respecte els seus arxius i els seus usuaris dels possibles atemptats cibernètics. En alguns casos la intenció amb la qual els financen no és simplement mantenir la seguretat, sinó atacar i defensar-se d'altres països.

Fig 28. Participants del congrés de hackers CCC

3.1 GRUPS DE HACKERS FAMOSOS ASSOCIATS A GOVERNS

3.1.1 SYRIAN ELECTRONIC ARMY (SÍRIA)

És un grup de hackers que va es va formar el 2011 per donar suport al govern sirià, presidit per en Bashar al-Assad.

Utilitzant l'spam, la desfiguració de llocs web, malware, phishing i atacs de denegació de servei, marca com objectius els grups polítics d'oposició i els que es mostren neutrals al conflicte sirià, així com també ha hackejat llocs web de governs europeus.

La història d'aquest grup començà els anys 90 del segle anterior, quan el líder polític Bashar al-Assad encapçalava dirigia la Syrian Computer Society i mantenia una censura respecte a Internet, però es va aixecar la prohibició respecte a Facebook i YouTube. El 5 de maig de 2011, la SEA va registrar el domini de la seva pàgina web, però negant que era a càrrec de l'estat.

Fig 29. Logo de la SEA

3.1.2 AJAX SECURITY TEAM (IRAN)

En aquest cas, el grup també concentra les forces en l'eix polític, no només realitzant atacs a llocs web, sinó mitjançant l'espionatge.

Principalment, els seus atacs estan dirigits a dissidents iranians o governs enemics, com el nord-americà.

Encara que el grup nega mantenir contacte amb el govern, però és lògic que és de molta utilitat per al govern iranià disposar d'un equip de ciberespies entrenats.

L'AST forma part dels grups hacktivistes més agressius, és dels que treballa sense escrúpols per aconseguir els seus objectius.

3.1.3 APT28 (RÚSSIA)

Encara que no hi ha dades que confirmin que aquest grup pertany al país, algunes agències d'investigació conclouen que els seus membres són de parla russa, i és lògic en certa manera ja que Rússia té un pes molt gran al ciberespai.

Alguns dels seus objectius són la Casa Blanca i Geòrgia i, fins i tot, la guerra amb Ucraïna. D'aquesta manera, el govern rus podria estar en contra la CIA, una important agència d'intel·ligència, amb blancs molt importants pel president Putin.

3.1.4 UNIT 61398 (XINA)

La Madiant, una firma de ciberseguretat americana, ha estat una de les quals ha acusat el govern xinès de finançar i donar suport a aquest grup de hackers perquè robés informació valuosa de més de 140 organitzacions angloparlants.

Fig 30. Grup de hackers xinesos d'Unit 61398

Encara que Xina nega qualsevol tipus de contacte amb aquest grup, tot indica que era obra d'alguna

cosa més que simples hackers.

3.1.5 AXIOM (XINA)

Un altre grup perillós identificat en aquest país és l'Axiom, el qual ha estat detectat per importants organitzacions com Microsoft, Symantec o Bit9, i també s'ha considerat el responsable de l'atac a Google el 2010.

Tot i que se sap que és un grup pertanyent al país, es desconeix la seva ubicació i, en teoria, els atacs a organitzacions i institucions a favor de la democràcia són actes aïllats al govern xinès... Tanmateix, aquests actes apunten cada cop amb més intensitat cap una col·laboració clandestina amb la nació.

3.1.6 GOP I BUREAU 121 (COREA DEL NORD)

No podien faltar grups d'aquest caire en aquest país tan misteriós i que tanta por infon a la resta del món a causa de la seva política restrictiva.

Aquests grups són Guardians of Peace i Bureau 121.

Fig 31. Grup militar nord-coreà

Alguns dels seus atacs han estat els ciberatacs contra la pel·lícula "The Interview" i l'empresa Sony Pictures, que no només van retardar l'estrena, sinó que van crear un debat intern a l'empresa. Ara bé, aquests atacs van estar atribuïts a Guardians of Peace, mentre que la facció Bureau 121, també vinculada al govern de Kim Jong-Un, també va ser esmentada com a sospitosa.

3.1.7 HIDDEN LYNX (XINA)

Batejat així per la corporació nord-americana Symantec, és dels grups de hackers més nous i perillosos, tenint al seu registre un intent d'atac a la pròpia empresa de seguretat Bit9.

És un esquadró d'alt perfil que s'enfoca en organitzacions de màxima seguretat, com la de la pròpia Xina, Estats Units o Corea del Sud.

Amb un personal que oscil·la en els 100 membres, és un dels equips actualment amb millors habilitats, encara que no se sap si és un grup independent o té relació amb el govern xinès. Ara bé, considerant la infraestructura de la qual disposen, és evident que són aliats del poder.

Fig 32. Logo i eslògan de Hidden Lynx

3.2 ELS GRUPS DE HACKERS INDEPENDENTS MÉS PODEROSOS

En aquest cas, no ens referim a hackers en específic, com podrien ser Kevin Mitnick o Tsumou Shimoura, sinó a grups que es dediquen a concentrar forces per explotar vulnerabilitats amb finalitat acadèmica, de diversió o lucrativa.

Fig 33. Kevin Mitnick

3.2.1 CHAOS COMPUTER CLUB

És l'associació de hackers més gran d'Europa i té la seva seu a Alemanya i a altres països de parla alemanya. Els seus principals interessos són el hacking, la ciència, la sociologia, la cultura hacker i la comunitat.

El 1981, aquest grup va traspassar els sistemes de seguretat d'un banc alemany robant cent mil dòlars de l'època, els quals van tornar el dia següent amb una nota que deia: "Vigileu amb el vostre sistema de seguretat, té errors."

3.2.2 TEAMP0ISON

És un grup de recerca de seguretat informàtica format entre tres i cinc membres. Va guanyar notorietat entre el 2011 i el 2012 a causa de les seves activitats de hackers de barret negre, atacant els EUA, la NASA, una web de les Nacions Unides, Facebook i moltes més corporacions i entitats governamentals.

Són considerats hacktivistes polítics i han interceptat correus electrònics filtrats amb informació confidencial de polítics als medis.

Fig 34. Logo de TeaMp0isoN

3.2.3 THE LEVEL SEVEN CREW

Al llarg dels anys 90, van aconseguir hackejar seixanta ordinadors de la NASA, la xarxa d'hotels Sheraton, van segrestar la web de l'ambaixada nord-americana a Xina i van enderrocar sistemes de seguretat per obtenir informació.

Finalment, l'any 2000, després d'haver estat perseguits i pressionats per diverses agències de seguretat a nivell mundial, el grup va ser dissolt per l'FBI.

3.2.4 LULZSEC

És un grup de hackers de barret gris i el seu lema es "Laughing at your security since 2011", el qual significa "Burlant-nos de la teva seguretat des del 2011".

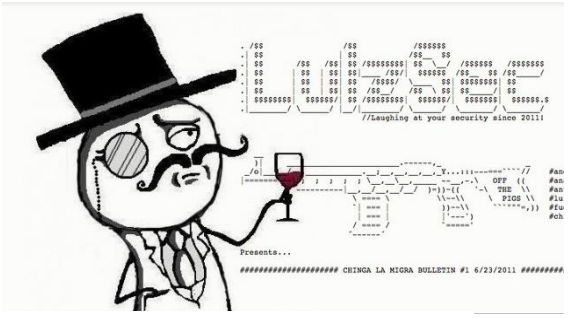

Fig 35. Logo de LulzSec

Encara que van aconseguir causar estralls a les webs de la CIA i l'FBI, la seva millor gesta va ocórrer l'any 2012, quan van hackejar un milió de perfils d'usuaris de Play Station 3.

Actualment, aquest grup es troba gairebé desmantellat, ja que Sabu, un dels seus líders, va delatar un gran nombre de membres per reduir la seva sentència penal.

3.2.5 THE NETWORK CRACK PROGRAM HACKER GROUP

Aquest grup, format el 1994, prové d'un país asiàtic, va guanyar notorietat després d'haver hackejat el 40% de les pàgines webs d'associacions de hackers a Xina i, a mesura que els seus atacs anaven incrementant, van rebre atenció dels mitjans de comunicació a principis del 2017.

Després que el seu líder fos reclutat pel govern, la resta del grup també ho va ser i van conformar un tipus de comandament no oficial de ciberseguretat de Xina. Els són atribuïts una sèrie de ciberatacs a sistemes del govern nord-americà.

3.2.6 ANONYMOUS

Sorgit dels fòrums 4chan i Hackers Forum en un principi com a moviment de diversió, aquest grup es manifesta amb accions de protesta i de reivindicació de la llibertat d'expressió, de la independència d'Internet i en contra d'organitzacions de serveis públics i societats de drets d'autor.

Al començament, els seus participants només actuaven a través d'Internet, però actualment també en desenvolupen fora de la xarxa.

Es tracta d'una organització descentralitzada i no jeràrquica formada per hacktivistes de diferents països, i xarxes socials com Twitter o YouTube han eliminat diverses vegades els seus comptes com a mesura de protecció de la informació.

Fig 36. Logo del grup Anonymous

4. CRIPTOGRAFIA

Parlant des d'un àmbit general, aliè a la informàtica, la criptografia és una ciència que tracta les escriptures ocultes. Les seves arrels etimològiques són criptos (del grec kryptos, ocult) i graphos (del grec graphein, escriptura).

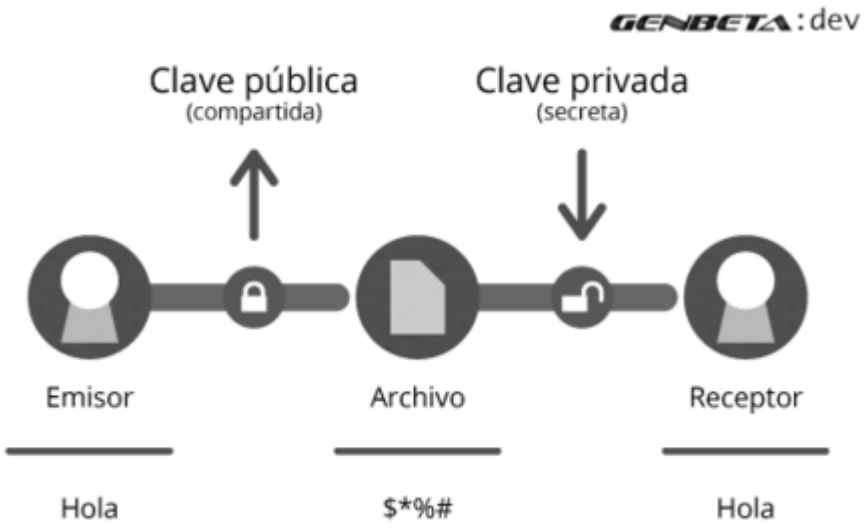

Fig 37. Representació gràfica de la criptografia

Està estructurada en: criptografia, criptoanàlisi i esteganografia.

La criptografia és la ciència que s'encarrega d'estudiar les tècniques per transformar la informació de manera que no pugui ser entesa a simple vista. Ara bé, la seva finalitat no és únicament protegir aquestes dades i mantenir-les en secret, també s'encarrega d'evitar que siguin modificades i comprovar-ne la font.

D'altra banda, la criptoanàlisi, és la ciència que s'encarrega de l'anàlisi d'un text xifrat per obtenir la informació original sense conèixer la clau secreta, de manera que es pot considerar una ciència complementària però contrària a la criptografia.

L'esteganografia, estudia la forma d'ocultar l'existència d'un missatge, de manera que amaga a l'interior d'un missatge un altre missatge secret, el qual només serà entès per l'emissor i el receptor i passarà inadvertit per la resta.

4.1 HISTÒRIA DE LA CRIPTOGRAFIA

4.1.1 PRIMERS MÈTODES

Aquesta ciència neix a causa de la necessitat que ha desenvolupat l'ésser humà de transmetre informació confidencial a altres persones, ja sigui per

motius militars, diplomàtics, comercials... on mantenir la informació en secret és la clau per mantenir la integritat d'un individu o una comunitat.

Un dels primers mètodes consistia en fer forats a les lletres del missatge secret per passar-hi per sobre amb un teixit que servia per amagar el missatge.

Aproximadament l'any 1500, els comerciants assiris feien servir taules d'argila, on tallaven imatges que establien la manera de dur a terme les transaccions comercials, les quals es posaven dins un recipient i es segellaven.

Al llarg del segle V a.C., els grecs van crear una eina per xifrar missatges. Aquest instrument era conegut com l'Escítala dels Lacedemonis**,** i consistia en un cilindre de fusta en el qual s'enrotllava una cinta de papir o de teixit. Un cop estava enrotllat, s'hi escrivia segons les generatrius del cilindre i després tornava a desenrotllar.

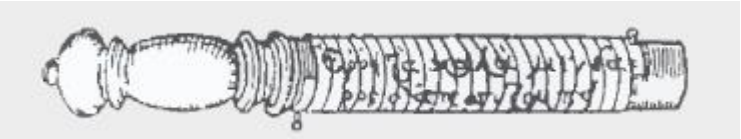

Fig 38. Escítala dels Lacedemonis

D'aquesta manera, s'enviava a un receptor el qual disposava d'un cilindre de la mateixa mida, pel qual enrotllant-hi el papir podia veure el missatge original. Encara que sembli obvi, quan el missatge no estava enrotllat era confús i incoherent.

Un altre mètode que era utilitzat pels escrivans hebreus era utilitzar l'alfabet a l'inrevés, és a dir, quan volien escriure la primera lletra de l'alfabet escrivien l'última, i així successivament. Aquest mètode era anomenat codi mirall o Atbash.

A mitjans del segle II a.C., va sorgir un altre mètode, atribuït a l'historiador Polybios. Era similar a l'anterior, ja que consistia en substituir un caràcter per un parell de caràcters que li corresponien segons una taula dissenyada amb aquest propòsit.

Al cap de cinquanta anys, durant el segle I a.C., va aparèixer un procés similar als anteriors conegut com el xifrador del Cèsar, ja que era utilitzat pel militar i polític romà Juli Cèsar. Aquest, però, consistia en substituir cada caràcter del missatge original per un altre situat tres posicions més endavant a l'alfabet.

A finals d'aquest mateix segle, van haver innovacions en les tècniques de xifrar missatges. Per exemple, a l'antiga Roma, els missatges eren escrits en una taula que es cobria amb cera per amagar la informació. També, van utilitzar un mètode molt diferent als anteriors, que consistia en rapar un esclau, escriure-li el missatge al cap i, un cop li havia tornat a créixer el cabell, enviar-lo al receptor, qui l'havia de rapar per poder llegir el missatge. Ara bé, era comú tallar la llengua als esclaus, de manera que si eren interceptats, no poguessin dir que duien un missatge al cap.

Durant la persecució cristiana, els creients catòlics també es van veure obligats a utilitzar aquesta ciència, de manera que expressaven la seva idea de l'existència de Déu mitjançant símbols (els quals eren marques de tallers

monetaris, perquè els perseguidors no ho poguessin relacionar amb el cristianisme, ja que eren comuns per tothom).

4.1.2 DESENVOLUPAMENT DE LA TÈCNICA CRIPTOGRÀFICA

Aproximadament l'any 1300, els àrabs havien desenvolupat uns 7 procediments de xifrat:

- Substituir lletres per altres.
- Escriure paraules a l'inrevés.
- Invertir lletres de manera alternada.
- Assignar valors numèrics a les lletres i, a més a més, escriure aquests valors amb símbols.
- Reemplaçar cada lletra per dues altres de manera que, sumant el seu valor numèric, s'obtingués el mateix valor numèric que la lletra substituïda.
- Substituir cada lletra amb el nom d'una persona o d'un ocell
- Substituir les lletres per símbols lunars, flors o ocells

Cap a l'any 1380, Cicco Simonetta, conseller i secretari dels ducs Sforza de Milà, va crear el tractat de desxiframent més antic que es coneix, anomenat Liber Zifrorum, en el qual estudia i analitza diversos sistemes criptogràfics, i també es va crear un manual de criptografia per encàrrec de l'Antipapa Clement VII, similar a l'anterior.

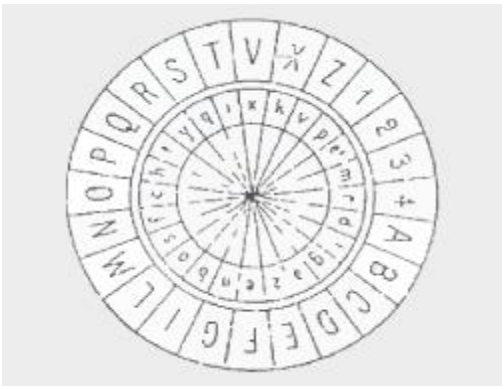

Fig 39. Xifrador de Leon B.A.

Al cap d'uns 80 anys, León Battista Alberti, que era secretari pontifici de la cort romana, va deixar de banda la substitució de lletres per símbols i va afegir una mica de complexitat a l'encriptament del missatge, inventant un disc de xifrat format per discs concèntrics.

Al segle XVI, una altra obra destacada va ser publicada, la Poligraphiae, creada per l'historiador i religiós alemany Trithemius. En ella es desenvolupa un procediment de xifrat que consisteix en substituir lletres per paraules, de manera que la seva juxtaposició formés un text lògic i no fos sospitós.

Aquest mateix segle, va néixer un nou mètode anomenat trepa o màscara rotativa, ideat per Girolamo Cardano, que consistia en una petita taula amb perforacions que es col·locava damunt una altra taula, de manera que girant la perforada en el sentit de les agulles del rellotge el missatge era llegible.

Fig 40. Llibre de codis de Felip II

El 1595, Blaise Vignère va inventar un mètode de xifrat que consistia en assignar un número a cada lletra de l'alfabet i sumar els nombres que els representaven a una clau per poder obtenir el criptograma. Durant aquest segle, els llibres de codi per xifrar els missatges van ser molt utilitzats, com per exemple, els llibres de codi de Felip II.

El 1790, Thomas Jefferson va crear un cilindre format per diversos discs coaxials on cadascun tenia un escrit en la part exterior. Cadascun s'ajustava de manera que en una generatriu del cilindre es mostrés el missatge de manera clara, i el criptograma es podia obtenir de qualsevol generatriu.

El 1854, Charles Wheatstone va dissenyar un mètode de xifrat anomenat Playfair, el qual era semblant al de Polybiod, però, en aquest cas, cada caràcter se substituïa per un, en comptes de dos.

Cap al final de la següent dècada, Wheatstone havia ideat un nou disc de xifrat que en realitat era una versió mecànica del disc d'Alberti, però aquesta versió mostrava l'alfabet anglès amb un signe de "+" col·locats ordenadament en sentit de les agulles del rellotge i el disc inferior només tenia 26 caselles amb l'alfabet col·locat de manera desordenada.

Van sorgir molts mètodes matemàtics a l'època anterior a la Segona Guerra Mundial, principalment amb l'aplicació de les tècniques estadístiques al desenvolupament del criptoanàlisi i del xifrat, per William F. Friedman, i de la ruptura inicial de Marian Rejewski de la versió de l'exèrcit alemany d'Enigma. Però a partir de la Segona Guerra Mundial, tant la criptografia com el criptoanàlisi es van fer molt més matemàtics.

4.1.3 CRIPTOGRAFIA A LA SEGONA GUERRA MUNDIAL

Durant la Segona Guerra Mundial, les màquines de xifrat mecàniques i electromecàniques s'utilitzaven molt, encara que els sistemes manuals continuaven utilitzant-se i és van fer grans avenços de la ruptura de xifrats en secret. El matemàtic Rejewski va reconstruir el 1932 la màquina Enigma de l'exèrcit alemany, gràcies a la documentació proporcionada per la intel·ligència militar francesa.

Fig 41. Màquina Enigma

Poc després que comencés aquesta guerra, l'1 de setembre de 1939, el personal clau de l'Oficina de Xifrat, que dirigia la criptografia d'aquell període, va ser evacuat. Un cop els integrants de l'Oficina de Xifrat van ser prop de París, van continuar treballant en desxifrar l'Enigma amb la col·laboració dels criptòlegs britànics de Bletchley Park. Amb el temps, els criptòlegs entre els quals es trobaven Gordon Welchman i Alan Turing, van fer progressar ràpidament l'escala i la tecnologia del desxifrat Enigma.

El 19 d'abril de 1945, es va ordenar als oficials superiors britànics que no es podia revelar que s'havia desxifrat el codi de la màquina Enigma de l'Alemanya nazi, ja que li donaria l'oportunitat a l'enemic de dir que havia estat una victòria injusta.

4.1.4 CRIPTOGRAFIA MODERNA

4.1.4.1 Shannon

L'era de la criptografia moderna comença amb Claude Shannon, el pare de la criptografia matemàtica. Fou qui publicà l'article Communication Theory of Secrecy el 1949 i poc després, el llibre Mathematical Theory of Communication, junt amb Warren Weaver.

Aquests treballs van establir la base teòrica de la criptografia i el criptoanàlisi.

4.1.4.2 Criptosecretisme

Lentament, la criptografia va anar incorporant-se a les organitzacions governamentals que es dedicaven a l'espionatge i al contraespionatge. De totes aquestes, la més important va ser la NSA, als Estats Units, la qual va bloquejar gairebé totalment qualsevol publicació sobre avenços en el camp de la criptografia des de principis dels anys 50 fins a mitjans dels anys 70 i, per això, tota la informació disponible sobre el tema era molt bàsica i antiquada.

Per aconseguir-ho, van disposar d'una plantilla de treballadors molt àmplia i amb equipament molt car, van obligar els investigadors que tenien relació amb la NSA mantenir la informació en secret, es va pressionar perquè no es publiquessin articles o llibres sobre criptografia, ja que per llei revelar informació sobre la criptografia era considerat un acte de traïció. També se supervisaven totes les sol·licituds de patents relacionades amb la criptografia i era permès considerar com secreta qualsevol idea perillosa per un domini públic.

4.1.4.3 Criptoanàlisi moderna

Encara que els xifrats moderns com l'AES estan considerats irrompibles, encara hi ha mals dissenys i hi ha hagut ruptures criptoanalítiques importants.

Alguns exemples famosos de dissenys criptogràfics que s'han trencat són el DES, el WEP (el primer esquema de xifrat Wi-Fi), el sistema Content Scramble System, utilitzat per xifrar i controlar l'ús dels DVD i els xifrats A5/1 i A5/2, utilitzats als telèfons mòbils GSM.

A més a més, no s'ha demostrat que aquests sistemes siguin irrompibles, per tant, probablement al futur hi haurà un descobriment que els farà insegurs.

4.2 CRIPTOGRAFIA A L'EMPRESA

Des del punt de vista de l'empresa, s'ha de desenvolupar un sistema que permeti mantenir converses segures a través de mitjans insegurs i protegir la informació i per això s'han creat les firmes digitals.

Una firma digital és un mecanisme que està destinat a verificar l'origen del missatge. És un mecanisme complementari a la criptografia, ja que es basa en algoritmes criptogràfics mentre que la criptografia es preocupa de verificar que en el procés de transmissió la informació no sigui interceptada.

Per tant, dins d'una empresa, la firma digital permet:

- Validar la integritat de les dades, de manera que qualsevol canvi en el missatge tindria com a resultat que el receptor registraria la firma com a invàlida.

- L'autenticació, perquè el destinatari pugui confirmar que la persona qui ha enviat el missatge és la correcta, ja que és l'única que té la clau secreta.

- L'absència de rebuig, de manera que qui enviï el missatge, després no pugui negar que el va generar i enviar.

- Una protecció contra el reenviament, sobretot en les instruccions de pagament com factures, mitjançant una seqüència de temps que fa els missatges únics i els permet ser verificats pel destinatari per poder assegurar que no han estat interceptats.

Ara bé, l'autenticació a vegades pot ser un aspecte amb vulnerabilitats de les quals se n'aprofiten empreses d'SPAM i software maliciós mitjançant l'spoofing, és a dir, suplantacions d'identitat.

Per evitar això, s'utilitza un sistema de validació PKCS, en el qual es fa servir criptografia asimètrica i una entitat certificadora externa que fa de notari. D'aquesta manera, es crea un certificat digital que es farà servir amb una

finalitat concreta, correu electrònic, pàgina web... i és reconegut per aquesta entitat, la qual també s'encarrega de reconèixer l'usuari.

Mitjançant aquestes tècniques també existeixen els protocols SSL i els sistemes de pagament SET, els quals permeten validar tant un servidor web com un usuari que hi accedeix. Són els mitjans considerats com més efectius per fer qualsevol transacció o comerç electrònic. Encara que tingui un gran cost, té molts beneficis, ja que la entitat certificadora és universal i permet sortir del nivell nacional.

Un altre tipus de sistema de validació és el PGP, el qual és més personal i permet mantenir relacions confidencials on l'anterior sistema és massa car o el seu ús està injustificat. El principal avantatge d'aquest sistema és el baix cost que suposa implantar-lo, a part d'oferir una estructura al client perquè pugui obtenir informació sobre els autèntics emissors de la informació.

Finalment, si volem implantar un emmagatzematge encriptat perquè la seguretat de les dades es mantingui vigent, cal pensar en:

- **Un pla de continuïtat**, de manera que sempre sigui possible la recuperació de les dades per mitjans aliens als treballadors ja que, d'altra banda, seria molt perillós perquè en cas que un treballador morís, es podria perdre l'accés a tota la informació.
- **Accessibilitat a la informació,** és a dir, disposar d'un gestor de correu que permeti fer recerques als documents.
- **Vigilar els costs d'implantació,** tenint en compte que només dues o tres persones de l'empresa disposaran del coneixement de tota la informació. També, la criptografia pot ser recomanable per evitar accessos indesitjats mitjançant visors de documents.

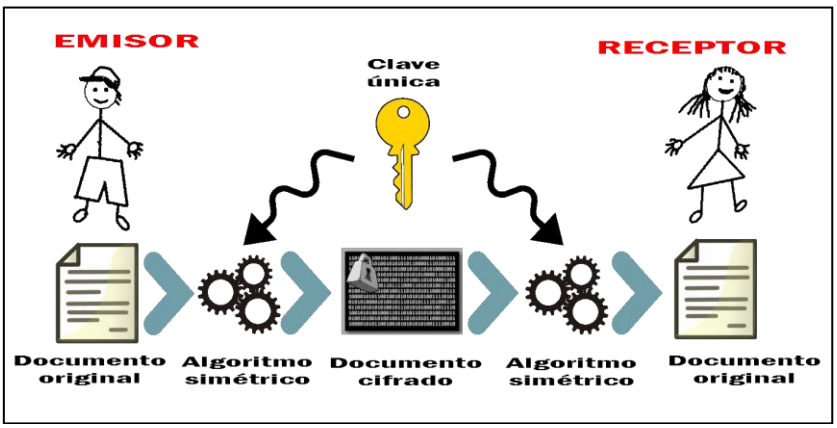

Fig 42. Representació gràfica de la criptografia a l'empresa

5. PART PRÀCTICA

5.1 CREACIÓ D'UNA APLICACIÓ PER A ANDROID

5.1.1 METODOLOGIA DEL TREBALL

Abans de començar la part pràctica del treball, vaig parlar amb el tutor del treball i vam acordar que consistiria en crear una aplicació que pogués ser útil i ambientada a l'INS Flix.

Per poder crear-la vaig haver de:

- Pensar un model d'aplicació útil per al professorat i que fos adient a les seves necessitats respecte a la seguretat informàtica.
- Decidir amb quines eines la desenvoluparia. El tutor em va recomanar l'App Inventor, ja que és molt pràctic.
- Aprendre a utilitzar l'App Inventor, ja que a l'institut on vaig cursar l'ESO no el vam utilitzar.
- Repassar el funcionament de programes d'edició d'imatge per crear el logo i/o modificar alguna imatge.

5.1.2 OBJECTIUS

El principal objectiu amb què he creat l'aplicació ha estat didàctic puix el fet de no haver treballat mai amb aquesta eina ha fet que em resultés interessant i em motivés a aprendre'n el seu funcionament. No obstant això, també he intentat que sigui útil per utilitzar-la en el dia a dia.

L'aplicació permetrà crear un usuari amb la contrasenya desitjada i emmagatzemar les contrasenyes de plataformes educatives com poden ser el correu XTEC, Gmail, el Moodle Àgora i el Clickedu, entre altres de miscel·lània, com dades bancàries, de xarxes socials...

La part més complicada a l'haver de fer-la útil és a l'hora de programar l'aplicació, ja que si es vol fer-la segura hi ha molts aspectes que s'han de vigilar perquè no hi hagi llacunes de seguretat.

5.1.3 PROCEDIMENT

Per poder començar a programar-la, després d'haver adquirit els coneixements sobre l'App Inventor necessaris, haurem d'accedir a la pàgina web http://appinventor.mit.edu/explore/# i clicar al botó "Create apps!". Allí escollirem el nostre compte de Gmail i ja podrem accedir a la pantalla de crear el projecte d'aplicació.

Fig 43. Pàgina web de l'App Inventor

Un cop ja haguem accedit, farem clic a "Start a new project" i li posarem com a nom "TDR".

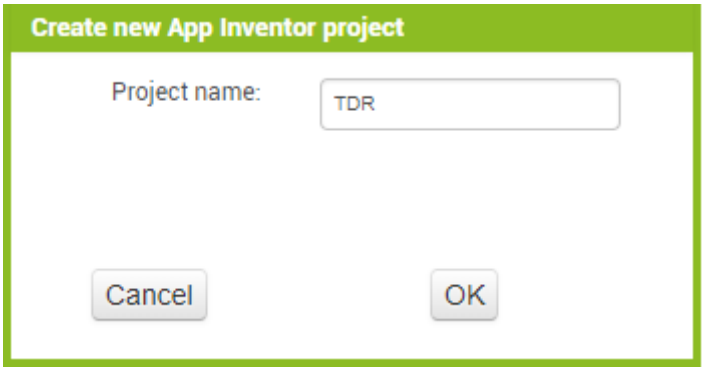

Fig 44. Nom del projecte d'aplicació

Ara, ja podrem començar a crear l'aplicació. El procés constarà de dos apartats: el disseny i la programació.

Encara que la programació sigui el més important, el disseny tampoc pot quedar-se enrere, ja que la impressió que causa a primera vista també és molt important.

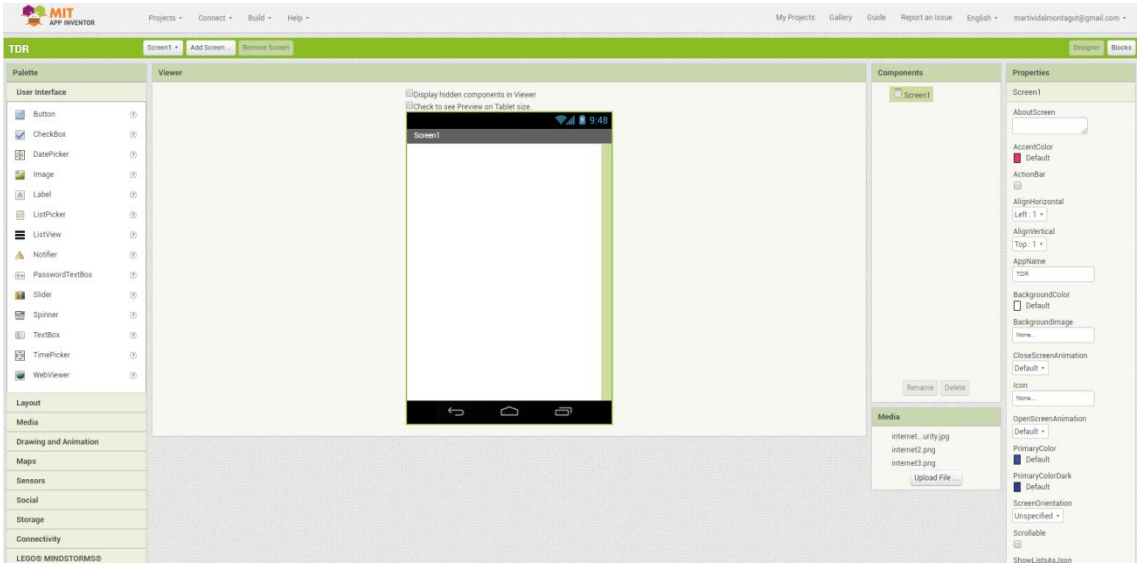

Fig 45. Pantalla de creació

L'aplicació tindrà diverses pantalles. La primera serà mostrada sempre en iniciar l'aplicació. Aquesta pantalla, mostrarà el logo que he creat per a l'aplicació durant 5 segons i després ens portarà a la pantalla d'inici de sessió, encara que si premem el logo, no ens haurem d'esperar, ens hi durà automàticament.

Per crear el logo, he utilitzat el programa d'edició d'imatge Macromedia Fireworks. El logo de l'aplicació serà un cercle dividit en dues seccions. En la secció superior hi haurà un candau amb colors suaus sobre un fons blau amb una mica de transparència, i en la inferior el títol "INS FLIX" amb una il·luminació taronja sobre un fons blau marí.

Fig 46. Disseny del logo

5.1.3.1 Primera pantalla

Disseny

Per crear aquesta pantalla, tornant a l'App Inventor, utilitzarem diverses eines. La primera que utilitzarem serà la "Canvas", l'utilitzarem com a fons, ja que ens permetrà moure el logo. Com ja he dit, posarem el logo amb l'eina "ImageSprite", la qual ens permetrà interactuar amb el logo.

Perquè puguem dur a terme la funció que al cap de 5 segons (si no es prem el logo) l'aplicació ens porti a la següent pantalla, haurem d'utilitzar l'eina "Clock" i li aplicarem un TimerInterval de 5000, el qual significarà 5 segons, ja que la unitat utilitzada són els mil·lisegons.

Fig 47. Elements utilitzats

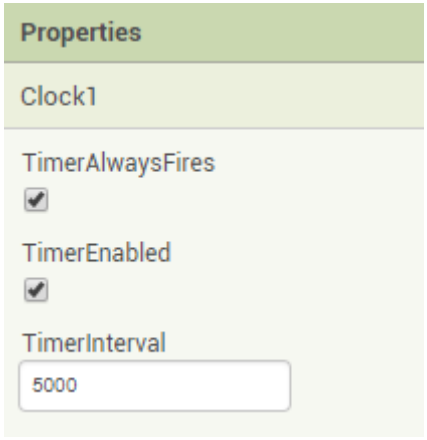

Fig 48. Informació sobre l'element Clock1

Per acabar aquesta pantalla, posarem a l'ImageSprite el logo fet anteriorment amb una amplada i alçada de 200x200 píxels.

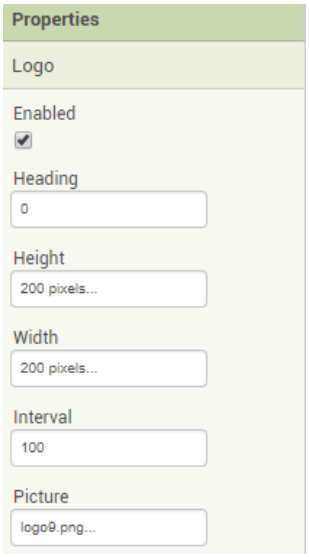

Fig 49. Informació sobre el logo

Fig 50. Resultats del disseny de la primera pantalla

Programació

Com que les eines utilitzades en aquesta pantalla han estat poques, conseqüentment la programació no serà gaire complicada.

Començarem amb la funció de "when Screen1 initialize do", la qual farà que en obrir l'aplicació, quan s'executi la primera pantalla (Screen1) farà el que li assignem.

Fig 51. Funció "when Screen1initialize do"

En aquest cas, li farem establir les coordenades del logo restant les dimensions totals de la pantalla amb el logo i dividint-les entre 2, de manera que el logo quedarà centrat. Per fer-ho, utilitzarem la funció "set to" dos cops, un per la coordenada X i un per la coordenada Y i ho aplicarem a la resta de l'amplada i l'alçada de la Screen1 amb el Logo.

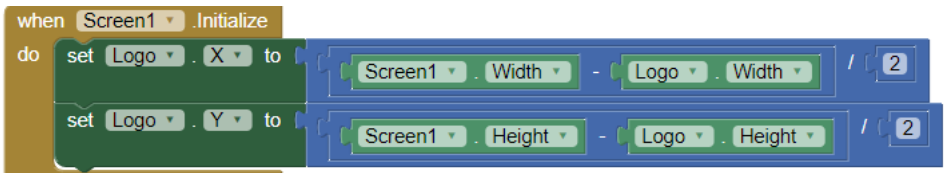

Fig 52. Funció final del "when Screen1 initialize do"

Ara, perquè puguem interactuar amb el logo, utilitzarem la funció de "when Canvas1 touched do", de manera que quan el premem ens porti a la següent pantalla. Per fer-ho, utilitzarem la funció "set Clock1 TimerEnabled to false", per apagar el Timer del rellotge i la de "open another screen screenName" per obrir la següent screen o pantalla.

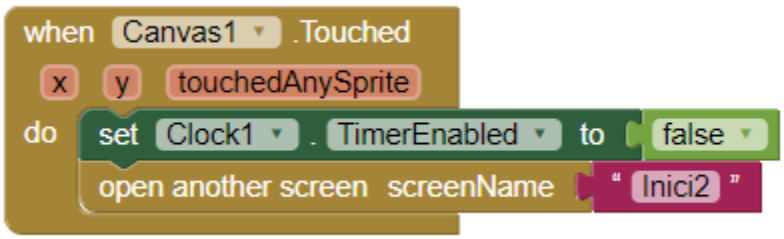

Fig 53. Funció "when Canvas1 touched do"

Per últim, utilitzarem la funció "when Clock1 Timer do", que ens permetrà fer l'acció que volem quan el temps que havíem assignat al rellotge passi.

En aquest cas serà apagar el rellotge i donar pas a la següent pantalla. Per fer-ho, utilitzarem les mateixes funcions que en el cas anterior.

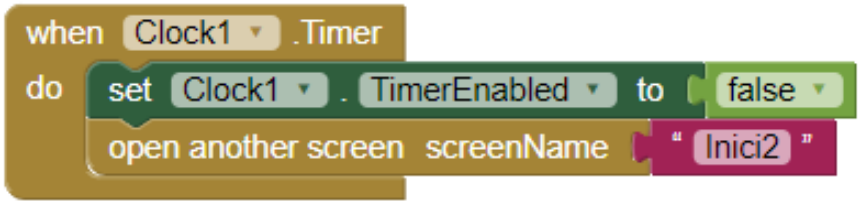

Fig 54. Funció "when Clock1 timer do"

5.1.3.2 Segona pantalla

Disseny

En aquest cas, haurem d'utilitzar més eines, ja que aquesta pantalla ens servirà per identificar-nos i, en cas que encara no tinguem compte, registrar-nos.

Aquesta screen o pantalla s'estructurarà en 3 parts, formades per elements "VerticalArrangement". La primera part serà un VerticalArrangement d'alçada 30%, en la qual posarem el logo de l'aplicació.

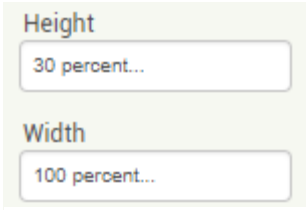

Fig 55. Informació del VerticalArrangement

Fig 56. Part superior de la pantalla

La segona, serà la pantalla d'inici de sessió o login, la qual estarà formada per un altre VerticalArrangement, però en aquest cas l'amplada no serà del 100%, sinó del 85%, per donar-li un millor efecte visual, i l'alçada serà del 75%.

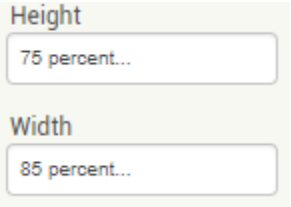

Fig 57. Informació del VerticalArrangement2

A la part superior hi haurà un text o Label en el que hi escriurem "Escriviu les vostres dades". A continuació, hi haurà un quadre de text o TextBox, un quadre de contrasenya o PasswordTextBox, un botó o Button el qual ens servirà per entrar a l'aplicació si la contrasenya és correcta, un quadre de confirmació o CheckBox que ens servirà per recordar les dades, un botó en el que hi apareixerà "No tens compte?" i que, en cas que no en tinguem, ens podrem registrar. Finalment, hi haurà dos botons "VeureTDB" i "EsborrarTDB" que serviran per veure les dades emmagatzemades a la base de dades i per esborrar-les, els quals serien eliminats si l'aplicació fos publicada, ja que sinó resultaria inútil emmagatzemar dades si qualsevol les pot veure o esborrar.

També, cal dir que tots els elements seran separats per un Canvas de 10 píxels d'alçada, per fer el disseny més còmode a la vista.

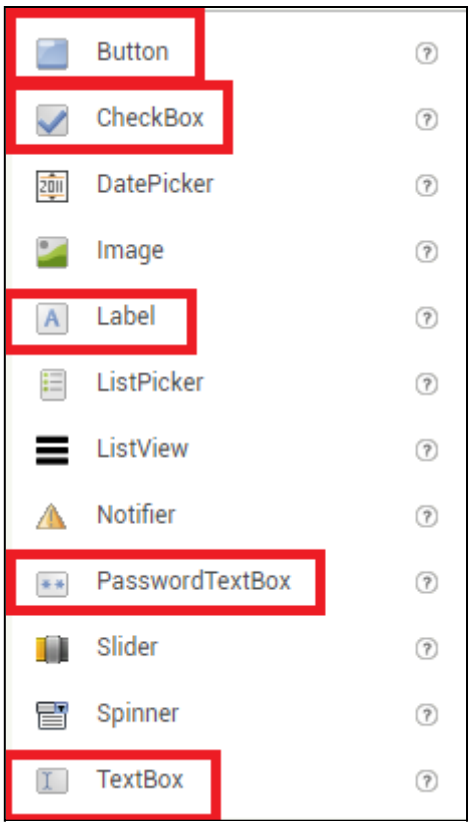

Fig 58. Elements utilitzats

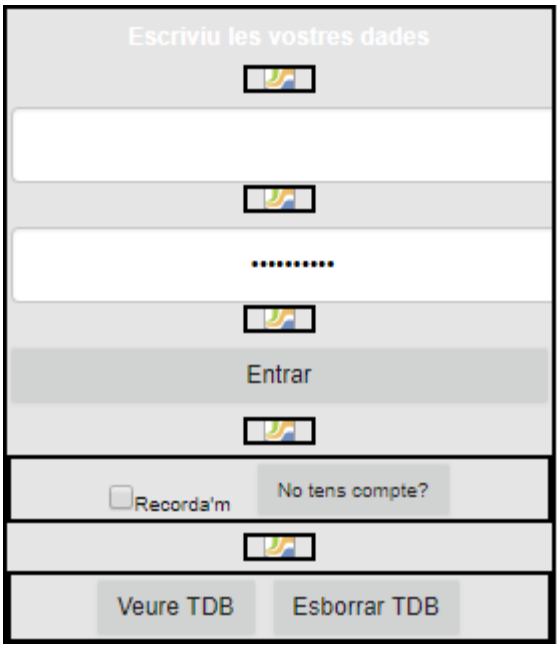

Fig 59. Pantalla d'inici de sessió

Per acabar, l'última part serà la del registre, la qual serà similar a l'anterior. Estarà formada per un Label de "Escriviu les vostres dades", dues TextBox per introduir els noms i cognoms i el nom d'usuari, una PasswordTextBox per introduir la contrasenya i dos botons, "Registrar" i "Cancel·lar". El primer servirà per continuar amb el registre i el segon per tornar a la pantalla anterior.

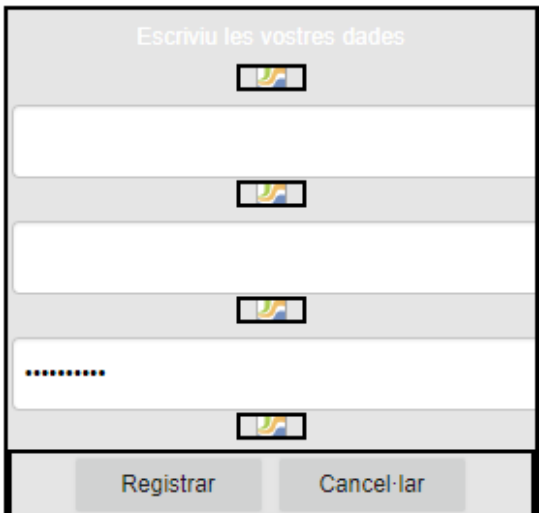

Fig 60. Pantalla de registre

Programació

En aquest cas, com que hem treballat amb més elements, la programació també serà més extensa i difícil.

Començarem establint colors, ja que considero que els predeterminats no són òptims. N'establirem 5: primari, secundari, dels botons, del text, i del text secundari.

Per fer-ho, utilitzarem la variable "initialize global to" i hi encaixarem la funció "make a list", dins de "make color".

Fig 61. Funció per establir el color

Dins aquesta funció hi hauran 3 ítems, en els quals haurem d'introduir el color del codi RGB, el qual l'obtindrem d'una pàgina web.

A continuació, seguirem el mateix procediment per la resta de colors.

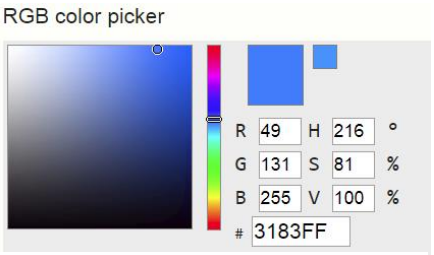

Fig 62. Seleccionador de colors

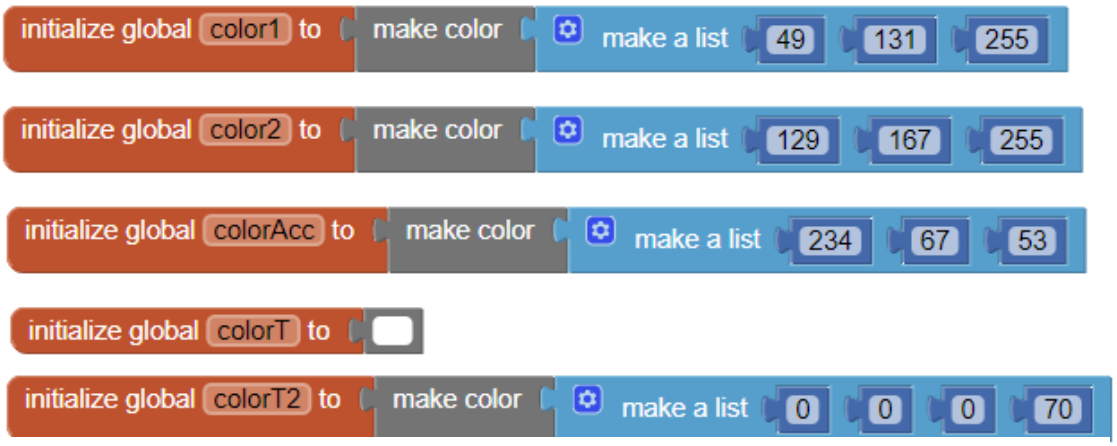

Fig 63. Colors establerts

Com que no volem que es mostrin a la mateixa Screen la pantalla d'inici de sessió i la de registre, establirem un procediment. Anomenarem l'estat "VALoginVisible" i hi posarem dos "set visible to get/not get estat", de manera que quan l'estat sigui positiu (true), el VA2, que és la pantalla d'inici de sessió serà visible, i quan sigui negatiu (false), la VA3, la pantalla de registre, serà visible.

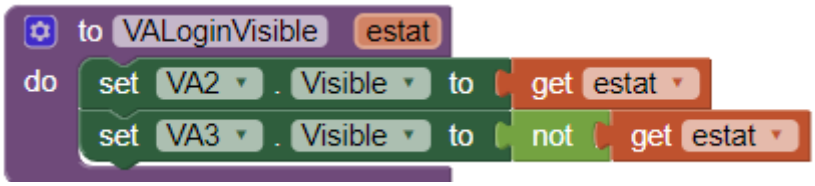

Fig 64. Procediment "VALoginVisible"

També establirem el procediment de "pintarScreen", en el qual posarem els diferents elements de la Screen dels colors que hem establert anteriorment. Per fer-ho, utilitzarem la funció "set BackgroundColor to get" diversos cops, variant segons l'element que vulguem pintar i el color que vulguem utilitzar.

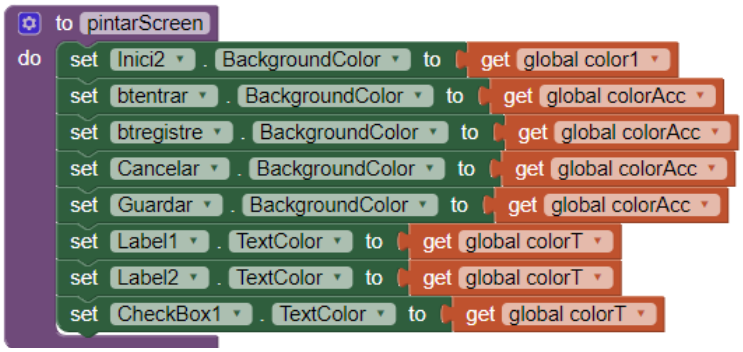

Fig 65. Procediment "pintarScreen"

Perquè en iniciar es compleixin aquests dos procediments, utilitzarem la funció de control "When initalize do", de manera que en iniciar la pantalla es faran automàticament. L'estat del primer procediment l'establirem com a positiu, ja que la pantalla que s'ha de mostrar és la d'inici de sessió.

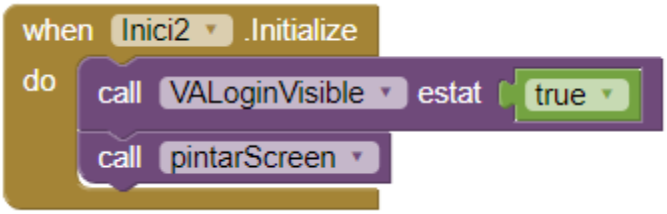

Fig 66. Funció "when Inici2 initialize do"

Un cop fet aquest pas, començarem establint la funció dels botons. Començarem amb la del botó de registre. Utilitzarem la funció "When click do", de manera que quan es faci clic es compleixi la funció. Dins d'aquesta, utilitzarem un "if then else if", ja que poden haver-hi dues opcions. La primera, si en fer clic l'usuari no està registrat, podrà accedir a la pantalla de registre, però si ja està registrat, apareixerà una notificació amb el text "Ja estàs registrat!" i es quedarà a la mateixa pantalla.

Per fer-ho, utilitzarem el procediment ja establert "VALoginVisible", però n'haurem d'establir tres de nous.

El primer l'anomenarem "mostrar", i la funció que farà serà mostrar la notificació que l'usuari ja està registrat. Per tant, utilitzarem un "call Notifier1 ShowAlert notice" i l'encaixarem amb el tag establert, anomenat "missatge".

Fig 67. Procediment "mostrar missatge"

El segon serà "JaRegistrat", i l'utilitzarem per poder detectar si l'usuari està registrat o no. Per fer-ho també utilitzarem un procediment "to do" i hi establirem un tag. Ho encaixarem amb un "call TinyDB1 GetValue tag" i un "get tag", el qual obtindrà la informació de la base de dades junt amb un "is empty", de manera que si no hi ha dades establertes i, per tant, no hi ha cap usuari registrat, ens deixarà accedir a la pantalla de registre.

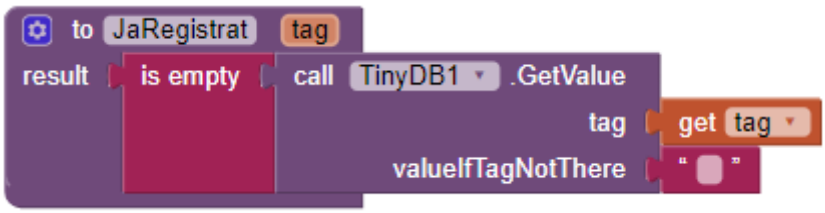

Fig 68. Procediment "JaRegistrat"

El tercer serà el "JaRegistrat2" i serà igual a l'anterior però sense el "is empty", de manera que si es detecta que ja hi ha informació a la base de dades, l'usuari ja s'ha registrat anteriorment i apareixerà el missatge que ja està registrat.

Un cop establerts aquests procediments, podrem completar la funció "if then else if then". A l'"if" hi encaixarem un "call JaRegistrat usuari . Text" i al then un "call VALoginVisible" estat "false", de manera que si l'usuari no està registrat la pantalla de Login desapareixerà i apareixerà la de registre. A l'else if hi encaixarem un call igual a l'anterior, però utilitzant el procediment "JaRegistrat2" i al then el procediment "mostrar missatge Ja estàs registrat!", de manera que si l'usuari ja està registrat, seguirà a la pantalla de Login i li apareixerà aquesta notificació.

Continuarem establint la funció del botó d'entrar. Utilitzarem també un "When click do", i dins hi encaixarem un "if then else", i dins d'aquest un "if then else if then else". En aquest cas, caldrà establir 4 nous procediments.

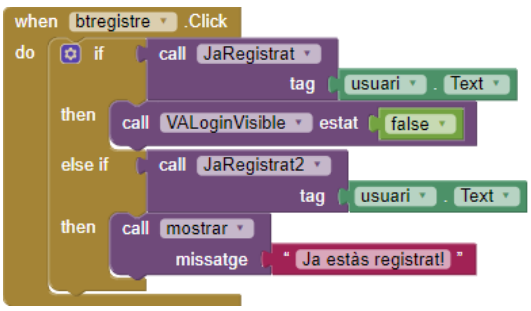

Fig 69. Funció "when btregistre click do"

El primer serà "cBuit2", que ens farà saber si la TextBox de l'usuari o a la PasswordTextBox de la contrasenya estan buits. És senzill, simplement utilitzarem el procediment "to result", hi encaixarem una funció lògica "or" i dins un "is empty usuari text" i un "is empty PasswordTextBox2 text", de manera que si qualsevol d'aquests dos camps està buit, es complirà el procediment.

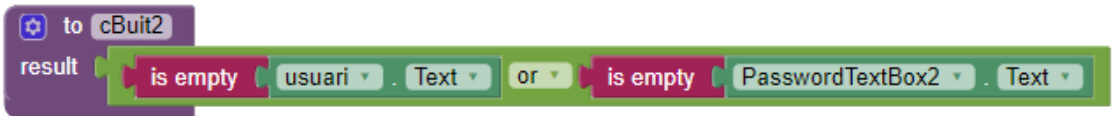

Fig 70. Procediment "cBuit2"

Tot seguit, establirem el següent procediment, el "UsuariNoExist", però és completament igual al "JaRegistrat", encara que en aquest cas verifica si l'usuari no existeix. Podríem haver utilitzat l'anterior, però crec que d'aquesta manera és més dinàmic.

El tercer procediment serà el "VerificarClau". Començarem amb un "to result" i dins hi posarem una funció lògica "=". Dins d'aquesta funció, hi posarem un "select item list index" amb un "call TinyDB1 GetValue tag" i hi encaixarem un "usuari Text" amb l'índex 3 i ho igualarem a "PasswordTextBox text", de manera que si l'ítem número 3 del registre, la contrasenya, coincideix amb el text que hem escrit a la PasswordTextBox de la pantalla d'inici de sessió, es verificarà que la contrasenya és correcta.

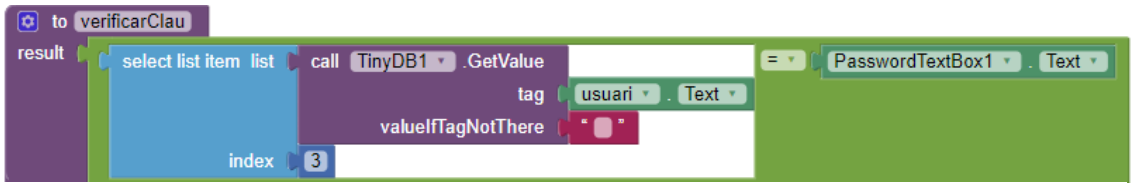

Fig 71. Procediment "verificarClau"

L'últim procediment serà el "obrirScreen". Simplement serà un "to do" amb la funció de "open another screen screenName", de manera que si es compleixen les condicions anteriors ens durà a la següent pantalla, anomenada "Selecciona".

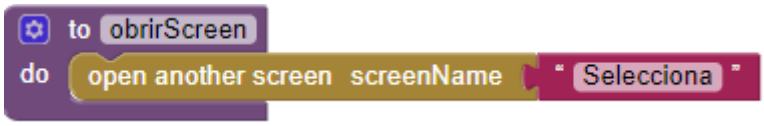

Fig 72. Procediment "obrirScreen"

Ara, cal completar la funció de "when click do", junt amb les encaixades. Al primer "if" utilitzarem el procediment "call cBuit2" i al "then" el "call mostrar missatge Dades incompletes!", de manera que si el camp de l'usuari o la contrasenya estan buits ens mostrarà una notificació dient que estan incomplets. Llavors, si això no passa, anirem a l'"else". Dins aquest, al primer "if" utilitzarem una funció lògica de "≠", en el que si el text introduït al camp de la contrasenya és diferent al de l'establert a la base de dades TinyDB, mitjançant el "call mostrar missatge" ens avisarà que les dades introduïdes són incorrectes.

Si aquest tampoc és el cas, passarem a l'"else if", en el qual amb el "call verificarClau" es comprovarà si la contrasenya és correcta. Si ho és, es continuarà amb el procediment "obrirScreen" i accedirem a la següent pantalla, però si la clau és incorrecta, passarem a un "call mostrar missatge" que ens dirà que no és correcta.

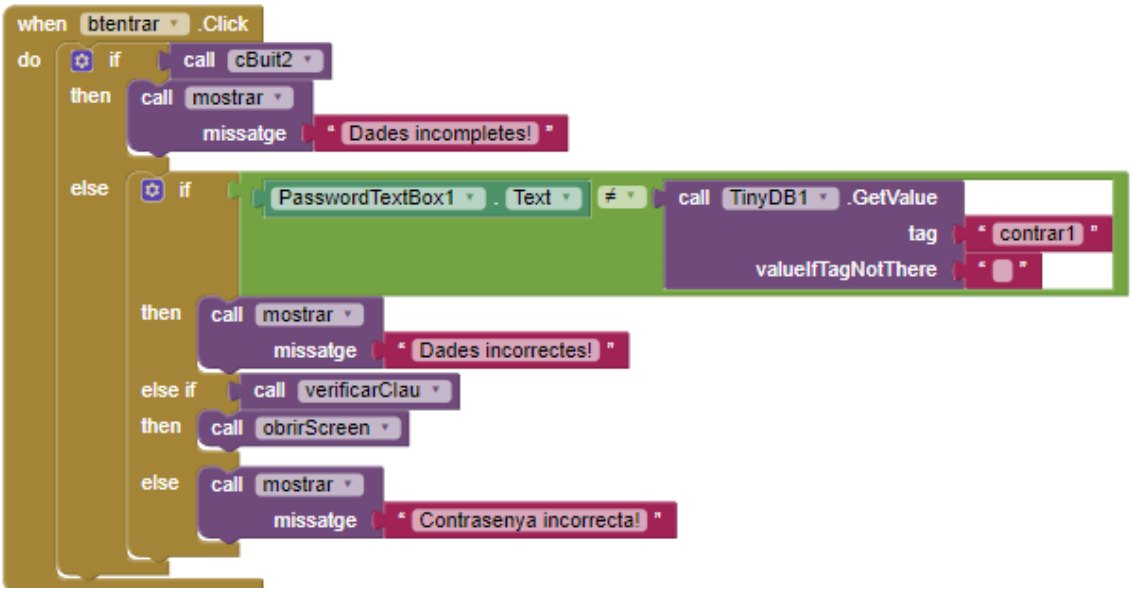

Fig 73. Funció "when btentrar click do"

Seguirem amb la funció dels botons "Cancel·lar" i "Guardar", de la pantalla de registre, al fer clic. En el primer cas, simplement establirem el "VALoginVisible" en estat true, de manera que tornarem a la pantalla d'inici de sessió.

Fig 74. Funció "when Cancelar click do"

Al botó de guardar, hi encaixarem una funció "if then else if then else". Començarem amb el primer if, en el qual utilitzarem el procediment "call cBuit". Si algun dels camps de registre, ja sigui el de nom i cognom, el d'usuari o el de contrasenya, està incomplet, ens mostrarà un missatge en el que ens avisarà que no està complet. Seguirem amb l'else if, en el qual utilitzarem el "call UsuariNoExist", encaixant-ho amb el tag "usuari . Text". Per tant, si el text escrit a la TextBox d'usuari no coincideix amb cap dels usuaris registrats, ens permetrà crear l'usuari. Si això es compleix, passarem al "then", on es farà el procediment "call crearUsuari", mostrarà un missatge que dirà que ens hem registrat amb èxit i posarà el "VALoginVisible" amb estat true, de manera que haurem registrat l'usuari a la base de dades i tornarem a la pantalla d'inici de sessió. Finalment, si el nom d'usuari introduït ja existeix, ens mostrarà un missatge reafirmant la seva existència.

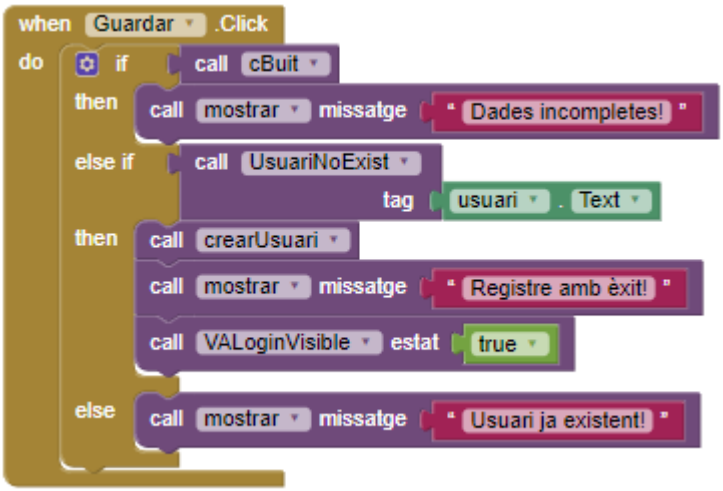

Fig 75. Funció "when Guardar click do"

Per acabar amb aquesta pantalla, passarem a la funció dels botons "Veure" i "Esborrar". Aquesta part seria esborrada si l'aplicació es distribuís al professorat, ja que qualsevol persona podria veure i esborrar les dades. Per tant, només existirà dins aquest procés didàctic.

Respecte el botó "Veure", començarem amb el procés "when click do", en el que hi establirem un "call ShowMessageDialog message title buttonText", el qual ens mostrarà un quadre de diàleg en el que podrem veure els tags emmagatzemats a la base de dades, juntament amb el títol de "Dades emmagatzemades" i un botó per acceptar.

Respecte el d'esborrar, simplement hi encaixarem el procediment "call TinyDB1 ClearAll", el qual esborrarà totes les dades existents a la base de dades TinyDb.

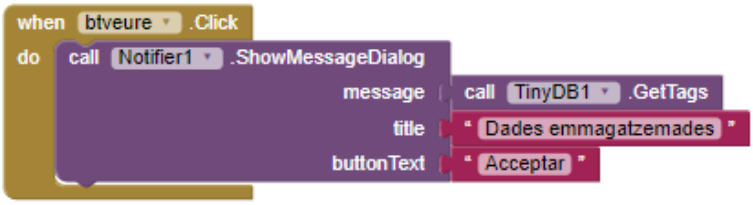

Fig 76. Funció "when btveure click do"

Fig 77. Funció "when btesborrar click do"

5.1.3.3 Tercera pantalla

Disseny

Aquesta pantalla estarà formada per 5 elements principals, encara que hi haurà força elements decoratius i que ajudaran a fer el disseny més còmode.

Començarem establint un color de fons adient, que no sigui gaire viu i que sigui còmode de veure. Serà un blau de color clar, amb el codi #89b2ffff.

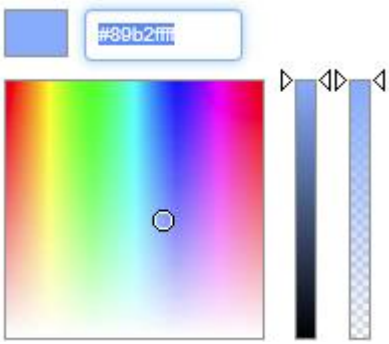

Fig 78. Seleccionador de colors

A la part superior de la pantalla, hi posarem un canvas sense color amb una alçada de 10 píxels, perquè els elements que posem no estiguin situats a dalt de tot. Tot seguit, posarem un VerticalArrangement d'una alçada de 15% i una amplada de tota la pantalla, on hi introduirem una imatge amb alçada de 100 píxels, que serà el logo de l'aplicació. Per acabar aquesta part, posarem un altre canvas de 10 píxels d'alçada, per separar lleugerament el logo de l'element següent. Encara que a l'editor l'imatge es vegi tallada, a l'aplicació es veu correctament.

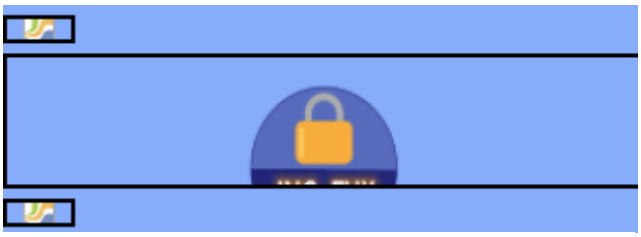

Fig 79. Part superior de la pantalla

A continuació, establirem 5 elements, que seran llocs web dels quals podrem guardar les contrasenyes i als quals podrem accedir, el Gmail, el correu XTEC, el Clickedu, el Moodle Àgora de l'institut de Flix i un apartat de miscel·lània, on l'usuari podrà triar quines altres contrasenyes guarda de manera personalitzada.

Continuarem establint 5 HorizontalArrangement de 10 i píxels d'alçada i tota la pantalla d'amplada, que actuaran com a divisors. És a dir, el primer i l'últim seran de 10 i el segon, el tercer i el quart seran de 5. Entre cada divisor hi haurà altres HorizontalArrangement, els quals estaran formats per un VerticalArrangement de 50 píxels d'amplada amb la imatge corresponent dins, dos canvas de 10 píxels d'amplada que separaran el Label (el títol del lloc web) de l'element anterior i el botó d'accedir, de color vermell i amb una alçada i alçada que completen l'element.

Entre cada element i cada divisor hi haurà un canvas un de 10 píxels d'alçada incolor que els separarà, excepte amb l'últim cas.

Aquest últim, el de miscel·lània, també tindrà un color de fons diferent, un blau de diferent gamma, ja que el considero aliè als elements anteriors, encara que el disseny serà exacte a aquests excepte en el cas de la imatge i el color.

El tipus de lletra establert és sans serif, el tamany és 16 i està en negreta.

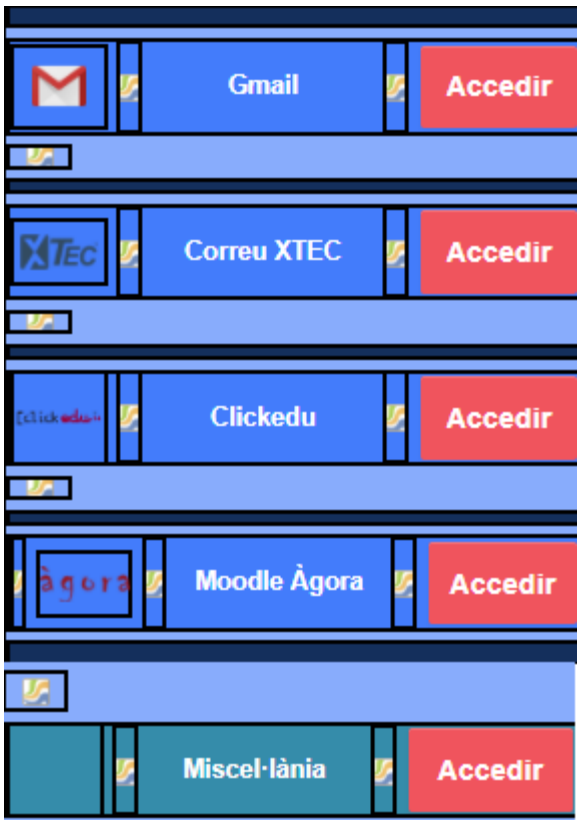

Fig 80. Part inferior de la pantalla

Programació

En aquest cas, encara que el disseny ha estat extens, la programació és força senzilla. Simplement, haurem d'establir les funcions dels botons d'accedir.

Només haurem d'encaixar les funcions "when click do" amb un "open another screen screenName", de manera que en tindrem 5 establertes. Quan fem clic a accedir, ens durà a un dels criptogrames dissenyats.

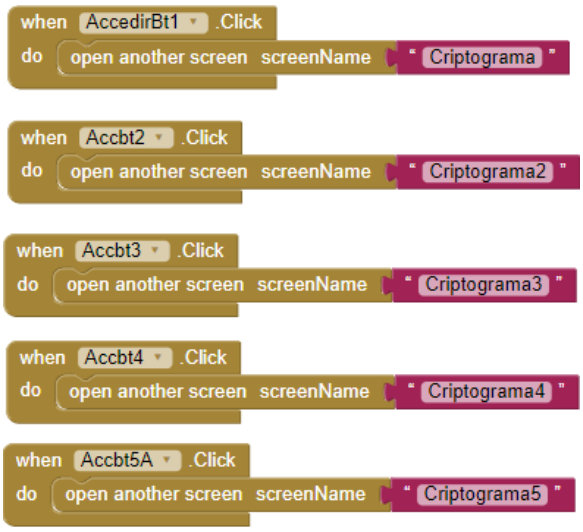

Fig 81. Funció dels botons "when click do"

5.1.3.4 Quarta pantalla

Disseny

El disseny utilitzat en aquesta pantalla serà molt semblant al de la pantalla anterior, però en aquest cas, en ser elements modificables, hi haurà alguns canvis.

El color de fons serà el mateix i la part superior també, però en la part dels HorizontalArrangement que contenen el títol del lloc web, en canvi, el VerticalArrangement que contenia la imatge estarà buit i el Label el reemplaçarem per una TextBox de color blau. En aquest cas també hi haurà dos botons, “Guardar” i “Esborrar”, de color vermell amb el text blanc, dividits entre dos HorizontalArrangement de 5 i 10 píxels d’alçada.

En aquest cas, els HorizontalArrangement divisors també són de 5 i 10 píxels. El primer i l’últim són de 10, mentre que els del mig són de 5.

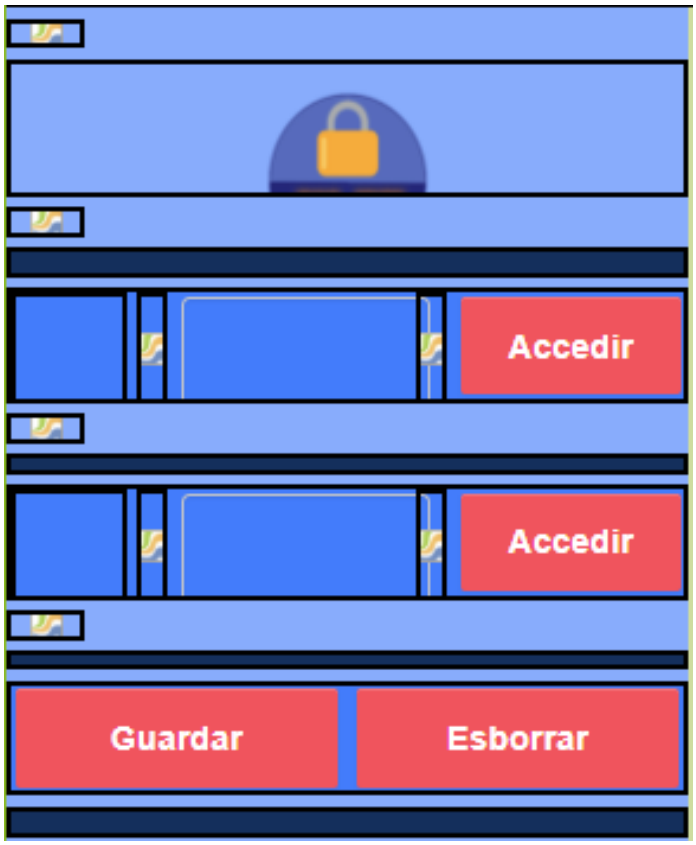

Fig 82. Disseny de la quarta pantalla

Programació

Encara que aquesta pantalla és gairebé igual a l’anterior en el disseny, canvia molt a l’hora de programar, ja que els títols són modificables i s’han d’emmagatzemar en una base de dades TinyDB.

Començarem establint la funció del botó “Guardar”. Utilitzarem la funció “when click do” i hi encaixarem dos “call TinyDB1 StoreValue tag valueToStore”. El primer tag l’anomenarem com “altres1” i el segon com “altres2”. La informació emmagatzemada en aquests tags serà el text que hi hagi escrit a les respectives TextBox.

Seguirem amb la funció del botó “Esborrar”. Seguirem el mateix procediment que amb l’altre botó, però a “valueToStore” hi posarem un text buit, de manera que s’esborraran les dades emmagatzemades.

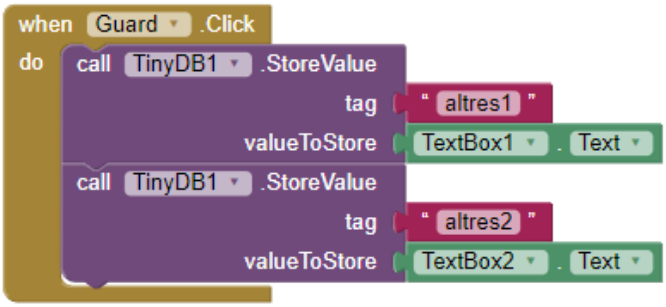

Fig 83. Funció “when Guard click do”

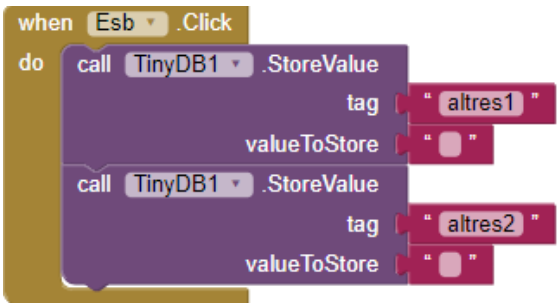

Fig 84. Funció “when Esb click do”

Un cop establertes aquestes funcions, perquè les dades emmagatzemades siguin recuperades un cop s’iniciï la pantalla, establirem la funció “when Initialize do”, en la qual hi encaixarem dos “set TextBox Text to call TinyDB Get Value tag if tag notThere”, de manera que si hi ha dades emmagatzemades, el text de la TextBox1 serà allò emmagatzemat al tag “altres1” i el de la TextBox2 serà el del tag “altres2”, mentre que si no n’hi ha, la TextBox corresponent estarà buida.

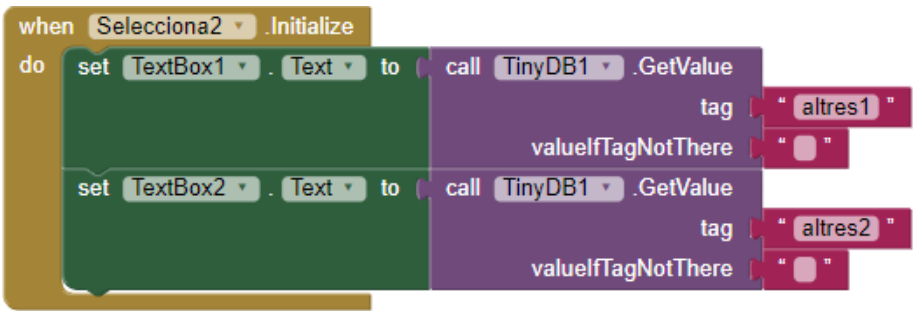

Fig 85. Funció “when Selecciona2 Initialize do”

Finalment, acabarem amb les funcions dels botons d’accedir. En aquest cas, el procediment serà el mateix que en la pantalla anterior.

Utilitzarem la funció “when click do” juntament amb la “open another screen ScreenName”, però en aquest cas no ens portarà a un criptograma perquè ja l’haurem passat, sinó a l’apartat de contrasenyes emmagatzemades.

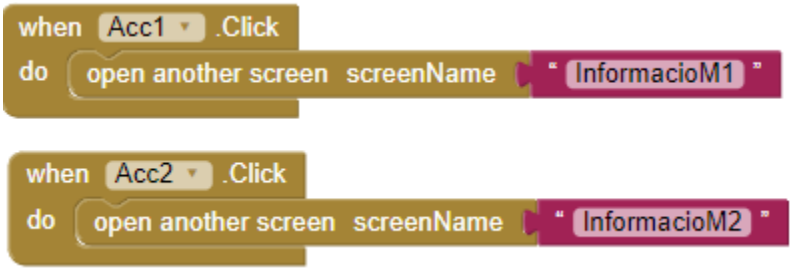

Fig 86. Funció "when click do" dels botons d'accés

5.1.3.5 Criptogrames

Encara que són diferents pantalles, com que l'únic que canvia és el text del criptograma, ho posaré en conjunt.

Disseny

Com a les altres pantalles, la part superior estarà formada per un VerticalArrangement d'una alçada del 15% amb el logo de l'aplicació a l'interior, d'una alçada de 100 píxels. Seguirem amb un HorizontalArrangement divisor d'una alçada de 10 píxels i uns altres dos HorizontalArrangement. Però, aquests seran de 50x200 píxels i contrindan un Label, que serà el criptograma, amb el text de color blanc, en negreta, tamany 20 i tipus de lletra sans serif, els quals estaran separats per un altre HorizontalArrangement sense color de 5 píxels d'alçada, acabant amb un altre divisor de 10 píxels d'alçada.

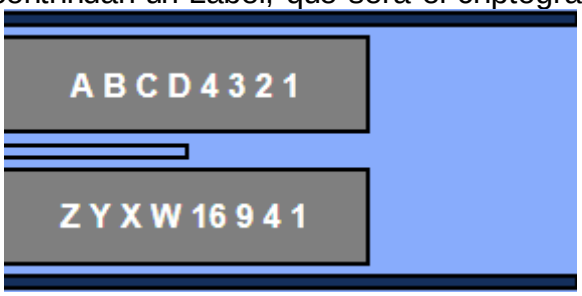

Fig 87. Part central del primer criptograma

Tot seguit, posarem un canvas incolor de 5 píxels d'alçada i un HorizontalArrangement de 30x70 píxels de fons negre amb un label que contindrà la clau del criptograma, amb un tamany de lletra de 16, sans serif i de color blanc, precedint un altre HorizontalArrangement d'una alçada de 5 píxels sense color.

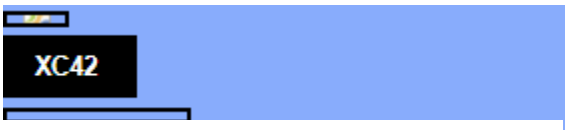

Fig 88. Codi del primer criptograma

Després, col·locarem un HorizontalArrangement d'una alçada de 50 píxels i amb amplada completa, on hi situarem una PasswordTextBox i un botó d'accedir, separats per un HorizontalArrangement de 5 píxels d'amplada. El fons serà blau i el del botó d'accedir vermell. A continuació, posarem un altre divisor de 5 píxels d'altura i un altre HorizontalArrangement, de 50 píxels

d'alçada, el qual contindrà dues TextBox de 25x25 píxels, separades per un canvas de 5 píxels.

Finalment, posarem dos botons sense color amb un tamany de 25x25 píxels dins un HorizontalArrangement, també incolor, els quals revelaran la clau del criptograma.

Fig 89. Part inferior del primer criptograma

Encara que el procediment és exactament igual en totes les pantalles de criptograma, els Label són diferents i, per tant, la clau del criptograma també.

Per tant, encara que no torni a explicar el procediment, adjuntarem els diferents criptogrames.

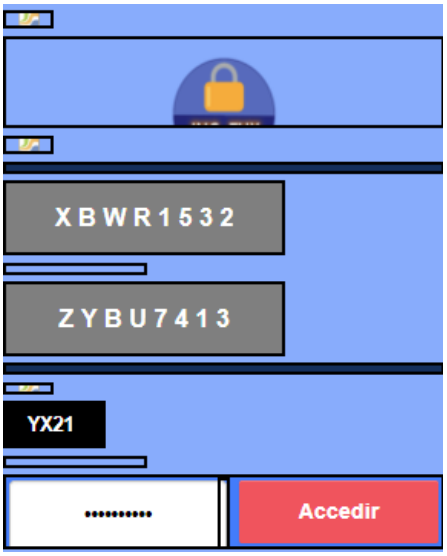

Fig 90. Segon criptograma

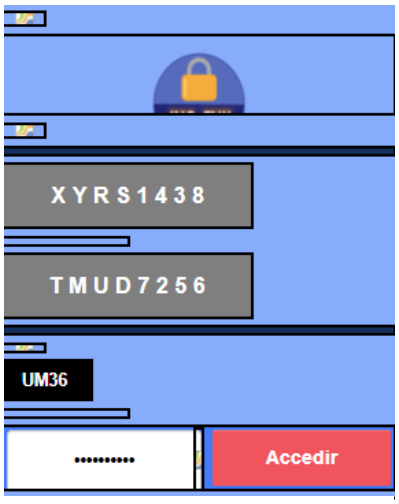

Fig 91. Tercer criptograma

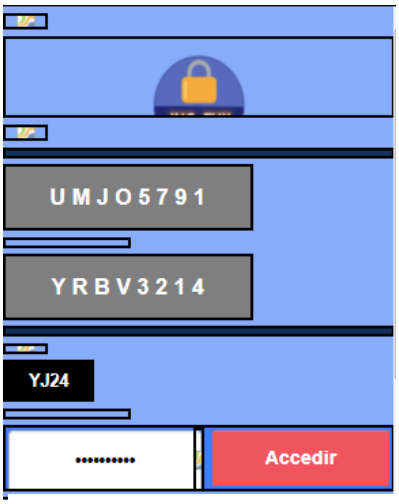

Fig 92. Quart criptograma

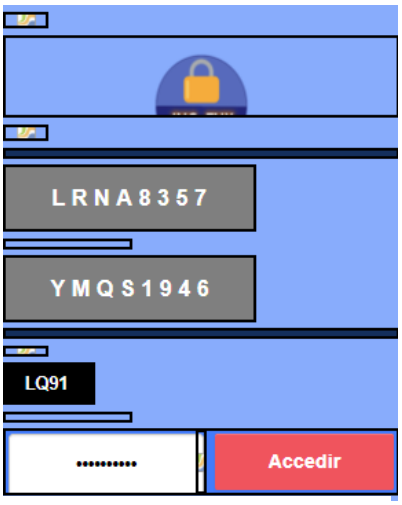

Fig 93. Cinquè criptograma

Programació

Igual que en el disseny, la programació dels diferents criptogrames és pràcticament igual, ja que només canvien els noms. Ara bé, la programació dels criptogrames és molt simple i breu.

Començarem establint la funció del botó d'accedir. Utilitzarem un "when click do", encaixant-hi una funció "if then else". A l'"if" utilitzarem la funció lògica "=", en la qual igualarem el text de la PasswordTextBox amb la clau del criptograma, la qual dependrà segons aquest. Si coincideix, passarem al then, on hi haurà un "open another screen screenName", i accedirem a la pantalla on tindrem la contrasenya guardada. Si la contrasenya és incorrecta, passarem a l'"else" on, com a mesura de seguretat, es tancarà l'aplicació mitjançant la funció "close application".

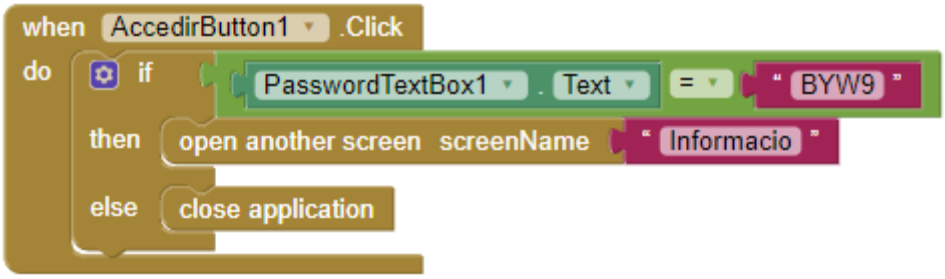

Fig 94. Funció "when AccedirButton1 click do"

Per continuar, establirem la funció dels dos botons ocults, els quals ens proporcionaran el mètode per desxifrar la contrasenya. Per exemple, si ens diuen "-" i "1", significarà que haurem de seleccionar en sentit negatiu un caràcter cap a l'esquerra en diagonal. Utilitzaré com a exemple el primer criptograma, en el qual ens diu "YX21" i la clau és "-" i "1", per tant, la contrasenya serà "BYW9".

La funció dels botons l'establirem amb un "when longclick do", de manera que si es clica accidentalment no s'accionaran, es necessita un clic llarg. Dins, hi encaixarem un "set TextBox text to", de manera que la clau s'assignarà a les respectives TextBox.

Fig 95. Funció dels botons ocults

Com ja he dit anteriorment, la programació dels altres criptogrames serà igual, però canviant la contrasenya i la clau de desxiframent.

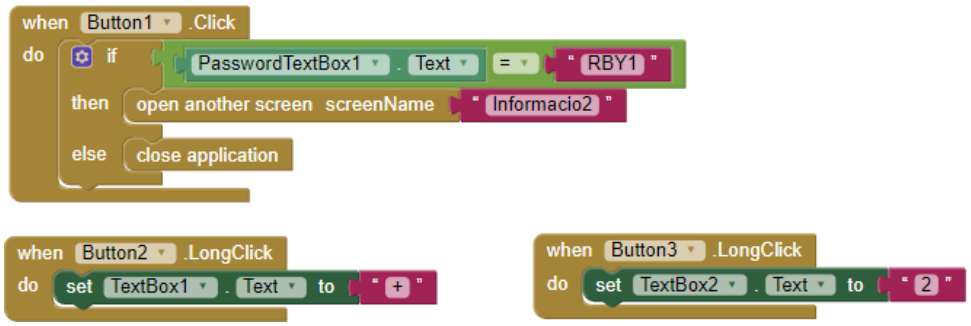

Fig 96. Programació del segon criptograma

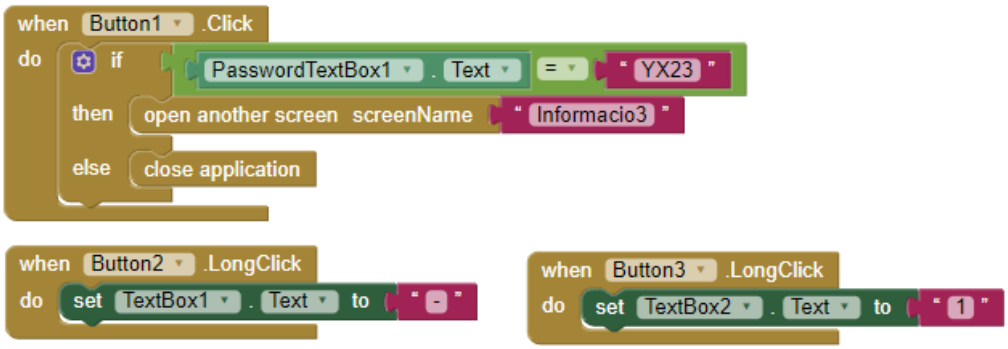

Fig 97. Programació del tercer criptograma

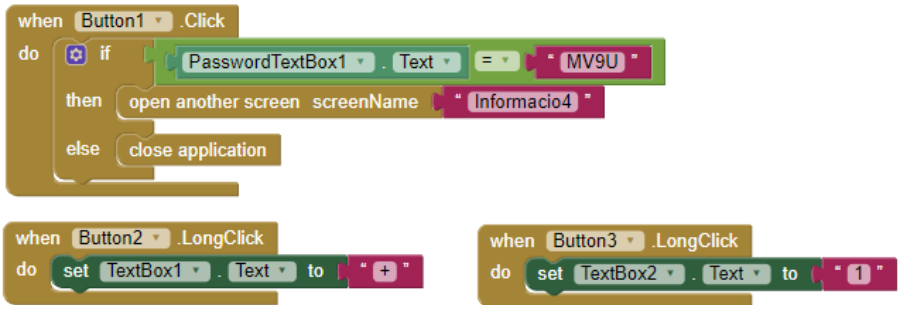

Fig 98. Programació del quart criptograma

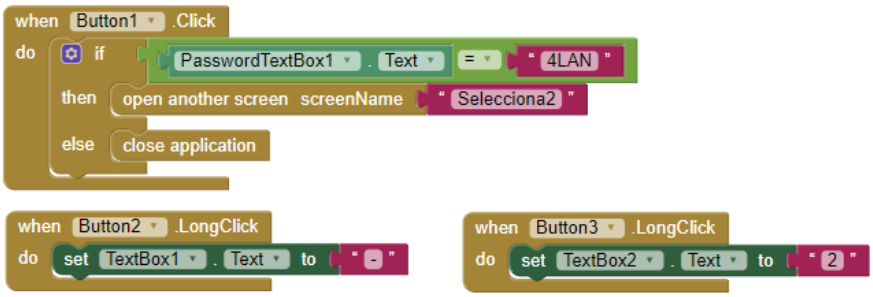

Fig 99. Programació del cinquè criptograma

5.1.3.6 Pantalla d'emmagatzematge d'usuari i contrasenya

Com en el cas dels criptogrames, també hi ha diverses pantalles d'emmagatzematge de les dades, però les descriuré de manera general ja que són pràcticament iguals, encara que dues d'elles, les respectives als llocs web modificables, canvien una mica.

Disseny

Com a les altres pantalles, la part superior estarà formada per un VerticalArrangement d'un 15% d'altura amb el logo de l'aplicació dins, de 100 píxels d'altura. Estarà envoltat per dos canvas de 10 píxels d'altura i a continuació, col·locarem un HorizontalArrangement de 50 píxels d'altura. Aquest, estarà format per un Label amb tamany de lletra 28, tipus de lletra sans serif i de color blanc, i el logo del lloc web, també envoltats de dos canvas als laterals per centrar aquests elements, a part dels divisors HorizontalArrangement de 10 píxels.

Fig 100. Part central de la pantalla d'emmagatzematge de dades del Gmail

En el cas de les dades dels llocs web modificables, aquest Label serà una TextBox que correspondrà al nom del lloc web assignat.

A continuació, posarem un altre canvas de 10 píxels i dos HorizontalArrangement de 40 píxels d'alçada, els quals contindran un Label d'usuari i contrasenya i una TextBox on podrem emmagatzemar les nostres dades. Cal dir que aquests HorizontalArrangement estan separats per un divisor i dos canvas de 5 píxels d'alçada.

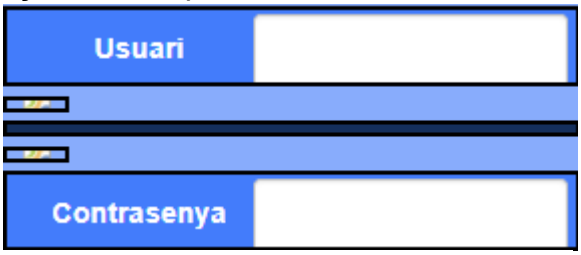

Fig 101. Part inferior de la pantalla d'emmagatzematge de dades

Finalment, després d'un altre canvas de 10 píxels d'alçada, posarem tres botons, "Guardar", "Accedir" i "Esborrar", dins un HorizontalArrangement de 40 píxels d'alçada, encara que en els altres dos casos excepcionals només hi haurà el botó "Guardar" i "Esborrar.

Fig 102. Botons dels llocs web preestablerts

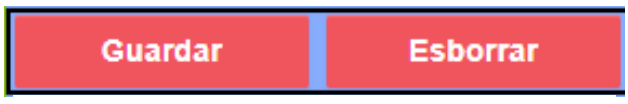

Fig 103. Botons dels llocs web modificables

Programació

Començarem programant el primer cas, la pantalla d'informació dels llocs web ja establerts.

Com a inici, utilitzarem la funció "when initialize do", encaixant-hi dos "set TextBox Text to call TinyDB GetValue tag valueIfTagNotThere". En el cas del Gmail, els tags serien "usuariGMDB" i "contrasenyaGMDB", en els altres seria el mateix, però canviant aquest "GM" pel nom corresponent.

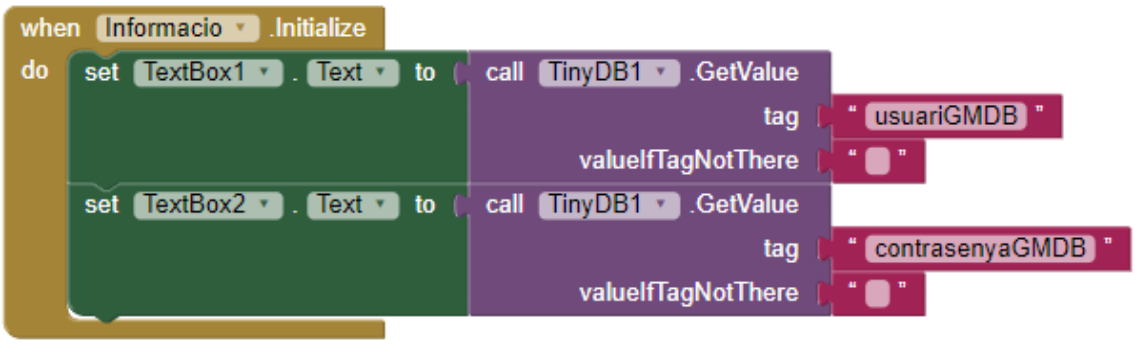

Fig 104. Funció "when Informacio intialize do" dels llocs web preestablerts

Continuarem establint la funció dels botons. Per establir la del botó d'esborrar, farem ús de la funció "when click do" i hi encaixarem dos "call TinyDB StoreValue tag valueToStore" amb els tags anteriorment citats i un text buit, de manera que quan cliquem aquest botó les dades emmagatzemades en aquests tags s'esborrin.

Pel botó d'accedir, simplement utilitzarem la funció "when click do" amb la "open another screen screenName", de manera que quan hi cliquem ens durà a la següent pantalla.

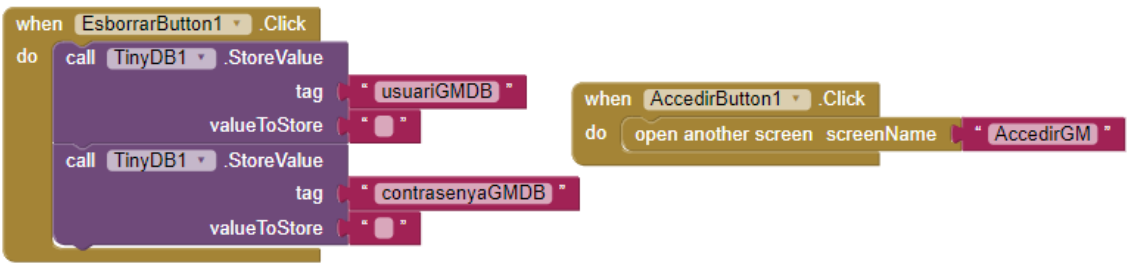

Fig 105. Funció dels botons dels llocs web preestablerts

Finalment, establirem la funció del botor de guardar, amb un "when click do", encaixant-hi dos "call TinyDB StoreValue tag valueToStore". El primer tag correspondrà al d'usuari que hem establert anteriorment i s'emmagatzemarà el text escrit a la TextBox1. El segon, correspondrà al de la contrasenya, i s'emmagatzemarà el text escrit a la TextBox2.

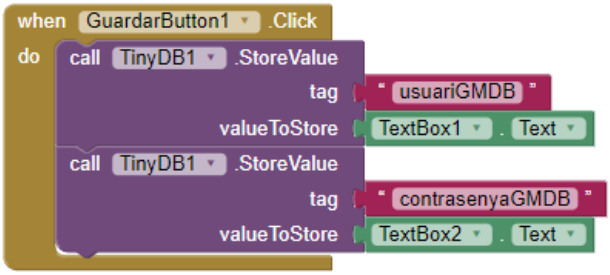

Fig 106. Funció del botó de guardar

Respecte les dues pantalles d'usuari i contrasenya que són diferents, l'única diferència a l'hora de programar és que a la primera funció, a la de "when initialize do" hi afegirem el valor establert en la segona pantalla, mitjançant un "set TextBox Text to call TinyDB GetValue tag valueIfTagNotThere", en el qual el tag serà el prèviament establert, "altres1".

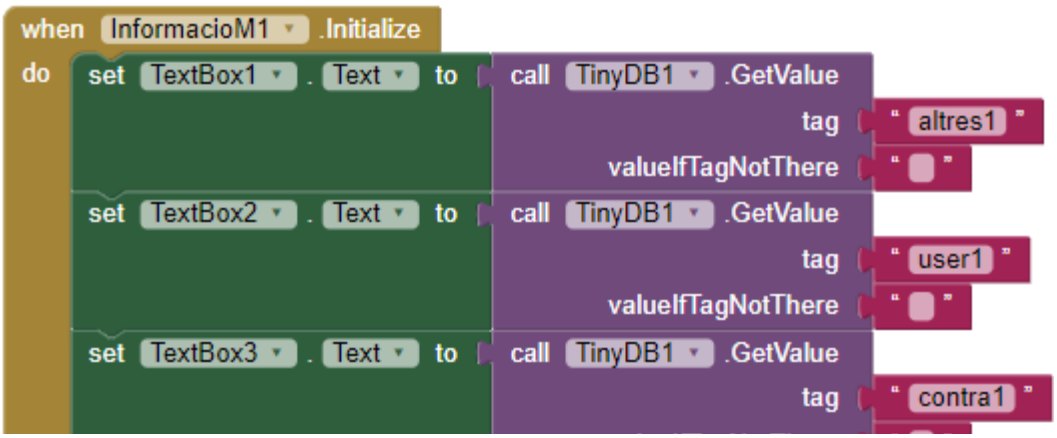

Fig 107. Funció "when initialize do" dels llocs web modificables

5.1.3.7 Pantalles d'accés als llocs web

En aquest cas, el disseny simplement serà un element WebViewer i no hi haurà programació.

Per exemple, en el cas del Gmail, afegirem un WebViewer i establirem com a HomeUrl l'enllaç d'inici de sesió de Gmail, de manera que des de la pròpia aplicació podrem accedir-hi.

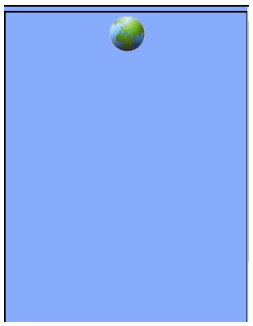

Fig 108. Disseny de la pantalla d'accés

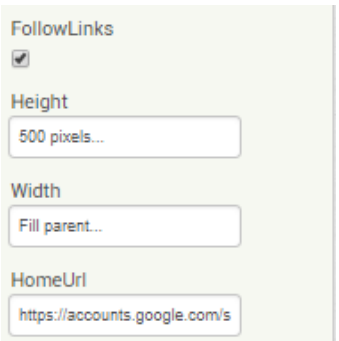

Fig 109. Informació de l'element WebViewer

5.1.4 SEGUIMENT DELS RESULTATS

Per observar el resultat final i comprovar que tot funciona correctament, utilitzarem l'aplicació en un dispositiu Android.

Per fer-ho, haurem de descarregar l'aplicació mitjançant un lector de codis QR per poder accedir des d'aquest codi, prèviament creat a la pàgina web http://es.qr-code-generator.com, a l'enllaç de descàrrega automàtica.

Un cop descarregada l'aplicació, haurem d'instal·lar-la.

Fig 110. Codi QR de l'aplicació

Acte seguit, ja podrem començar a provar la funcionalitat de l'aplicació.

Podrem observar com a la primera pantalla, si no premem el logo de l'aplicació, al cap de 5 segons ens durà automàticament a la pantalla d'inici. Un cop allí, si no tenim compte, clicarem al botó "No tens compte?" per registrar-nos. Escriurem les dades necessàries i procedirem amb el registre.

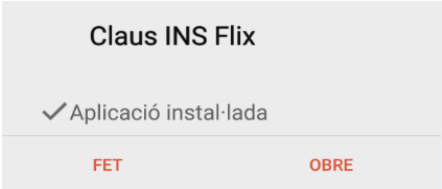

Fig 111. Instal·lació de l'aplicació

Fig 112. Primera pantalla

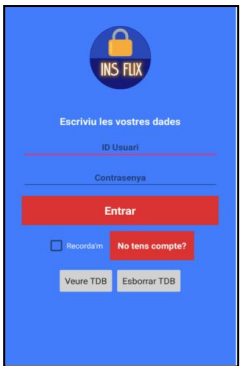

Fig 113. Pantalla d'inici de sessió

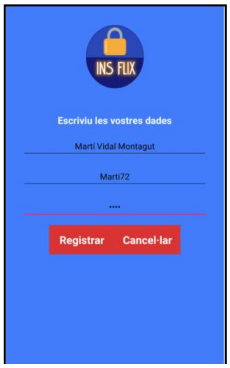

Fig 114. Pantalla de registre

Quan ja ens haguem registrat, ja podrem accedir al nostre compte per emmagatzemar les contrasenyes que vulguem.

A continuació, accedirem al menú, on haurem de comprovar que tots els apartats estiguin correctes, tant en tema de disseny com de programació.

Fig 115. Inici de sessió

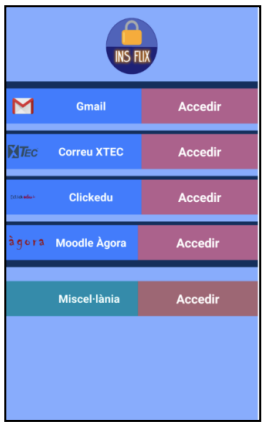

Fig 116. Menú de llocs web

Començarem pel primer, pel de Gmail, accedint al seu criptograma fent clic al botó "Accedir".

Premerem els botons ocults i veurem com apareix un "-" i un "1" i, per tant, si el codi és XC42, la contrasenya serà BYW9. Com que la contrasenya és correcta, ja podrem emmagatzemar les nostres dades i guardar-les. Podrem comprovar com si sortim de la pantalla i hi tornem accedir, les dades seguiran guardades.

També, mitjançant el botó accedir, podrem iniciar sessió a Gmail directament.

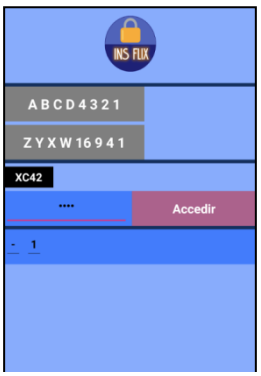

Fig 117. Primer criptograma

Fig 118. Dades Gmail

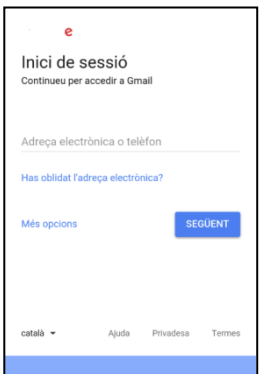

Fig 119. Accés a Gmail des de l'aplicació

Seguirem amb l'opció del correu XTEC, on la clau serà "+" i "2" i el codi YX21, per tant, la contrasenya serà RBY1. També podria considerar-se RBYX perquè hi ha dos números 1, però també forma part del criptograma que si hi ha dos nombres iguals, sempre s'agafa el de dalt.

Un cop allí, farem el mateix procediment de guardar les dades i comprovar el funcionament de l'accés a la pàgina web.

Fig 120. Segon criptograma

Fig 121. Dades XTEC

Fig 122. Accés a XTEC des de l'aplicació

Continuarem amb el Clickedu, on "-" i "1" serà la clau i el codi UM36, per tant, la contrasenya serà YX23. Un cop emmagatzemades les nostres dades, comprovarem l'accés a la pàgina web.

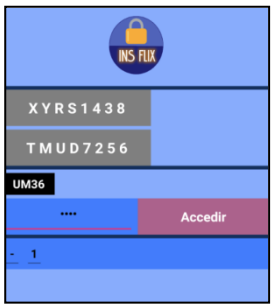

Fig 123. Tercer criptograma

Fig 124. Dades XTEC

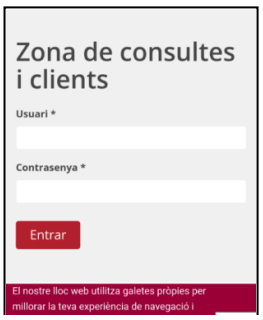

Fig 125. Accés a Clickedu des de l'aplicació

A continuació, passarem a l'últim cas del lloc web preestablert, el Moodle Àgora de l'INS Flix. La clau serà "+" i "1" i el codi YJ24, per tant, la contrasenya serà MV9U. Un cop guardades les dades, accedirem al lloc web.

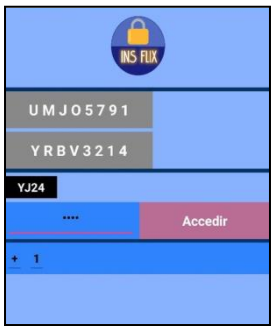

Fig 126. Quart criptograma

Fig 127. Dades Moodle Àgora

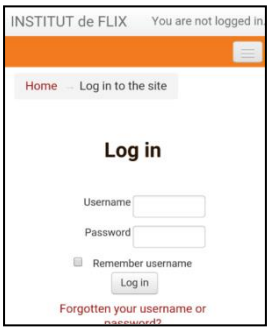

Fig 128. Accés al Moodle Àgora des de l'aplicació

Finalment, passarem a l'apartat de miscel·lània, on hi haurà 2 apartats modificables. Haurem de superar un altre criptograma, on el codi serà LQ91 i la clau "-" i "2", per tant, la contrasenya serà 4LAN.

En aquest menú, els camps dels llocs web els haurem d'escriure nosaltres. Posaré com a exemple Facebook i Instagram. Un cop haguem clicat el botó "Guardar", hi accedirem i podrem veure com el nom que hem escrit prèviament apareix a la pantalla d'emmagatzematge de dades.

Fig 129. Menú de llocs web modificables

Fig 130. Primera pantalla de lloc web modificable

Fig 131. Segona pantalla de lloc web modificable

6. CONCLUSIONS

D'aquest treball es desprèn que la seguretat informàtica i el hacking, encara que semblin conceptes antònims, van molt lligats. Primerament, hem de recordar que hi ha diferències entre un hacker i un cracker, ja que el concepte de cracker es limita a la informàtica i té intencions il·lícites, mentre que un hacker és aquell que resol un problema de qualsevol àmbit i pot fer-ho amb bona o mala intenció.

Encara que és un món molt recent (la seva existència va començar amb els Autèntics Programadors als anys 80 del segle XX), el creixement que ha sofert durant l'última dècada ha estat abismal i suposo que així seguirà, a mesura que la tecnologia també avanci. Cada cop les potències digitals tenen més impacte a les guerres entre països, sobretot en els països asiàtics, on es disposa de centenars de hackers qualificats per protegir el país i atacar l'enemic respecte a informació o sistemes digitals.

També, he après a classificar tots els tipus de malware, quina funció fan, d'on provenen i com ens en podem protegir. És molt important saber-ho, encara que no tinguem coneixements de seguretat informàtica, ja que podem prevenir moltes infeccions o, per exemple, en el cas d'un ransomware, ser conscients que és un simple malware i que no hem de pagar diners perquè la policia ens ha descobert veient pornografia.

Respecte a la criptografia, cada cop la trobo més interessant i enigmàtica, però els models que s'utilitzen a l'actualitat són massa complexos d'entendre sense tenir un coneixement previ sobre aquests.

El que més m'agrada sobre l'aplicació creada és la utilitat que proporciona en un àmbit molt proper com és l'institut de Flix, ja que pot ajudar a mantenir les dades dels docents guardades amb certa seguretat, i també els permet accedir als llocs web relacionats amb la seva feina des de la pròpia aplicació. A part d'això, l'App Inventor era una eina que sempre m'havia despertat curiositat, ja que a diferència dels meus companys de classe, jo no l'havia après a utilitzar durant l'ESO i quan en parlaven no podia seguir el fil.

Pel que fa a la part pràctica, en un principi, tenia expectatives més elevades, segurament pel fet de triar un tema que m'apassiona des de ben petit. Adonar-me que havia de tocar de peus a terra, seguir les orientacions del tutor i fer quelcom adequat al meu nivell i coneixements. Això ja ha estat un primer aprenentatge. En finalitzar el treball he assolit els objectius que m'havia proposat: aprofundir en els tipus de malware i el seu origen, desmentir els mites sobre hackers i crear una aplicació per a Android per a guardar contrasenyes i que resulti pràctic per al professorat de l'institut de Flix.

A partir de la investigació feta per realitzar el TdR he descobert noves possibilitats, noves línies d'investigació. Després d'haver fet aquest treball, m'agradaria aprofundir en el tema del hacking ètic puix considero que és molt

útil a l'hora de protegir-te. Podem afirmar que la millor manera de defensar-te és conèixer els mètodes de l'atacant.

Buscar informació sobre experts en informàtica i conèixer les seves opinions a través de les entrevistes també m'ha resultat interessant.

Per acabar diré que he comprès que fer avenços en el camp de la seguretat informàtica com a programador no és gens fàcil. Requereix molt esforç, dedicació i vocació. Encara que hi hagi persones que ho infravaloren, no qualsevol pot dedicar-s'hi, la seguretat és un aspecte amb el qual s'ha de tenir molta cura.

Com diu Magí Clavé, "El risc zero no existeix"[1].

[1] Magí Clavé, subdirector general d'informàtica del Banc Central Europeu. Vegeu la transcripció de l'entrevista a Magí Clavé als annexos.

7. BIBLIOGRAFIA/WEBGRAFIA

https://thehackerway.com/about/ (1 de juny 2017) (Informació sobre el concepte de hacking)

https://es.wikipedia.org/wiki/Seguridad_informática (3 de juny de 2017) (Informació sobre malware)

https://www.xataka.com/basics/cual-es-la-diferencia-malware-virus-gusanos-spyware-troyanos-ransomware-etcetera (8 de juny de 2017) (Diferència entre tipus de malware)

https://www.nitro-pc.es/blog/como-detectar-evitar-y-eliminar-virus-y-malwares/ (17 de juny de 2017) (Com evitar una infecció de malware)

https://www.vix.com/es/btg/tech/14183/7-peligrosos-grupos-hackers-que-serian-financiados-por-sus-gobiernos (21 d'agost de 2017) (Grups de hackers associats als governs)

http://www.tecnologiadiaria.com/2014/05/top-7-grupos-hackers-mas-poderosos-de-la-historia.html (1 d'octubre de 2017) (Grups de hackers més poderosos de la història)

http://ai2.appinventor.mit.edu/?locale=en#5299932004876288 (2 d'octubre de 2017) (Pàgina web de l'AppInventor, on he creat l'aplicació)

http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/

(9 d'octubre de 2017) (Història de la criptografia)

http://www.sertecnet.com/docs/crypto.pdf (15 d'octubre de 2017) (Criptografia a l'empresa)

http://es.qr-code-generator.com (10 de novembre de 2017) (Pàgina web on he creat el codi QR per l'aplicació)

https://emprenem.ara.cat/creixer/catala-que-guarda-BCE_0_1862813798.html (1 de gener de 2018) (Pàgina web on ha estat publicada l'entrevista a Magí Clavé)

https://emprenem.ara.cat/creixer/catala-que-guarda-BCE_0_1862813798.html (1 de gener de 2018) (Pàgina web on ha estat publicada l'entrevista a Fabián Martínez Portantier)

http://blog.educacionit.com/2017/06/27/entrevista-a-fabian-martinez-portantier-co-founder-en-securetia-e-instructor-de-seguridad-informatica-en-educacionit/ (2 de gener de 2018) (Pàgina web on ha estat publicada l'entrevista a Anonymous)

http://parceladigital.com/2017/09/01/yaiza-rubio-primera-mujer-espanola-hacker-en-participar-en-los-encuentros-blackhat-y-defcon/ (2 de gener de 2018) (Pàgina web on ha estat publicada l'entrevista a Yaiza Rubio)

https://www.dragonjar.org/ (3 de gener de 2018) (Blog on he trobat el llistat sobre les pel·lícules)

8. ANNEXOS

8.1 ENTREVISTES

8.1.1 ENTREVISTA A MAGÍ CLAVÉ

Entrevista a Magí Clavé, subdirector general d'informàtica del Banc Central Europeu, feta el 3 de setembre de 2017 per Àlex Font Manté publicada a https://emprenem.ara.cat/. La reproduïm tot seguit:

El català que guarda el BCE

La seguretat informàtica del Banc Central Europeu està en mans de Magí Clavé, un català d'Arbeca que avisa: "El risc zero no existeix".

Fig 132. Magí Clavé

Al segle XXI els vigilants dels bancs ja no són tant aquells policies de les pel·lícules antigues com els responsables informàtics dels bancs. I resulta que un dels bancs més importants del món, el Banc Central Europeu, té des del 2010 com a subdirector general d'informàtica un català d'Arbeca nascut el 1965 i que respon al nom de Magí Clavé*. Aquesta ha sigut la seva trajectòria, explicada per ell mateix.*

- Vaig néixer a Arbeca, però gairebé sempre he estat a Barcelona, tot i que vaig molt a Lleida. Vaig estudiar informàtica a la Universitat Autònoma entre el 1983

i el 1986. L'últim any vaig rebre una oferta per anar a un centre d'investigació a Alemanya. Vaig treballar sis anys per a Siemens. Vaig tornar a Barcelona el 1991, però després dels Jocs Olímpics hi va haver una baixada econòmica i ho vaig aprofitar per fer un MBA a Esade. Tot i que vaig intentar iniciar-me en la consultoria, al final vaig entrar al Deutsche Bank, a Barcelona, amb l'objectiu de crear un centre de desenvolupament de software. Vam arribar a ser gairebé 400 treballadors i una altra empresa alemanya va comprar aquesta divisió. L'objectiu era agafar projectes d'Alemanya i fer-los a Espanya perquè el cost laboral era més barat: per cada consultor alemany en teníem almenys dos a Barcelona. En un moment determinat, el 2005, el BCE em va fer una oferta per ser director d'informàtica, i vaig venir a Frankfurt.

- L'euro ja estava establert, però s'havien fet coses molt ràpidament per obtenir objectius molt agressius. En aquell moment ens va correspondre consolidar els processos i fer sistemes informàtics més sòlids. Em va sorprendre que la liquiditat [els diners que hi havia al sistema] es calculava d'una manera molt rudimentària i molt complicada, de manera que ho vam canviar per un sistema més automatitzat.

- La meva feina actual es divideix en diversos blocs. D'una banda, la tasca més estratègica: cap a on va el BCE, què necessitem en el futur, etc. En segon lloc, la feina operativa: tenim un llistat de 500 tasques que s'han d'anar fent cada any, dividides per grans, petites i mitjanes. Finalment, hi ha el dia a dia del banc: que els aparells funcionin bé i aquest tipus de coses.

- Fa quatre anys el Parlament Europeu ens va encarregar fer la supervisió de la banca europea. Era una qüestió estratègica crítica. Vam haver de fitxar moltíssima gent per arribar al dia D, que va ser el 4 de novembre del 2014, podent gestionar qualsevol cosa que pugui passar a les entitats financeres. Onze mesos abans, el gener d'aquell any, pràcticament no teníem treballadors per fer aquestes funcions. Va tenir molt mèrit.

- El BCE ha tingut dues fases en què ha actuat com una *start-up* : la primera va ser la implantació de l'euro, i la segona, l'assumpció de funcions de supervisor de la banca europea. En aquest segon cas, mentre esperàvem que arribés tota la gent que havíem de fitxar, teníem una manca de coneixement dels requeriments del negoci. Vam haver de fer moltíssimes suposicions que després es van validar a mesura que la gent va anar arribant. Vam haver de desenvolupar sistemes amb un risc i una incertesa que vam anar corregint amb el temps, això sí, abans del dia D.

- Un altre gran repte va ser la gestió de la crisi financera, especialment el 2009. A informàtica vam treballar en torns 49 caps de setmana dels 52 que té un any. El dijous el consell de govern del BCE prenia una decisió i ja l'havíem de tenir desplegada el dilluns següent. Eren canvis importants: reconfiguració dels sistemes, gestió de col·laterals [garanties dels bancs], llançament de programes d'ajuda al sistema... Havíem d'adaptar els sistemes en poques hores, fer proves i tenir la garantia que estava tot correcte. Crec que ha sigut la prova més dura que hem tingut fins ara. Quan et demanen coses que impliquen canviar diversos sistemes, i tens poques hores per desplegar-ho, pot ser que facis alguna cosa malament, no?

- El 2009 es van fer molts canvis en el *framework* de col·laterals [és a dir, en els criteris sobre les garanties dels bancs]. La banca va patir molt, i l'espanyola també. Aquestes decisions es prenien amb molt poc temps per aplicar-les. Entre el 2010 i el 2012 hi va haver la pitjor etapa de la crisi del deute sobirà, però operativament per a nosaltres va ser menys intensa. No dic que no hi hagués moments crítics, però.

- Els ciberatacs són un problema i la supervisió mirarà molt en aquest sentit. El BCE està molt preparat, però el risc zero no existeix. Treballem amb la Reserva Federal americana, amb el Banc del Japó... només s'hi pot lluitar amb inversió i coordinació internacional. ¿Quanta inversió destinem a la seguretat? Prefereixo

no donar aquesta dada. La Fed gasta més que nosaltres, molt més, però ells tampoc donen aquesta dada.

- Fa un parell d'anys vam tenir una fuga d'adreces de correus electrònics, sense informació crítica. Hi ha coses que no pots controlar. El *hacker* va aconseguir tenir accés a una llista de correus electrònics. No vam entrar en el joc del xantatge que volia el *hacker*. Ho vam comunicar obertament, amb transparència. No entrarem mai en un xantatge, encara que sigui d'informació sensible.

- Tenim ben documentats tots els passos que cal seguir cada cop que un país s'incorpora a l'euro, i el que fem és seguir el manual. No hi ha temes operatius molt crítics. Hi ha feina, però és bastant estàndard.

- ¿Estaríem preparats perquè un país sortís de l'euro? Tecnològicament, sí. Si el temps de sortida d'un país fos el mateix que té per entrar a l'euro, operativament seria equivalent. Però això seria en un escenari ideal. Si els períodes fossin diferents i calgués actuar amb rapidesa, seria més crític. Si fos una solució d'urgència, operativament sabríem el que s'ha de fer, però el que ens faltaria és temps[2].

[2] https://emprenem.ara.cat/creixer/catala-que-guarda-BCE_0_1862813798.html

8.1.2 ENTREVISTA A FABIÁN MARTÍNEZ PORTANTIER

Entrevista a Fabián Martínez Portantier, co-fundador a Securetia i Instructor de Seguretat Informàtica a EducaciónIT, feta el 27 de juliol de 2017 per l'empresa EducaciónIT publicada a http://blog.educacionit.com/. La reproduïm tot seguit:

¿Cómo surgió tu interés por la tecnología y por qué decidiste orientarte hacia el campo de la Seguridad Informática?

Fig 133. Fabián Martínez Portantier

La tecnología me empezó a gustar a eso de los 11 o 12 años. En ese momento le pedí a mis papás una computadora o una Nintendo64. Me compraron la computadora porque sabían que con eso, además de jugar, iba a poder estudiar. Cuando la tuve me interesó cada vez más cómo funcionaba. Y lo de la ciberseguridad, me fue interesando casi sin darme cuenta, era lo que me gustaba.

Dentro de Seguridad Informática, ¿cuál de todas sus ramas es la que más te apasiona?

Si bien me gusta todo lo que tenga que ver con la ciberseguridad, las tecnologías que más me apasionan son Linux, Redes y Web. También estoy trabajando muy de cerca con lo que es ciberinteligencia e inteligencia de amenazas (Threat Intelligence). Además de gustarme mucho estas dos últimas, son dos de las cosas que se vienen más fuerte para los próximos años.

¿Cuáles son las principales amenazas en ciberseguridad que deben enfrentar hoy las empresas?

Lo principal sigue siendo el malware. Hay muchos tipos diferentes, pero el que está más "de moda" ahora es el ransomware. También son muy populares las estafas online. En general, todo lo que pueda llegar a traducirse en un rédito económico para los cibercriminales. Además de eso, las empresas tienen que prestar particular atención a los temas de espionaje industrial, sabotajes, etc. Son cosas que parecen de película, pero son mucho más comunes de lo que uno se imagina.

¿En qué tipo de industrias y organizaciones es donde se registran mayores ataques y vulnerabilidades de seguridad? ¿Por qué?

Con respecto a ataques, siempre se apunta a las organizaciones que mueven más dinero. Bancos, plataformas de pago (como PayPal), plataformas de videojuegos (como Steam).

Obviamente, el objetivo actual de los cibercriminales es ganar dinero, y apuntan a los mercados en los cuales pueden obtenerlo. También hay un mercado muy grande de venta de malware y exploits personalizados en los que uno compra software malicioso de la misma manera que podemos comprar un software tradicional. Para trazar un paralelismo, sería algo así como un mercado negro de armas.

Últimamente se han observado reiterados ataques de ransomware a nivel mundial. Para quienes no conocen, ¿en qué consiste este ataque y por qué ha alcanzado semejante popularidad?

Los ransomware básicamente cifran todos los archivos importantes de un sistema y hacen que el usuario pierda la posibilidad de acceder a ellos. La única manera de recuperarlos es con una contraseña que solamente los cibercriminales conocen. Llegado ese punto, se pide una suma de dinero a modo de "rescate" para proporcionar dicha contraseña (ransom significa "rescate" en inglés).

Son tan populares principalmente por dos motivos: Son fáciles de desarrollar, y son difíciles de detectar.

Es fácil desarrollarlos porque no hacen nada del otro mundo. Reutilizan funciones de cifrado estándar. Es decir, no inventan nada nuevo.

Son difíciles de detectar porque tienen un comportamiento que, a simple vista, se puede llegar a confundir con el funcionamiento de software benigno.

Además, no necesitan tener permisos de adminstrador en el sistema para causar daño. Eso facilita las cosas para los cibercriminales.

¿En qué situación se encuentra actualmente el mercado laboral en el área de Seguridad Informática? ¿Cómo considerás que evolucionará a futuro?

En constante crecimiento. Y la tendencia se va a mantener, por lo menos, por varios años. Estamos cada vez más conectados y se vienen aún más conexiones! El Internet de las Cosas (IoT – Internet of Things) pretende conectar TODO a Internet. Los electrodomésticos, los autos, etc. Todo va a ser conectable a internet, y todo va a ser hackeable. Eso presenta nuevos desafíos para los profesionales de la ciberseguridad y hace que cada vez sean necesarias más personas capacitadas.

¿Qué cualidades y fortalezas son indispensables para quienes aspiren a desempeñarse en este campo?

Sobre todo tener ganas de aprender e investigar. Esta es una profesión donde todo el tiempo salen cosas nuevas, tecnologías, productos, ataques, etc.

Por eso, es fundamental estar motivado en seguir aprendiendo día a día. Teniendo en cuenta que todo lo que sabemos siempre es poco, porque es un mundo muy complejo, con tecnologías muy diversas.

No es necesario que conozcamos todo, pero es indispensable que tengamos una idea de cuáles son los productos que se usan y cuáles son las posibles vulnerabilidades de las principales tecnologías.

¿Cuáles son las principales enseñanzas y consejos que les transmitís a tus alumnos en base a tu experiencia?

Sobre todo, que aprendan, que se diviertan y que pregunten tranquilos, sin miedo. Como dije, es un mundo muy complejo y hay tantas tecnologías que al principio puede parecer avasallante. Pero esta es una profesión muy gratificante, sobre todo porque, en cierta forma, nos la pasamos todo el tiempo "jugando", "aprendiendo", "rompiendo" y "arreglando".

Lo siguiente creo que lo resumen bien:

"Cuando estoy usando una computadora, muchas veces me preguntan si estoy trabajando o jugando. Casi nunca puedo diferenciar[3]."

8.1.3 ENTREVISTA A ANONYMOUS

Entrevista al grup de hackers Anonymous, publicada el 30 de setembre de 2010 a https://www.pandasecurity.com/spain/mediacenter/entrevistas/. La reproduïm tot seguit:

P: ¿Qué es Anonymous?

R: Simplemente es una descripción de lo que somos. Anonymous no es una organización con una jerarquía y líderes. Nos consideramos anarquistas. Estamos formados por gente de todo tipo. En resumen, somos un grupo de gente tremendamente motivada para hacer todo lo que esté en nuestra mano para responder ante aquello que consideramos moralmente cuestionable.

P: ¿Cuál es vuestra misión actual?

[3] http://blog.educacionit.com/2017/06/27/entrevista-a-fabian-martinez-portantier-co-founder-en-securetia-e-instructor-de-seguridad-informatica-en-educacionit/

R: Luchar contra el lobby anti-piratería. Recientemente ha habido un aumento enorme de los ataques a la libertad personal en Internet promovidos por este grupo. Fíjate en la Ley de Economía Digital del Reino Unido y la normativa europea de los "tres avisos". Ambas iniciativas amenazan con cerrar las conexiones a Internet de los usuarios basándose en acusaciones de la industria musical y cinematográfica. En Estados Unidos se acaba de presentar un proyecto de ley que podría permitirle al gobierno norteamericano obligar a registradores de dominio de nivel superior como ICANN y Nominet a cerrar sitios Web sin NINGÚN tipo de juicio justo. ¡Se te declara culpable antes de demostrar si lo eres o no! Nuestras tácticas se inspiran en las de la gente que nos ha provocado: AiPlex Software. Hace unas cuantas semanas admitieron haber atacado sitios de intercambio de ficheros mediante ataques de denegación de servicio.

P: ¿Estáis a favor de la piratería?

R: Sí. Se trata del siguiente paso en la revolución cultural de la información compartida. Imagínatelo como el comienzo de una nueva era de la información; el inicio de una auténtica "igualdad de oportunidades", en la que no importa la riqueza o capacidad de cada uno. Yo mismo nunca hubiera llegado a dónde estoy ahora mismo sin los libros que he pirateado. ¡No me los podía permitir!

P: ¿Qué sitios habéis atacado?

R: Las Asociaciones Americanas de la Industria Musical y Cinematográfica [MPAA y RIAA], la Industria Fonográfica Británica [BPI], la Federación Australiana contra el Robo del Derecho de Autor [AFACT] , la Asociación Holandesa para la Protección de los Derechos de la Industria del Entretenimiento [BREIN], ACS:Law, Aiplex, Websheriff, y Dglegal.

P: Vuestro póster original decía que se utilizarían "redes de bots" en el ataque. ¿Alguno de vosotros se beneficia económicamente de ciber-delitos?

R: Eso depende de si empleas la definición de 'criminal informático' que utiliza el lobby anti-piratería. Para serte claro no aprobamos la obtención de beneficios económicos a partir de redes de bots o de malware; pero la gran mayoría de lo que constituye un ciber-delito es algo tan sencillo como descargarte tu canción favorita en lugar de pagar un precio ridículo por la misma (un precio del que el artista sólo se queda con un porcentaje mínimo).

P: ¿Qué relación tenéis con 4chan? ¿Sois todos miembros activos?

R: Algunos de nosotros frecuentamos 4chan, pero no tenemos ningún tipo de afiliación con ningún foro o sitio Web. Sólo lo utilizamos para comunicarnos.

P: ¿Cuánto tiempo va a durar el ataque?

R: No hay un plazo fijado. Seguiremos con él hasta que se nos pase el enfado.

P: ¿Estáis dispuestos a ir a la cárcel por esta causa?

R: Sí, pero hemos tomado todas las medidas necesarias para asegurarnos de que nuestro anonimato permanece intacto. Es más, ¿por qué no se le hace esa pregunta a la gente que contrató a Aiplex para atacarnos?

P: Si pudierais resolver esta situación, ¿qué os gustaría que hicieran los organismos audiovisuales mundiales?

R: Personalmente, me gustaría que desaparecieran de una puta vez. Que eliminasen todas esas leyes brutales que han promovido. Que tratasen a las personas como PERSONAS en vez de como criminales. Tienen que cambiar esa concepción tan anticuada y tradicional que tienen de la que las leyes sobre los derechos de propiedad intelectual sólo pueden ser aplicadas por empresas ricas y poderosas. Eso ya no resulta válido en la era de Internet, la Era de la Información.

Los artistas controlados por la industria audiovisual tienen muy poca voz sobre los contenidos que producen y sólo obtienen un porcentaje mínimo de los beneficios. Esto es evidente, como lo demuestra el hecho de que muchos artistas se han apartado del control de la industria. Ahí están los ejemplos de Nine Inch Nails y Radiohead. Los dos grupos han aceptado la piratería y aún así siguen obteniendo importantes beneficios.

P: ¿Sois conscientes de que estos ataques son ilegales en muchos países y de que vuestro grupo podría acarrear problemas legales a gente inocente que apoya vuestra causa?

R: Creo que la mayor parte de gente/participantes es consciente de ese riesgo. En un mundo en el que se ignora nuestra voz, creemos que no nos queda otra opción que la acción directa.

P: Algunas personas ven esto como el futuro de las protestas. ¿Prevés que pueda haber protestas como ésta en el fututo por otras causas?

R: Seguramente. En cuanto a las protestas, espero que el futuro de las protestas sea la ACCIÓN. No el andar en círculos con pancartas inútiles que todo el mundo ignora[4].

[4] https://www.pandasecurity.com/spain/mediacenter/entrevistas/entrevista-con-anonymous/

8.1.4 ENTREVISTA A YAIZA RUBIO

Entrevista a Yaiza Rubio, llicenciada en Ciències de la Informació i primera dona espanyola "hacker" en participar a les trobades Blackhat i Decon, publicada l'1 de setembre de 2017 a http://parceladigital.com/. La reproduïm tot seguit:

Yaiza Rubio es Licenciada en Ciencias de la Información, y cuenta en su «curriculum» académico con tres masters (Análisis de Inteligencia, Logística y Economía de la Defensa, y Derecho Tecnológico y de las TIC). En la actualidad, Yaiza desarrolla su labor profesional en ElevenPaths —la unidad de ciberseguridad de Telefónica— como analista de inteligencia dentro del ámbito de la ciberseguridad. En los últimos meses Yaiza ha contado con importante presencia en diversos medios de comunicación por ser la primera mujer española «hacker» en participar en los macro-encuentros Blackhat y Defcon. En la actualidad, con una trayectoria profesional tan reseñable, Yaiza se ha convertido en un rostro muy popular dentro del mundo de la ciberseguridad.

¿Quién es Yaiza Rubio?

Una persona a la que le influyó mucho el deporte de pequeña y que años después estos valores los sigue aplicando en su vida cotidiana como son la disciplina, la búsqueda de nuevos retos y la exigencia por conseguirlos.

Actualmente, ¿donde desempeña su labor profesional?

En ElevenPaths, la unidad de ciberseguridad de Telefónica.

¿Qué es un Analista de Inteligencia?

Se trata de un especialista dedicado a la obtención, gestión y análisis de información con el objetivo de generar conocimiento para apoyar la toma de decisiones. En mi caso, aplicado al ámbito de la ciberseguridad.

Semanas atrás asistió a los eventos Blackhat y Defcon. Se le ha calificado a usted como la primera mujer española «hacker» que participa en ese tipo de conferencias ¿Qué opina usted sobre ello?

Es evidente que hay menos mujeres que hombres dedicados al sector de la ciberseguridad, pero en España hay mujeres con conocimientos en seguridad

de sobra para poder ir. Puede ser simplemente que no se lo hayan planteado como objetivo. En general, muchos piensan que a estos eventos solo pueden ir profesionales de otro planeta, personas con un cerebro privilegiado. No lo comparto. Simplemente hay que ser valiente, identificar cuál es tu especialización dentro de este mundo y valorar si lo que haces es suficientemente bueno. Y si no es así, saber qué necesitas para conseguirlo. Así es como hemos trabajado Félix (Brezo) y yo durante estos años. De nada sirve ver los toros desde la barrera y hacer de menos el trabajo de los demás cuando se tiene la capacidad para hacer cosas igual de interesantes. La actitud siempre debe estar orientada a construir y no a destruir.

La palabra «hacker» tiene muchas definiciones, pero para el público en general, sobre todo para los profanos en la materia informática, solo conocen el significado negativo de la palabra ¿Qué opina sobre esto?

Es un concepto erróneo, a pesar de que la RAE lo considere como un sinónimo de pirata informático. Más bien está relacionado con una persona amante de la tecnología que tiene el objetivo de mejorarla.

En el diario El País se publicó un artículo titulado «Por qué las mujeres hackers son invisibles», en el cual le mencionan a usted ¿Qué opina sobre la afirmación a la que hace referencia el título del artículo?

Una afirmación bastante generalista. El artículo venía a diferenciar entre profesionales que defienden y atacan sistemas. En la práctica, la línea es más difusa.

Su curriculum académico es impresionante: Licenciada en Ciencias de la Información y con tres masters (Análisis de Inteligencia, Logística y Economía de la Defensa, y Derecho Tecnológico y de las TIC). En la informática, ¿formación profesional o universidad?

Comencé en este sector de casualidad. Tuve la suerte de conocer a la gente apropiada. He compaginado siempre el trabajo con formaciones, en mi caso, de «hacking ético» y de análisis forense, pero la realidad es que la mayoría de los conocimientos que tengo son a raíz de haber tenido cierta inquietud sobre algo que me ha parecido importante aprender.

Gene Spafford afirmó: «El único sistema seguro es aquél que está apagado en el interior de un bloque de hormigón protegido en una habitación sellada rodeada por guardias armados» ¿Qué opina de esta afirmación?

Que es incompleta, porque Spafford mostraba ciertas dudas de que fuera lo suficientemente seguro. Lo mejor es asumir que todo sistema puede ser vulnerable, de esta manera podremos estar preparados.

Los sitios web españoles, genéricamente, ¿son seguros?

Es mucho generalizar. Suele ir en proporción al interés que tengan las organizaciones en proporcionar a sus usuarios la seguridad necesaria. Sin embargo, en España tenemos la suerte de tener organismos públicos dedicados a proporcionar seguridad a nuestras empresas como INCIBE o el CCN-CERT para sectores estratégicos.

¿Windows, Linux, iOS, o Android?

Linux.

¿Software libre o software cerrado?

Software libre.

¿Software gratuito o software de pago?

La gratuidad es indiferente.

¿Nos puede decir un proyecto informático de terceros que le haya marcado (o admire) a lo largo de su recorrido profesional?

Es de admirar el proyecto de archive.org. Cuando Google no había ni nacido, este proyecto comenzó a capturar el estado de diferentes webs. Los analistas solemos recurrir bastante de este recurso.

¿Su dispositivo más utilizado: PC de escritorio, portátil, MAC, Tablet, o teléfono móvil?

Portátil y telefóno móvil.

¿Quién es su personaje «malo» en la historia de la informática?

Bill Gates.

¿Quién es su personaje «bueno» en la historia de la informática?

Jimmy Wales, fundador de Wikipedia.

¿El mejor invento de la informática?

Internet[5].

8.2 PEL·LÍCULES SOBRE HACKERS

A continuació, adjuntem un llistat de les millors pel·lícules sobre hackers segons la web https://www.dragonjar.org/.

Aquestes pel·lícules no t'ensenyaran tècniques màgiques de hacking i cracking, sinó que et serviran de diversió si t'agrada el món de la informàtica.

[5] http://parceladigital.com/2017/09/01/yaiza-rubio-primera-mujer-espanola-hacker-en-participar-en-los-encuentros-blackhat-y-defcon/

Fig 134. Pel·lícula The Net

The Net (1995)

Primer dia de vacances d'una programadora d'ordinadors. Rep un estrany disquet perquè l'investigui. Se'l guarda i descobreix que posseeix una clau per accedir al control de les bases de dades protegides dels Estats Units. Al mateix temps veu com totes les dades de la seva vida que figuren en arxius informàtics són suprimits o tergiversats.

Fig 135. Pel·lícula Die Hard 4: Live Free or Live Hard

Die Hard 4: Live Free or Die Hard (2007)

Als Estats Units, la infraestructura d'ordinadors que controla tot tipus de comunicacions, transports i energies pateix una aturada devastadora per part d'un grup terrorista. El cervell que s'amaga darrere d'aquesta trama ha tingut en compte fins al més mínim detall d'aquest devastador pla. Amb el que no comptava era amb John McClane (Bruce Willis), un policia de la vella escola que coneix una o dues coses sobre com frustrar amenaces terroristes, l'home adequat per a aquest tipus de treballs.

Fig 136. Pel·lícula Takedown

Takedown (2000)

Kevin Mitnick, el hacker més conegut d'Estats Units, es troba en llibertat condicional a causa dels seus piratejos informàtics. Malgrat tot, Kevin intenta piratejar el sistema de seguretat informàtica inventat per Shimomura, un especialista que treballa per al govern.

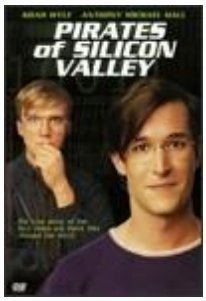

Fig 137. Pel·lícula Pirates of Silicon Valley

Pirates of Silicon Valley (1999)

Silicon Valley és una regió de Califòrnia on es troben, des de la dècada dels vuitanta, moltes de les noves empreses relacionades amb la informàtica i les noves tecnologies. "Pirates of Silicon Valley" relata, amb els noms reals, el principi de les empreses Apple i Microsoft a través dels seus fundadors: Steve Jobs i Steve Wozniak per part d'Apple, i Bill Gates i Paul Allen com a fundadors de Microsoft. Creadors de dues de les majors multinacionals del món dels ordinadors i el programari d'avui en dia, la pel·lícula mostra els començaments d'aquests joves amb enorme talent però no massa bon caràcter. A més, aquest telefilm de ficció va tenir certa polèmica en la seva estrena, ja que afirma clarament que Gates i Allen (de Microsoft) van copiar de Macintosh per al seu sistema operatiu Windows.

Fig 138. Pel·lícula The Matrix

The Matrix (1999)

Un programador pirata rep un dia una misteriosa visita ... Res més s'ha d'explicar de la sinopsi de Matrix. Gran part de l'èxit mundial d'aquesta fascinant i entretingudíssima pel·lícula es basa en el seu original guió, sorprenent idea producte de l'era tecnològica en què vivim. Si a això li unim la seva revolucionària estètica -amb espectaculars i trepidants escenes d'acció mai vistes al gènere-, tindrem el perquè de la consagració d'aquesta enlluernadora cinta fantàstica com el major film de culte de final de segle. Pot ser que en uns anys quedi obsoleta, però per llavors ja res ens farà oblidar el dia que vam descobrir què és Matrix ...

Fig 139. Pel·lícula Hackers

Hackers (1995)

Poden trencar qualsevol codi i entrar en qualsevol sistema. Normalment són només adolescents i ja es troben sota la vigilància de les autoritats. Són els pirates informàtics. Zero Cool, de nom Dadee Murphy, és una llegenda entre els de la seva classe. El 1988 va provocar ell sol la caiguda de 1.507 ordinadors a Wall Streeet i les autoritats li van prohibir tocar un sol teclat fins que complís 18 anys.

Fig 140. Pel·lícula

The Conversation

The Conversation (1974)

Harry Paul, un detectiu, el prestigi del qual com a especialista en vigilància i en sistemes de seguretat és reconegut pels seus col·legues a tot el país, rep l'encàrrec per part d'un magnat d'investigar la seva jove esposa. Haurà d'escoltar les seves converses amb un empleat d'aquest home del qual sembla estar enamorada. La missió, per a un expert de la seva categoria, resulta a primera vista inexplicable, ja que la parella no ofereix cap interès fora del corrent. No obstant això, quan Harry dóna per finalitzat el seu treball, adverteix que alguna cosa estranya s'amaga després de la banalitat que ha estat investigant, ja que el seu client es nega a identificar-se, utilitzant sempre intermediaris.

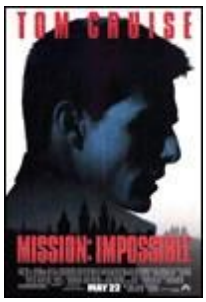

Fig 141. Pel·lícula
Mission Impossible

Mission Impossible (1996)

Ethan Hunt és un superespia capaç de resoldre qualsevol situación arriscada amb la màxima elegància. Forma part d'un competent equip dirigit per l'agent Jim Phelps, que els ha tornat a reunir per a una dificilíssima missió: evitar la venda d'un disc robat que conté informació secreta de vital importància.

Fig 142. Pel·lícula The Score

The Score (2001)

Nick Wells és un lladre de professió i és a prop de realitzar un robatori gairebé impossible, que implicarà unir forces amb un hàbil i jove còmplice. La dubtosa societat és arreglada per l'antic amic de Nick. Max interromp els plans de Nick de retirar-se del crim i establir-se amb la seva xicota. Això requereix que Nick trenqui una de les seves regles més importants: Sempre treballar sol.

Fig 143. Pel·lícula Takedown

The Thirteenth Floor (1999)

Hannon Fuller, un magnat dels negocis i emprenedor d'empresari, mor en estranyes circumstàncies. El seu amic Douglas Hall és introduït a una voràgine de crim i decepció quan la mort del seu superior comença a revelar una perillosa doble vida que es mou entre dos mons paral·lels, un a 1937 i un altre en el present.

Fig 144. Pel·lícula Swordfish

Swordfish (2001)

Stanley Jobson, un expert en informàtica que acaba de sortir de presó, és requerit pel terrorista Gabriel Shear perquè l'ajudi a descodificar un complicat codi de seguretat d'un compte secret. Només pocs hackers al món són capaços de realitzar aquest treball, i ell és un d'ells. Malgrat que no pot tocar un ordinador, els mètodes de Shear obligaran Jobson a ajudar-lo en la seva missió.

Fig 145. Pel·lícula The Italian Job

T*he Italian Job* (2003)

Charlie Croker i la seva banda de lladres intenten aconseguir el cop de les seves vides; fer-se amb un camió ple d'or, falsejant els semàfors de Los Angeles per crear el major embús mai vist a la ciutat. Així confien a aconseguir un cop perfecte i assegurar-se una escapada sense riscos.

Fig 146. Pel·lícula Foolproof

Foolproof (2003)

Kevin, Rob i Sam planegen assalts perfectes, sense la intenció de portar-los a terme. Un gàngster troba part del seu material de treball i decideix fer-los xantatge perquè realitzin un robatori milionari, i només la seva astúcia els podrà lliurar del problema.

Fig 147. Pel·lícula eXistenZ

eXistenZ (1999)

Emmarcat en un futur pròxim, Existenz inventa una societat en què els dissenyadors de jocs són venerats com superestrelles i on els jugadors poden entrar orgànicament en aquests jocs. Alegra Geller és l'autora del joc més innovador, Existenz, una creació on els usuaris no distingeixen els límits entre la realitat i la fantasia.

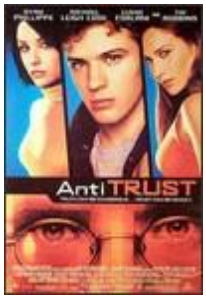

Fig 148. Pel·lícula Antitrust

Antitrust (2001)

Milo (Ryan Phillippe), un jove geni programador, té fusta per convertir-se en un dels millors informàtics del món. Des del garatge de casa seva, desenvolupa la tecnologia que ambicionen les empreses més grans del món: un revolucionari programari que permet l'enllaç de totes les formes de comunicació digital, a través d'una sola font d'alimentació. Quan Milo està a punt d'aconseguir el seu somni, rep una oferta que no pot rebutjar: diners, recursos i la multitud de possibilitats que Gary Winston (Tim Robbins), el director d'NURV, una milionària i poderosa empresa de programari, li ofereix en safata.

Fig 149. Pel·lícula Sneakers

Sneakers (1992)

Martin Bishop, un geni dels ordinadors, és el líder d'un grup d'experts especialitzats en comprovar els sistemes de seguretat de grans empreses. Un dia és obligat a treballar per a una agència secreta per tal de robar una caixa negra secreta. Després d'aconseguir-la, descobreixen que aquesta caixa té la capacitat de descodificar tots els sistemes d'encriptació existents en el món, i que els agents per als quals treballen no són exactament del govern.

Fig 150. Pel·lícula Revolution OS

Revolution OS (2001)

Per aquesta pel·lícula desfilen molts dels filòsofs i fundadors d'aquests projectes. Richard Stallman és el fundador de GNU; Linus Torvalds és el primer desenvolupador de Linux i Richard Perens, un personatge més aviat estrany, és l'autor de la definició de codi obert.

Fig 151. Pel·lícula Wargames

Wargames (1983)

David és un jove coneixedor de tot el referent a la informàtica: se salta els més avançats sistemes de seguretat, aconsegueix els més sofisticats codis secrets i entén la informàtica com un joc. Però el joc es complica quan inconscientment connecta el seu ordinador personal al del Departament de Defensa americà, encarregat del sistema de defensa nuclear i desencadena una situació de perill de proporcions incontrolables. Ajudat per la seva xicota i per un "geni" dels ordinadors haurà de lluitar contra el temps i evitar el major conflicte mundial de tots els temps: la Tercera Guerra Mundial.

Fig 152. Pel·lícula
Tron

Tron (1982)

Un hacker és dividit en molècules i transportat a les entranyes d'un ordinador en el qual un malvat programa controla els comportaments al seu gust.

Fig 153. Pel·lícula 23
Nada es lo que parece

23 Nada es lo que parece (1998)

Està basada en una història real d'uns joves hackers alemanys que venien informació al KGB en plena guerra freda. Una història excel·lent on es fa referència al CCC, el primer troià, el primer codi utilitzat per realitzar atacs de força bruta i un munt de detalls més que segur que t'engaxaran.

Fig 154. Pel·lícula Ranxo

3 Idiots (2009)

Explica la història de Ranxo, un noi amb una passió per estudiar i aprendre. Encara que no veiem una sola consola en la pel·lícula, ens mostra la veritable essència del hacking, poder veure les coses d'una altra manera i qüestionar-s'ho tot. Realment és una pel·lícula que no es pot deixar de veure.