Seguretat en dispositius mòbils

PID_00245986

Marc Domingo Prieto
Javier Salvador Calvo

Temps mínim de dedicació recomanat: 4 hores

Universitat Oberta de Catalunya

Índex

Introducció

La seguretat en dispositius mòbils s'ha convertint en un aspecte molt important a causa de l'increment d'«atacs» rebuts i les conseqüències que tenen. Aquests atacs estan incentivats per la popularització d'aquests dispositius mòbils, l'augment d'informació personal i confidencial que emmagatzemen i les operacions fetes a través d'aquests, com per exemple les bancàries.

Atac

Atac és el mètode pel qual un individu intenta prendre el control d'un dispositiu mòbil, desestabilitzar-lo o danyar-lo.

Els dispositius mòbils estan formats per un conjunt de components de maquinari capaços de suportar una gran varietat de tecnologies sense fils (GSM, UMTS, 3G, 4G, 5G, Wi-Fi, Bluetooth, etc.) i hi destaquen un o diversos processadors d'altes prestacions que permeten executar un sistema operatiu molt complex i un gran nombre d'aplicacions que requereixen gran capacitat de càlcul. Aquesta situació incrementa amb escreix les diverses vulnerabilitats a les quals estan exposats aquest tipus de dispositius.

Un maquinari més potent implica que més dades (normalment personals) poden ser tractades, sia les que s'emmagatzemen a la memòria dels dispositius mòbils, o les que perceben els diferents sensors que incorporen. A més, suportar gran varietat de tecnologies sense fils també obre més vies d'atac.

Un sistema operatiu més complex també pot augmentar les vulnerabilitats dels dispositius mòbils. Quan els sistemes creixen és més fàcil tenir algun error al programari (*software*). A més, la perillositat augmenta perquè encara no estem mentalitzats d'aquests possibles problemes de seguretat.

Error

En anglès, *bug*.

Aquest mòdul no pretén ser un manual de seguretat ni recollir totes les vulnerabilitats existents sinó introduir els conceptes i principis de seguretat per als dispositius mòbils. Aquest material ha de servir perquè ens familiaritzem amb els riscos en els quals estan immersos els dispositius mòbils i també amb les mesures de seguretat aplicables per a reduir els danys causats per algun atac.

Començarem el mòdul veient alguns conceptes bàsics de seguretat i identificant les diferents capes on poden implementar seguretat els dispositius mòbils: comunicacions sense fils, sistema operatiu, aplicació i usuari. Posteriorment, analitzarem la seguretat en cadascuna d'aquestes capes.

Objectius

Amb l'estudi d'aquest mòdul es pretén que l'estudiant assoleixi els objectius següents:

1. Entendre els conceptes bàsics de seguretat.

2. Veure les mesures de seguretat que es fan servir en les tecnologies de comunicacions sense fils utilitzades en els dispositius mòbils.

3. Conèixer les mesures de seguretat que s'apliquen en el sistema operatiu.

4. Revisar els riscos que presenten algunes aplicacions.

5. Comprendre les conseqüències d'una pèrdua o robatori d'un dispositiu mòbil i conèixer els mecanismes per a limitar-ne els efectes.

6. Saber quines són les pràctiques de seguretat recomanades quan es fa servir un dispositiu mòbil.

1. La problemàtica de la seguretat

1.1. Conceptes bàsics de seguretat

Quan parlem de seguretat hi ha una nomenclatura imprescindible per a identificar el grau de protecció que estem fent servir. Si prenem com a exemple els diferents passos que tenen lloc durant una trucada telefònica sobre una xarxa sense fils, podem identificar els quatre conceptes clau de seguretat de la informació:

- **Confidencialitat**: ha de ser possible que ningú no pugui capturar la nostra trucada i assabentar-se del que diem.
- **Autenticació**: només els usuaris amb un telèfon de la xarxa, és a dir, pertanyents a la companyia, poden utilitzar la xarxa.
- **Integritat**: cal que la informació, de veu o dades, que viatgi per la xarxa sense fils no es pugui alterar sense que es detecti.
- **No-repudi**: no ha de ser possible que un usuari que ha utilitzat la xarxa ho pugui negar; és a dir, que s'ha de garantir que hi hagi proves que demostrin que un usuari ha fet una determinada trucada.

De manera més genèrica, i alhora formal, podem definir aquests conceptes de la manera següent.

La **confidencialitat** és la propietat que assegura que només els que hi estan autoritzats tindran accés a la informació. Aquesta propietat també es coneix com a *privadesa*.

La **integritat** és la propietat que assegura la no-alteració de la informació. Per *alteració* entenem qualsevol acció d'inserció, esborrament o substitució de la informació.

L'autenticació és la propietat que fa referència a la identificació. És el nexe d'unió entre la informació i l'emissor d'aquesta.

El **no-repudi** és la propietat que assegura que cap part no pugui negar cap compromís o acció presos anteriorment.

Privadesa

El mot *privadesa* és la traducció de la paraula anglesa *privacy*. Per al mateix concepte en anglès també s'utilitza el mot *secrecy*.

Cal destacar que la propietat d'autenticació és potser la més important de les que acabem de mencionar, ja que serveix de poc aconseguir confidencialitat i integritat si resulta que el receptor de la informació no és qui nosaltres pensem.

Aquests quatre conceptes bàsics de seguretat de la informació que acabem de definir són la base de la pràctica totalitat de requisits de seguretat que es poden necessitar, tant si es tracta de comunicacions sense fils com d'informació en general.

1.2. Capes de seguretat en dispositius mòbils

Per a poder entendre la importància de la seguretat en els dispositius mòbils cal conèixer les capacitats d'aquests dispositius i com s'hi ha arribat. Principalment, els dispositius mòbils han viscut una important revolució quant a les aplicacions que poden executar. Aquesta ha estat marcada per tres motius:

1) Un maquinari (*hardware*) potent, amb molts sensors.

2) Un sistema operatiu complex que facilita un SDK[1] senzill i potent per als desenvolupadors.

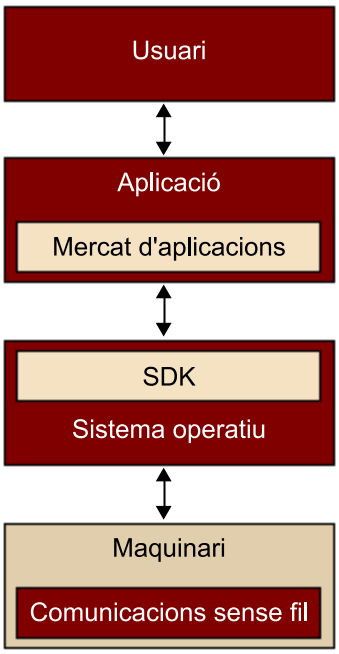
(1) *SDK* són les sigles en anglès de *software development kit*, traduït al català com a *equip de desenvolupament de programari*.

3) Un mercat d'aplicacions completament integrat en el sistema i molt intuïtiu, que facilita les transaccions tant als usuaris com als desenvolupadors.

A causa d'aquestes noves funcionalitats que ofereixen els sistemes operatius per a mòbils i a les aplicacions que s'han creat a sobre, els dispositius mòbils acaben emmagatzemant gran quantitat de dades, generalment confidencials. Ja no únicament desem els números de telèfon dels nostres contactes, el registre de trucades o els SMS, sinó que emmagatzemem una gran quantitat d'informació personal, com poden ser comptes bancaris, documents o imatges.

Aquest augment de la informació personal emmagatzemada fa que més persones puguin estar interessades a obtenir-la. A més, la complexitat actual dels sistemes operatius per a mòbils ha incrementat els forats de seguretat exposats. Per tant, quan utilitzem dispositius mòbils és recomanable seguir unes pràctiques de seguretat, que seran semblants a les utilitzades en els ordinadors.

Per a poder analitzar la seguretat dels dispositius mòbils de manera eficient s'ha organitzat aquest mòdul en quatre apartats: les comunicacions sense fils, el sistema operatiu, l'aplicació i l'usuari. Cada apartat contindrà una petita introducció, una petita descripció tant dels principals atacs com dels principals mecanismes de prevenció i un cas d'estudi.

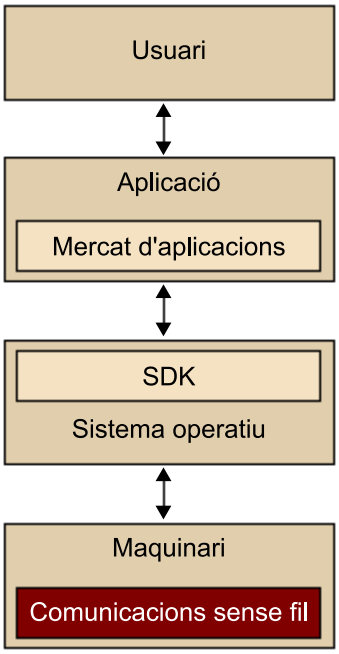

Usuari
Aplicació
Mercat d'aplicacions
SDK
Sistema operatiu
Maquinari
Comunicacions sense fil

2. Comunicacions sense fils

Les comunicacions sense fils permeten que dos o més dispositius mòbils es puguin comunicar entre si sense necessitat d'estar connectats per un medi físic, com és el cable. A més, creen una capa d'abstracció, i permeten que dispositius mòbils amb diferents sistemes operatius puguin intercanviar informació.

Vegeu també

Aquest mòdul no pretén estendre's en el funcionament i la seguretat de les comunicacions sense fils, sinó únicament mostrar d'una manera global els mecanismes de protecció fets servir i les possibles vulnerabilitats que podran ser explotades per un atacant. Per als que vulguin aprofundir en la matèria es recomana la lectura dels mòduls didàctics de l'assignatura de *Seguretat en comunicacions sense fils*, i també els documents de la bibliografia.



L'ús de les comunicacions sense fils presenta un seguit d'avantatges com ara l'escalabilitat i la mobilitat. Ara bé, quan ens centrem en temes de seguretat, les comunicacions sense fils mostren el vessant més fosc que tenen.

L'ús de l'espectre electromagnètic com a medi de comunicació implica que la informació viatja per l'aire sense que res ni ningú no li pugui posar límits. Això fa que aquesta informació sigui més difícil de protegir i que, per tant, les propietats de seguretat de què es disposa en altres entorns no sempre es puguin assolir en les comunicacions sense fils.

2.1. Atacs

Per a poder obtenir cotes de seguretat elevades en l'àmbit de les xarxes sense fils és interessant analitzar quines són les amenaces més importants d'aquest entorn i quina relació tenen amb les propietats que s'han definint al subapartat 1.1.

Malgrat que no hi ha una classificació estricta dels possibles atacs a la seguretat (i per això és important la definició de les propietats del subapartat 1.1), a continuació n'apuntem els més importants:

1) ***Masquerading***. Acció en què l'atacant suplanta la identitat d'alguna entitat del sistema (estació base o dispositiu mòbil) per obtenir accés a recursos d'aquest sistema. Aquest atac incideix directament en la propietat d'autenticació. Per a prevenir aquests tipus d'atac és necessari un bon procés d'autenticació tant per part del dispositiu mòbil com per part dels punts d'accés a la xarxa.

Exemple de *masquerading*

Un atacant pot suplantar una estació base de la xarxa (emetent un senyal de més potència que el de l'estació base legítima) i així capturar missatges d'autenticació dels usuaris. Un cop obtinguda la informació d'aquests missatges, es pot fer passar per un dels usuaris legítims de la xarxa per obtenir accés als recursos.

2) Denegació de servei[2]. Acció en què l'atacant aconsegueix que el servei no sigui disponible per als usuaris legítims o bé que el servei es retardi o s'interrompi. Aquest tipus d'atac és potser l'únic que no es pot identificar amb cap de les propietats de seguretat definides en l'apartat anterior. Aquest fet es deu a la circumstància que aquests atacs s'acostumen a dur a terme fins i tot amb anterioritat al procés d'autenticació, justament amb l'enviament massiu de sol·licituds d'aquest tipus.

[(2)]En anglès, *denial of service* (DoS).

Exemple d'atac de denegació de servei

Un atac de denegació de servei a una xarxa sense fils es pot fer mitjançant la generació d'un senyal de ràdio de la mateixa freqüència que el de la xarxa sense fils però amb una potència superior. Això atenua el senyal de la xarxa, amb la qual cosa no es permet als usuaris de poder-la utilitzar. Aquest tipus d'atacs també es coneix com a *jamming*.

3) ***Eavesdropping***[3]. Acció en què l'atacant obté informació d'una comunicació en la qual no és ni emissor ni receptor. En aquest cas, l'atacant vulnera la confidencialitat de la informació que ha interceptat. Aquest tipus d'atac es classifica com a *atac passiu*, ja que l'atacant obté informació de les dades en trànsit, però per mitjà d'aquest atac no pot dur a terme cap acció sobre la xarxa ni sobre la informació que hi circula. És important tenir en compte, però, que la informació obtinguda en un atac d'*eavesdropping* pot donar lloc a un atac posterior de *masquerading*.

[(3)]La paraula *eavesdropping* no té equivalent en català i es tradueix com a *escoltar d'amagat*.

4) Confidencialitat de posicionament. Acció en què l'atacant obté, mitjançant diferents tècniques, la posició física d'un dispositiu mòbil i, per tant, la del seu propietari. Aquest tipus d'atac pot afectar seriosament la privadesa de les persones en tant que poden ser localitzades en qualsevol moment pel sol fet de tenir un dispositiu mòbil en funcionament.

Especificitats de l'entorn sense fils

La confidencialitat de posicionament és un fet característic de les comunicacions sense fils; en aquest entorn és on té sentit parlar de posició física (en els entorns amb fil els dispositius tenen una localització física concreta o, en qualsevol cas, una mobilitat molt limitada).

Exemple d'atac de confidencialitat de posicionament

La posició del dispositiu mòbil es pot utilitzar a fi de bé en aplicacions per a controlar flotes de transports, però també es pot utilitzar de manera maligna, per exemple, per a l'enviament de propaganda no volguda (inundació o *spamming*) relacionada amb esta-

bliments pròxims a la localització del dispositiu mòbil. Un altre ús maliciós d'aquesta informació podria ser determinar que l'usuari no es troba a casa seva per tal d'entrar-hi a robar.

El factor humà

Els propis usuaris també poden proporcionar informació pública sobre la seva posició als atacants a través de la seva activitat, per exemple amb les seves publicacions a les xarxes socials.

2.2. Mecanismes de prevenció

La preocupació per la seguretat en els entorns sense fils és creixent, ja que l'ús d'aquest entorn per a aplicacions de comerç electrònic requereix un grau de seguretat elevat.

Quan parlem de *tècniques per a prevenir la seguretat* podem fer una distinció clara entre les que treballen en el nivell físic de la comunicació i les que treballen en la resta de nivells, tant si és en el nivell d'enllaç com en el nivell d'aplicació.

Les tècniques més habituals que s'apliquen al nivell físic són les de *difusió d'espectre*[4]. Aquestes basen el funcionament a fraccionar el senyal de ràdio i transmetre'l de manera imperceptible per diferents freqüències. D'aquesta manera, si no es coneix la manera en què el senyal ha estat distribuït per les diferents freqüències no es pot reconstruir, ja que els diferents senyals que es reben en cada freqüència són percebuts com a soroll.

(4)En anglès, *spread spectrum*.

Les tècniques de difusió d'espectre també permeten d'atenuar els atacs de *jamming*, ja que el senyal emès en una freqüència concreta per a produir l'atac només afectarà part de les dades enviades.

En qualsevol cas, les tècniques de difusió d'espectre ofereixen poca o nul·la seguretat i la justificació del seu ús cal buscar-la més en qüestions d'eficiència que no de seguretat. El que sí que és cert és que les tècniques de difusió d'espectre permeten la reutilització d'un espectre de ràdio per a diferents tecnologies de comunicació, ja que es minimitzen les interferències.

Des del punt de vista de les capes superiors al nivell físic, l'ús de la criptografia permet d'obtenir uns bons nivells de seguretat. Per mitjà de la criptografia es poden obtenir serveis d'autenticació i confidencialitat que permeten assolir les propietats de seguretat descrites anteriorment i, per tant, ajuden a reduir l'èxit dels atacs descrits.

Criptografia

Aquest mòdul només pretén introduir els conceptes bàsics de la criptografia. Per als que vulguin aprofundir en la matèria es recomana la lectura dels mòduls didàctics de l'assignatura de *Criptografia* o d'algun dels llibres sobre el tema que s'inclouen en la bibliografia del mòdul.

La majoria de sistemes de comunicació sense fils duen a terme el servei d'autenticació per mitjà del model **repte-resposta**[5]. Aquest protocol consisteix en un intercanvi de missatges entre les dues parts que es volen autenticar per a assegurar-se que cadascuna d'aquestes parts coneix certa informació prèviament intercanviada i que, per tant, cadascú és qui diu que és.

(5)En anglès, *challenge-response*.

Exemple del model repte-resposta

Suposem que l'Anna i en Bernat es coneixen i han decidit que compartiran el nombre $k = 7$ per a autenticar-se. Quan l'Anna (A) i en Bernat (B) es troben, A s'autentica davant B de la manera següent:

- B tria aleatòriament com a repte c un enter, per exemple el 4, i l'envia a A.
- A suma al repte $c = 4$ el valor $k = 7$, que prèviament havien acordat, i envia el resultat, $r = 11$, a B.
- B, que també ha calculat $r' = 4 + 7 = 11$, verifica que $r' = r$ i que, per tant, A és qui diu que és, ja que coneix el valor k que prèviament han acordat.

Òbviament, en els models d'autenticació que utilitzen aquest esquema no és fàcil obtenir el valor k a partir dels valors intercanviats r i c.

L'avantatge d'aquest sistema és que el valor del repte c varia aleatòriament per a cada procés d'autenticació, de manera que la intercepció de les dades en un procés d'aquest tipus no compromet, en principi, els processos posteriors.

És important destacar que el model repte-resposta que hem descrit i que fan servir la majoria de sistemes de comunicació sense fils per a l'autenticació necessita una informació k que l'emissor i el receptor coneixen prèviament al procés d'autenticació mateix.

Pel que fa al servei de confidencialitat, les tecnologies sense fils implementen esquemes basats en la **criptografia de clau compartida**. La criptografia de clau compartida, a diferència de la criptografia de clau pública, es basa en el fet que tant l'emissor com el receptor comparteixen una mateixa clau. Aquest mecanisme encaixa perfectament en el model d'autenticació de repte-resposta que acabem de descriure, en què totes dues parts també han de compartir certa informació.

Lectura recomanada

La criptografia de clau compartida que s'utilitza per a protegir la confidencialitat en la majoria de les comunicacions sense fils són les xifres de flux. En el mòdul didàctic «Xifres de flux» dels materials de l'assignatura de Criptografia podeu trobar més informació sobre els esquemes de xifratge en flux.

L'ús de la criptografia de clau compartida no representa un problema excessivament greu per a alguns models de comunicació sense fils. Per exemple, si pensem en la telefonia mòbil, usuari i operador s'intercanvien les claus en el moment que l'usuari adquireix el terminal mòbil; de fet, més concretament quan obté la targeta SIM. D'altra banda, en una WLAN els usuaris hi tenen accés pel fet de pertànyer a una entitat o grup, de manera que l'intercanvi de claus també és fàcil de fer. Aquest fet, però, dificulta el procés d'obertura de les xarxes sense fils en el sentit que si es pretén donar cobertura de WLAN en un aeroport oferint serveis de confidencialitat les coses es poden complicar.

2.3. Cas d'estudi: IEEE 802.11

L'estàndard IEEE 802.11 defineix l'arquitectura d'una xarxa d'àrea local en un entorn sense fils, on s'especifiquen dos serveis de seguretat: l'un per a obtenir la propietat d'autenticació i l'altre per a la propietat de confidencialitat i integritat.

Atès que en un dels processos d'autenticació s'utilitzen els algorismes que es descriuen en el procés de confidencialitat, descriurem primer aquest darrer.

El servei de confidencialitat de l'estàndard IEEE 802.11 es basa en l'algorisme *wired equivalent privacy* (WEP).

L'algorisme WEP proporciona les propietats de confidencialitat i integritat. La confidencialitat s'aconsegueix utilitzant criptografia de clau simètrica, en particular el xifrador en flux RC4. La integritat s'obté mitjançant una suma de comprovació (*checksum*) CRC32.

RC4

RC4 respon a les inicials de *Ron cryptosystem number 4* (Ron Rivest en va ser el creador el 1987). Rivest va cedir el desenvolupament de l'algorisme a l'empresa RSA Data Security. D'altra banda, l'algorisme va ser secret durant set anys, fins que el 1994 va aparèixer anònimament a Internet i actualment ja és públic.

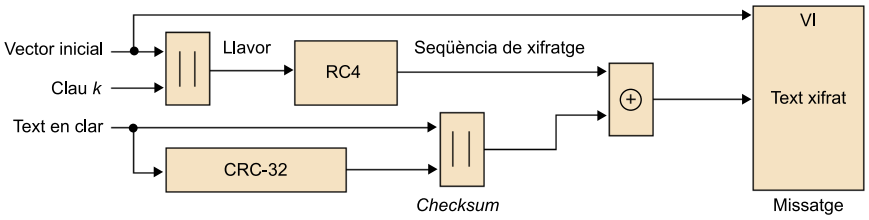
CRC-32

La funció CRC-32 és una funció lineal que tan sols utilitza sumes i multiplicacions. Aquest fet fa que sigui fàcil predir la suma de comprovació resultant d'una modificació en el text en clar.

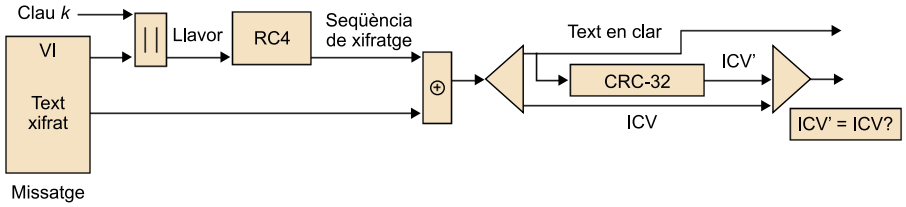
Tal com menciona l'estàndard, l'algorisme WEP pretén dotar les xarxes sense fils de les mateixes propietats de seguretat que les xarxes amb fil. Aquest argument ha estat utilitzat sovint per a rebatre els problemes de feblesa que té l'algorisme, ja que molts d'aquests problemes també són en les xarxes amb fil.

Esquema de xifratge del WEP

El WEP pren com a entrada, d'una banda, el text en clar –és a dir, la informació que s'ha de transmetre per la xarxa sense fils– i, de l'altra, un vector inicial *VI* (de 32 bits) i una clau *K* (entre 40 bits i 128 bits). Tal com mostra la figura, la clau *K* i el vector *VI* es concatenen i s'obté la llavor del xifrador en flux. L'RC4 genera una seqüència pseudoaleatòria de bits que se suma al text en clar per a obtenir el text xifrat. Prèviament, i per a obtenir la propietat d'integritat, s'aplica al text en clar la funció CRC-32 per a obtenir una suma de comprovació (*integrity check value*, ICV) de la informació. Aquest valor es transmet per a poder verificar posteriorment que la informació no ha estat alterada.



El procés de desxifratge de la informació que du a terme el receptor és exactament l'invers del que acabem de descriure, tal com es mostra en la figura següent.



Com que l'RC4 és un criptosistema de clau compartida, l'estació i el punt d'accés necessiten intercanviar tant el vector inicial *VI* com la clau *K* per a poder-se comunicar utilitzant el WEP. Com que el *VI* s'envia en clar, la seguretat de l'algorisme depèn només de la clau. Així i tot, cal assegurar la integritat de la transmissió del *VI*, ja que si el *VI* utilitzat per l'emissor no és exactament

igual que el del receptor, els processos de xifratge i desxifratge no seran inversos. Aquest intercanvi d'informació es fa durant el procés d'autenticació, que descriurem a continuació.

L'estàndard IEEE 802.11 té dues variants que implementen el servei d'autenticació:

- *Open system authentication* (OSA)
- *Shared key authentication* (SKA)

L'OSA és d'implementació obligada en l'estàndard i la inclouen per defecte la majoria dels productes que es poden trobar en el mercat. Com indica el nom, és un sistema d'autenticació obert i que, per tant, no limita l'accés, cosa que implica que, des del punt de vista de la seguretat, aquest sistema per si sol no tingui cap mena d'interès.

L'OSA simplement intercanvia missatges entre una estació i el punt d'accés sense fils. Qualsevol estació que pugui enviar i rebre missatges correctes podrà tenir accés a la xarxa.

El procés d'autenticació s'estableix a partir de dos passos entre l'estació i el punt d'accés:

- En el primer pas, l'estació indica al punt d'accés la seva adreça MAC i un identificador que indica que el missatge és d'autenticació.

- En el segon pas, el punt d'accés respondrà amb un missatge indicant si el procés d'autenticació ha tingut èxit o no.

Èxit del procés d'autenticació

L'èxit de l'OSA només depèn de la capacitat que tingui l'estació de generar correctament trames WLAN. Això, de fet, és poca cosa, perquè òbviament el punt d'accés i l'estació només es podran comunicar si utilitzen el mateix protocol amb el mateix format de trames. Si són diferents, no solament el procés d'autenticació OSA no tindrà èxit sinó que, possiblement, la comunicació en si mateixa tampoc.

A partir d'aquest moment, si s'utilitza el mètode OSA l'estació ja està autenticada.

Molts dels sistemes de xarxes LAN sense fils que es troben en el mercat implementen un mecanisme addicional de control d'accés sobre l'OSA basat en l'adreça MAC de l'estació. Aquest mecanisme consisteix a no admetre la connexió d'adreces MAC no autoritzades. Així, cada punt d'accés ha de gestionar la llista de les adreces MAC autoritzades. La problemàtica del manteniment de les llistes, l'escalabilitat (imaginem-nos un campus universitari en què cada estudiant té el seu portàtil) i la suplantació d'adreces MAC fan que aquest sistema no sigui una solució idònia per al procés d'autenticació. Per aquest motiu, és recomanable utilitzar el mètode d'autenticació SKA.

El mètode SKA[6] permet l'autenticació de les estacions i els punts d'accés per mitjà de l'algorisme WEP, juntament amb un sistema de repte-resposta.

(6) *SKA* són les sigles de *shared key authentication.*

És important destacar que, atès que l'estàndard IEEE 802.11 no especifica l'obligatorietat de l'algorisme WEP i l'SKA l'utilitza, les versions de l'estàndard que no tinguin activat el WEP no podran utilitzar l'SKA.

Aquest procés d'autenticació consisteix en l'intercanvi de quatre missatges entre l'estació que s'autentica i el punt d'accés. El sistema d'intercanvi de claus no implica l'enviament de claus en clar, tal com veurem més endavant, però requereix que la clau secreta compartida s'hagi proporcionat per un canal segur amb anterioritat al procés d'autenticació.

El punt d'accés envia contínuament un senyal de balisa per tal d'anunciar la seva presència. Una estació que vulgui accedir a la xarxa, en trobar el senyal de balisa, inicia el procés d'autenticació amb el punt d'accés, l'adreça del qual figura en el senyal de balisa.

Procés d'intercanvi de missatges

El procés d'intercanvi de missatges és el següent:

1) L'estació envia un missatge al punt d'accés per sol·licitar l'autenticació.

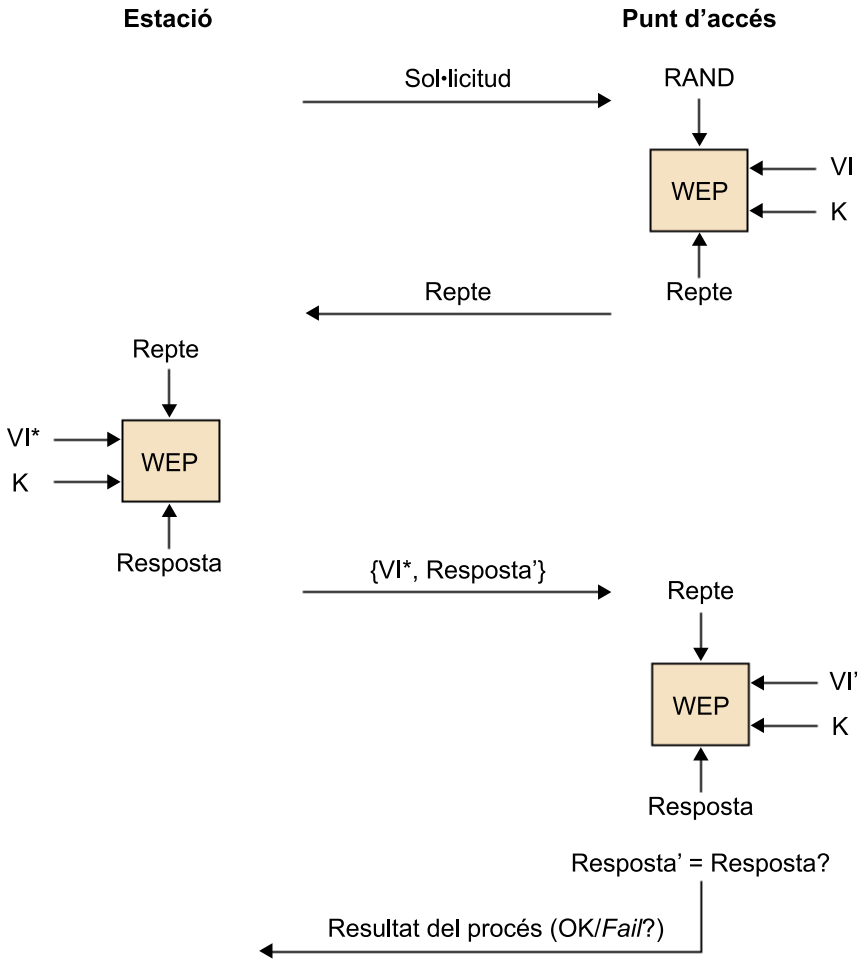
2) El punt d'accés genera un **Repte** de 128 *bytes* utilitzant l'algorisme WEP a partir d'un valor pseudoaleatori (RAND), una clau *K* que comparteix amb l'estació i un vector inicial (*VI*), que l'envia a l'estació.

3) L'estació genera la **Resposta'** utilitzant també l'algorisme WEB amb el valor **Repte**, la clau *K* i un vector inicial (*VI**) diferent del que s'ha utilitzat en el pas anterior. L'estació envia la **Resposta'** al punt d'accés, juntament amb el vector inicial *VI** utilitzat per a generar-la.

4) El punt d'accés calcula **Resposta** utilitzant l'algorisme WEP amb la clau compartida, el valor **Repte** que ha enviat a l'estació i el valor *VI** que ha rebut de l'estació. Si tots dos valors (**Resposta** i **Resposta'**) coincideixen voldrà dir que l'estació ha estat correctament autenticada i el punt d'accés enviarà un missatge per a indicar-ho. En cas contrari, el resultat de l'autenticació serà fallit.

El procés es repeteix per a autenticar el punt d'accés.

En l'actualitat, l'augment de la potència de càlcul permet desxifrar WEP en pocs minuts usant atacs estadístics. Per vèncer aquest tipus d'atacs es va crear el sistema WPA. WPA implementa la majoria de l'estàndard IEEE 802.11i. WPA implementa el TKIP (*Temporal Key Integrity Protocol*), que canvia claus dinàmicament a mesura que el sistema és utilitzat. També usa un vector d'inicialització de 48 bits. Després es va presentar WPA2, que ja implementava totalment l'estàndard IEEE 802.11i.



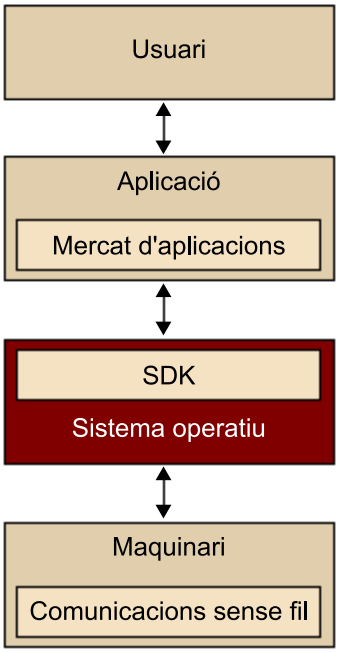
En l'actualitat, l'augment de la potència de càlcul permet desxifrar WEP en pocs minuts usant atacs estadístics. Per vèncer aquest tipus d'atacs es va crear el sistema WPA. WPA implementa la majoria de l'estàndard IEEE 802.11i. WPA implementa el TKIP (*Temporal Key Integrity Protocol*), que canvia claus dinàmicament a mesura que el sistema és utilitzat. També usa un vector d'inicialització de 48 bits. Després es va presentar WPA2, que ja implementava totalment l'estàndard IEEE 802.11i.

3. Sistema operatiu

El sistema operatiu és la capa que hi ha entremig del maquinari i les aplicacions de programari. És qui s'encarrega de gestionar els recursos de maquinari del dispositiu i oferir serveis comuns per a facilitar la programació d'aplicacions.

Vegeu també

Aquest mòdul no pretén estendre's en el funcionament del sistema operatiu, sinó únicament identificar els mecanismes de prevenció bàsics que aquests presenten en dispositius mòbils. Per als que vulguin aprofundir en la matèria es recomana la lectura dels mòduls didàctics de l'assignatura de *Sistemes operatius* i de *Seguretat en sistemes operatius*. O algun dels llibres sobre el tema que s'inclouen en la bibliografia.



En els darrers anys la complexitat del sistema operatiu dels dispositius mòbils ha augmentat considerablement. S'ha passat de tenir sistemes molt simples a ser comparables als d'un ordinador. Aquest creixement ha fet que la seva seguretat passi a ser un requisit primordial, però l'obtenció d'aquesta seguretat en els sistemes operatius per a dispositius mòbils és complexa.

Multitasca

Multitasca o *multitasking* és la capacitat d'executar simultàniament diversos processos.

A l'inici, quan els dispositius mòbils no eren un centre multimèdia i d'entreteniment, els sistemes operatius per a mòbils eren bastant simples. De fet, en aquells dispositius que tenien com a funció principal trucar o enviar SMS, el sistema operatiu tenia poca importància. Això era així ja que aquells primers sistemes operatius tenien com a funció principal ser compactes, eficients i fiables. En canvi, les funcions addicionals que aquests poguessin oferir eren secundàries. Però com que eren sistemes tan limitats en recursos físics i en funcionalitats no eren d'interès per als atacants.

En canvi, actualment quan parlem d'un sistema operatiu per a mòbils ens referim a un sistema complex, el qual conté característiques que fins fa uns anys eren impensables, com executar aplicacions 3D, navegar pel Web o multitasca. Aquestes noves funcionalitats obren més vies d'atacs i augmenten l'interès dels atacants.

Actualment, la majoria de mòbils fan servir com a sistema operatiu versions d'Android, o iOS per als dispositius Apple.

El principal problema dels sistemes Android és que molts dispositius no permeten l'actualització de la versió de sistema operatiu, amb la qual cosa no poden millorar les seves mesures de seguretat, ni eliminar les vulnerabilitats detectades en versions prèvies.

Hi ha els mòbils coneguts com ultrasegurs. Aquests dispositius compten amb implementacions propietàries de sistemes operatius amb un nivell molt alt d'encriptació i moltes mesures d'autenticació. Un exemple és el GranitePhone.

GranitePhone

http://www.sikur.com

3.1. Atacs

Les principals amenaces que hi ha pel que fa al sistema operatiu són causades per errors en l'aïllament dels recursos, sia pels dissenys que tenen, per errors en el programari o per una mala configuració dels serveis.

Exemple d'atac

En certes circumstàncies, un procés podria modificar els paràmetres ja verificats per un altre procés, però que encara no ha utilitzat. Les conseqüències d'aquest atac són imprevisibles, ja que el procés executarà operacions fent servir paràmetres per als quals no ha estat dissenyat.

Aquestes vulnerabilitats poden ser aprofitades per a executar atacs tant des dels serveis que ofereix el sistema operatiu mateix, com des de la capa d'aplicacions.

Si l'atac es fa sobre un servei del sistema operatiu, les conseqüències d'aquest dependran de la vulnerabilitat exposada. Una vulnerabilitat que només es pot explotar localment és molt menys crítica que una que es pugui explotar remotament.

Vegeu també

Les vulnerabilitats aprofitables des de la capa d'aplicacions les tractarem a l'apartat 4.

D'altra banda, també circulen versions no oficials dels sistemes operatius mòbils, anomenades *ROM*. Aquestes poden ser còpies de les versions oficials dels sistemes operatius, o ROM personalitzades. A més, aquestes ROM personalitzades poden contenir codi maliciós.

Exemple

Un desenvolupador pot modificar una versió del sistema operatiu Android incloent-hi un enregistrador de teclat (*keylogger*) per a registrar les pulsacions del teclat. Posteriorment, aquestes dades registrades són enviades a l'adreça electrònica del desenvolupador. Si aquest desenvolupador penja aquesta ROM personalitzada d'Android i altres usuaris la instal·len al seu dispositiu, el desenvolupador començaria a rebre dades confidencials d'aquests usuaris.

Enregistrador de teclat

Un enregistrador de teclat és una aplicació encarregada d'emmagatzemar totes les pulsacions de teclat.

3.2. Mecanismes de prevenció

Com ja hem vist, els recursos i la informació que gestiona el sistema operatiu poden estar en risc. Per tant, és important veure de quins mecanismes de seguretat disposen els sistemes operatius per a dispositius mòbils. Els mecanismes de seguretat més importants són els privilegis d'usuari, l'aïllament de processos i les actualitzacions.

3.2.1. Privilegi d'usuaris

Superusuari

El superusuari en molts sistemes operatius és conegut com a *root*.

Una de les característiques que acostumen a tenir aquests sistemes operatius és la gestió d'usuaris i privilegis, i tenen com a mínim dos usuaris: l'usuari normal i el superusuari. Aquesta distinció d'usuaris, tan comuna en ordinadors, *a priori* pot semblar estranya en un dispositiu mòbil, ja que no tenim el concepte d'iniciar sessió, però és molt important per a temes de seguretat.

Un sistema operatiu que gestioni diversos usuaris i privilegis pot aportar robustesa al sistema, ja que els danys que un atac pugui causar estan lligats als permisos de l'usuari que estigui efectuant aquest atac. Un usuari amb privilegis limitats tindrà un impacte baix sobre el sistema, mentre que un superusuari podrà produir una pèrdua total del sistema operatiu.

Generalment totes les aplicacions s'executen amb els privilegis de l'usuari normal, i es limiten molt els canvis o desperfectes que l'usuari pot causar al sistema. Per una banda això és molt important, ja que en cas d'haver-hi una vulnerabilitat, els danys que es podran produir estaran limitats pels privilegis que tingui l'usuari. Per altra banda, però, també és una limitació per a l'usuari, ja que aquest únicament podrà efectuar les accions que el sistema operatiu li permeti fer amb els privilegis actuals.

Usuaris del sistema iOS

L'iOS distingeix com a mínim entre dos usuaris, *root* i *device*. L'usuari *root* és un superusuari, mentre que l'usuari *device* té permisos limitats, encara que té accés a totes les nostres dades emmagatzemades. En els orígens d'aquest sistema operatiu, totes les aplicacions s'executaven com a *root*, amb accés total de l'aplicació sobre el dispositiu, alhora que posava en perill tot el dispositiu. Una fallada d'una aplicació podia tombar el sistema. I una aplicació maliciosa tenia total disponibilitat per a produir el seu atac. Afortunadament, en les primeres actualitzacions de l'iOS es va corregir aquest funcionament, i les aplicacions s'executen ara amb l'usuari *device*.

Per tant, per defecte l'usuari no té mai permisos de *root*. Però això limita molt les operacions que aquest pot fer sobre el sistema operatiu. Per exemple, únicament pot instal·lar aplicacions des del seu mercat d'aplicacions i restringeix molt les personalitzacions sobre l'iOS. A causa d'això, el terme *jailbreak*[7] s'ha fet famós. Aquest procés permet obtenir l'usuari *root* al sistema. Amb aquests nous privilegis s'eliminen les limitacions mencionades abans, però aquestes noves característiques poden portar a una reducció de la seguretat del sistema.

Tenir més control sobre el sistema operatiu no significa necessàriament que es redueixi la seguretat si se sap exactament què s'està fent, però de totes maneres és més fàcil deixar-se una porta oberta, o que alguna part contingui algun forat de seguretat. A més,

(7)Fer *jailbreak* és una pràctica legal als Estats Units des del 2010.

és important canviar les contrasenyes dels usuaris. Per defecte, tant l'usuari *root* com el *device* tenen una contrasenya coneguda.

És important recordar que els sistemes operatius mòbils utilitzen una autenticació basada en usuari i contrasenya. Per tant, si és possible és recomanable canviar la contrasenya amb la qual vénen per defecte.

A més, com a usuaris d'un sistema operatiu mòbil únicament hem d'activar els serveis que necessitem en aquell moment i sabent el que estan fent. D'aquesta manera estarem prevenint possibles atacs al nostre dispositiu.

Usuaris del sistema Android

A Android és molt més habitual que els usuaris es facin *root* en els seus dispositius. Amb això accedeixen a beneficis com millorar el rendiment en dispositius de gamma baixa, instal·lar bloquejadors d'anuncis, etc. En realitzar aquesta acció deixen els dispositius en risc davant multitud d'atacs, encara que després s'instal·lin contramesures com les *apps* SuperSU o Supersuser, que intenten controlar quines aplicacions accedeixen a capacitats que necessiten permisos de *root*.

3.2.2. Aïllament de processos

Una altra mesura que s'està implementant en sistemes operatius mòbils és limitar els permisos que té cada aplicació, aïllant-les. D'aquesta manera, cada aplicació únicament tindrà accés als seus recursos i no podrà pertorbar el funcionament de cap altra. En cas que s'hagi d'accedir a algun recurs compartit, com pot ser una regió de memòria, l'aplicació ha de tenir validat el permís per a fer-ho. D'aquesta manera podrà accedir a aquells recursos sobre els quals tingui permès l'accés.

Aquest aïllament de processos[8] acostuma a estar implementat fent servir un llenguatge de programació que habiliti aquest aïllament de processos, com és Java, i creant per a cada aplicació un nou usuari amb privilegis molt restringits, de manera que permet únicament accés als recursos a què hagi sol·licitat accés. D'aquesta manera, si una aplicació sol·licita únicament accés a la posició mitjançant GPS, aquesta no es podrà connectar a Internet.

(8)En anglès, *sandbox*.

Aïllar l'execució de cada aplicació garanteix que aquestes no poden interferir en el funcionament de les altres, de manera que fa el sistema operatiu molt més robust. De totes maneres, quan diverses aplicacions han de compartir algun servei s'ha de fer servir un sistema de permisos més complex. La bona implementació d'aquest aïllament i la gestió dels recursos compartits és fonamental perquè aquesta mesura sigui efectiva.

ART (Android Runtime)

Les aplicacions en Android s'executen sobre ART (Android Runtime) d'una manera semblant a com es fa en Java. A més, cada aplicació s'executa amb un usuari i grup de Linux diferent. Això fa que per defecte les aplicacions no tenen permís per a fer cap tasca que pugui interferir en les altres aplicacions. Això requereix fer servir uns permisos de seguretat més acurats i restringits que els fets servir generalment en Linux, que permeten especificar quines operacions pot executar aquella aplicació i un permís basat en una direcció URI[9] per a personalitzar l'accés a part de les dades. Aquests permisos són estàtics i els defineix el desenvolupador al fitxer de configuració *AndroidManifest.xml*. Aquests permisos han de ser acceptats per l'usuari quan instal·la l'aplicació en dispositius amb versions d'Android anteriors a Marshmallow. Des d'Android Marshmallow el programador és el responsable de demanar el permís en el moment en què vagi a fer servir la capacitat desitjada. Alguns d'aquests permisos són fer una trucada telefònica, modificar/esborrar dades de la targeta de memòria, llegir els números de telèfon de la nostra agenda o obtenir la informació del GPS.

(9)*URI* és l'acrònim de *uniform resource identifier* (identificador uniforme de recursos). Consisteix en una cadena curta de caràcters que identifica inequívocament un recurs.

3.2.3. Actualitzacions

Addicionalment, aquests sistemes operatius disposen d'actualitzacions periòdiques. En cas d'actualitzacions menors, aquestes acostumen a ser freqüents per a solucionar alguna carència detectada, generalment degudes a errors en el programari que presenten un risc en la seva seguretat. La manera de rebre aquestes actualitzacions difereix en cada sistema. Hi ha sistemes que la poden rebre mitjançant la comunicació sense fils, a través de l'aire[10] (OTA), quan el dispositiu es connecta amb cable a l'ordinador o mitjançant la memòria externa que incorporen.

(10)En anglès, *over-the-air*.

iTunes

L'iOS utilitza el reproductor iTunes per a sincronitzar les dades del dispositiu. A més, aquest permet fer actualitzacions de seguretat sobre el sistema operatiu d'una manera ràpida i transparent a l'usuari.

A més, els sistemes operatius també ofereixen actualitzacions majors, les quals, a més de solucionar errors en el programari, afegeixen noves funcionalitats i en milloren el rendiment. Com que aquestes actualitzacions duen a terme grans canvis en el sistema, algunes fan un esborrament complet del dispositiu. Això comporta que tota la informació personal serà esborrada. Per tant, és molt important que abans de dur a terme una actualització s'hagi fet una còpia de seguretat de tot el sistema, i en particular de les dades personals, per a restaurar-les posteriorment en el nou sistema.

Finalment, també és important que les ROM dels sistemes operatius per a dispositius mòbils es baixin de llocs de confiança. Algunes d'aquestes ROM són personalitzades i poden contenir codi maliciós.

3.3. Cas d'estudi: SSH en l'iOS

Un dels primers casos en què molts dispositius mòbils van quedar exposats a accés remot no autoritzat per part d'atacants es va donar en l'iOS, per una mala configuració per part dels usuaris del servei d'SSH.

SSH

SSH són les sigles de *secure shell*, que és el nom d'un protocol i el programa que l'implementa, i serveix per a accedir a màquines remotes a través de la xarxa.

En algun dels mètodes per a obtenir a accés de *root* a l'iOS, mitjançant *jailbreak*, s'instal·la el servei d'SSH. La configuració per defecte d'aquest servei permet accedir remotament al dispositiu mòbil amb l'usuari *root*. Això és perquè l'usuari *root* ve per defecte amb una contrasenya coneguda: *alpine*. D'aquesta

manera, qualsevol dispositiu amb iOS que tingui activat el servei d'SSH i amb la contrasenya de l'usuari *root* per defecte pot ser controlat remotament quan està connectat a una xarxa sense fils oberta.

Una manera addicional d'activar el servei d'SSH en l'iOS és mitjançant la instal·lació del paquet OpenSSH. La configuració per defecte del servei és la mateixa, i es manté el problema de seguretat mencionat.

Però la solució a aquest problema de seguretat és ben senzilla: una configuració correcta en el mecanisme d'autenticació del servei d'SSH. Aquesta configuració és tan fàcil com canviar la contrasenya amb la qual ve per defecte l'usuari *root*. Aquest procés requereix un seguit de passos:

1) Baixar i instal·lar una aplicació que faci de terminal de línia d'ordres. Un exemple és l'aplicació MobileTerminal.

2) Accedir a l'aplicació de terminal de línia d'ordres.

3) Obtenir permisos de *root* introduint l'ordre *su root* i la contrasenya *alpine*.

```
Leanders-iPhone-3GS:~ mobile$ su root
Password:
```

4) Canviar la contrasenya mitjançant l'ordre *passwd*. Després s'ha d'introduir dos cops la nova contrasenya.

```
Leanders-iPhone-3GS:/var/mobile root# passwd
Changing password for root.
New password:
Retype new password:
```

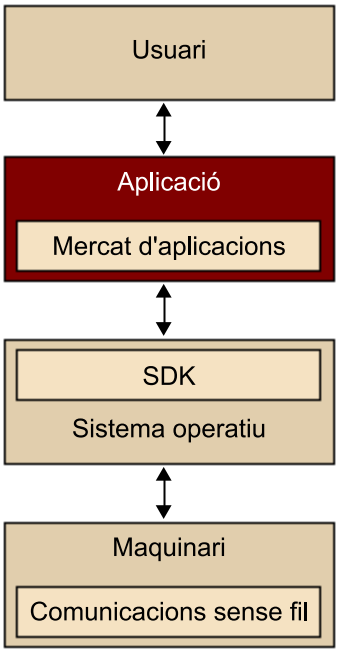
Un cop seguits aquests passos, el servei SSH del dispositiu mòbil queda protegit per la nova contrasenya introduïda.

És molt important la configuració correcta de tots els serveis activats en el sistema operatiu del dispositiu mòbil; tenen més importància els que permeten accessos remots al dispositiu.

4. Aplicacions

Un dels components més importants en els dispositius mòbils són les aplicacions que s'hi puguin executar, ja que serà amb el que interactuaran els usuaris.

En aquest nivell és molt important revisar les mesures de seguretat que s'han pres perquè les aplicacions no puguin desestabilitzar el sistema. Òbviament, aquestes mesures estan complementades per totes les que hi ha a les capes inferiors. Però les vulnerabilitats que es detectin en aquest nivell són crítiques, ja que podran ser usades directament per les aplicacions.



4.1. Atacs

Els atacs a la capa d'aplicacions els dividirem en dos tipus: els atacs que es poden executar des de qualsevol tipus d'aplicació i els atacs que es poden efectuar únicament des del navegador web, ja que aquesta aplicació és molt potent però alhora un punt crític en la seguretat d'aquests sistemes.

4.1.1. Atacs al programari: programari maliciós

Quan parlem del programari també és important revisar les diferents amenaces que aquest pot patir. Ens centrarem en el programari maliciós, també anomenat *malware*[11], i revisarem els diferents objectius que aquest pot tenir.

(11)La paraula *malware* ve de l'ajuntament de les paraules angleses ***mal****icious soft****ware***.

Un programari maliciós és una aplicació de programari que té un objectiu maliciós al dispositiu mòbil on s'instal·la i s'executa sense el consentiment del propietari. Pot tenir objectius molt diversos, i els més comuns són obtenir dades personals i benefici econòmic. El mode de funcionament que té pot ser automàtic o controlat remotament. Els principals tipus de programari maliciós són:

- **Virus**. És un programa maliciós que infecta altres arxius del sistema amb la intenció de modificar-los o fer-los inservibles. Un cop un arxiu ha estat infectat, aquest també és portador del virus i, per tant, una nova font d'infecció. Per tant, perquè un virus es propagui aquest ha de ser executat per l'usuari. Generalment té un objectiu ocult, com pot ser obtenir contrasenyes o fer un atac de denegació de servei.

- **Cuc**. És un programa maliciós autoreplicable, que aprofitarà vulnerabilitats en la xarxa per a propagar-se. Igual que el virus, generalment té un objectiu ocult.

- **Troià**[12]. És un petit programa ocult en una altra aplicació. L'objectiu que té és passar inadvertit per a l'usuari i instal·lar-se en el sistema quan l'usuari executa l'aplicació. Un cop instal·lat pot fer diversitat d'accions, però totes sense el consentiment de l'usuari. A més, aquestes accions es poden fer instantàniament o estar fixades per a fer-se en un futur.

(12)El nom *troià* ve de les similituds amb el cavall de Troia.

- **Porta secreta**[13]. És un programa que té l'objectiu d'obrir un accés a l'ordinador per al desenvolupador del programari maliciós, ignorant el procés normal d'autenticació. Això comporta que el dispositiu mòbil infectat pot ser controlat remotament per l'atacant.

(13)En anglès, *backdoor*.

- **Programari espia (*spyware*)**. És una aplicació que recull informació sobre una persona o organització sense el seu consentiment. Generalment, l'objectiu final d'aquesta informació recopilada és vendre-la a empreses de publicitat.

- **Enregistrador de teclat**. És una aplicació encarregada d'emmagatzemar totes les pulsacions de teclat. Per tant, pot capturar informació sensible com és el número de la targeta de crèdit o les contrasenyes.

- ***Hijacker***. És un programa que fa canvis en la configuració del navegador web. Un atac típic és canviar la pàgina inicial per una pàgina de publicitat.

- ***Dialer***. Són programes que d'una manera oculta fan trucades a telèfons amb tarifes especials. D'aquesta manera, l'atacant pot obtenir beneficis econòmics.

- ***Ransomware***. És un tipus específic de troià que bloqueja el dispositiu bé afegint una pantalla de bloqueig, canviant la contrasenya o xifrant el sistema de fitxers. Normalment el programari maliciós demana un rescat econòmic per a alliberar el dispositiu o desxifrar les dades.

Parlar de programari maliciós en ordinadors és normal avui dia, però no ho és tant quan ens referim a dispositius mòbils. Però, de fet, és normal que com més s'assemblen els dispositius mòbils als ordinadors, més vulnerabilitats comparteixin.

En un principi, els pocs programes maliciosos que hi havia per a dispositius mòbils eren més una prova de concepte que un codi maliciós real. Això era així perquè les dades personals que es desaven al mòbil eren molt poques i era difícil poder treure benefici econòmic d'alguna activitat maliciosa. Així i tot hi va haver aplicacions malicioses que aconseguien benefici a força d'enviar SMS a serveis publicitaris dels desenvolupadors mateixos del programari maliciós.

Cabir

El primer programari maliciós destinat a dispositius mòbils complexos va ser el Cabir, detectat el juny del 2004. Aquest va ser desenvolupat com una prova de concepte per a demostrar que era possible contagiar SymbianOS. La característica destacable d'aquest programari maliciós era que es podia propagar mitjançant Bluetooth. Va ser l'inici d'una era.

Ara, el programari maliciós té una gran perillositat i possibilitats per a estafar-nos, principalment perquè els usuaris som molt més vulnerables quan fem servir dispositius mòbils, ja que no prenem les mateixes mesures que prenem quan som davant d'un ordinador.

A hores d'ara, s'ha trobat programari maliciós en les diferents plataformes. La perillositat d'aquest programari maliciós augmenta a causa del desconeixement per part dels usuaris dels possibles perills als quals estan sotmesos els dispositius mòbils.

DroidDream en l'Android

En l'Android un dels primers programaris maliciosos que es va trobar va ser el DroidDream. Va ser trobat en moltes aplicacions del Google Play. El principal propòsit que tenia era recopilar informació sobre el dispositiu infectat, com l'identificador de l'usuari, el tipus de dispositiu, el llenguatge o la regió. Posteriorment, aquesta informació era enviada a un servidor remot. Però els objectius maliciosos que tenia no acabaven aquí. Mitjançant *exploits*[14], podia obtenir permís de *root* en algunes versions del sistema operatiu i a partir d'aquí trencar l'aïllament de l'aplicació i baixar codi maliciós des d'un servidor remot. De fet, aquest programari maliciós quedava a l'espera per a rebre ordres d'un servidor extern, i podia executar qualsevol acció sobre el sistema.

[14]Un *exploit* és una peça de programari que automatitza l'aprofitament d'una vulnerabilitat.

Symantec Mobile AV

Anteriorment al 2016, les comprovacions abans de publicar una *app* a Google Play eren molt menys exhaustives. Era possible publicar una aplicació amb un nom, icona i aparença gràfica molt similar a una altra famosa, i era un exemple de *malware* en moltes ocasions del tipus *ransomware*. Un exemple va ser el *masquerade* sobre el Symantec Mobile AV. Simulava ser un antivirus i en realitat era un *malware* del tipus *ransomware*, que

bloquejava el dispositiu i demanava un rescat econòmic de cinc-cents dòlars per tornar el control.

Ikee.A en els iPhone

En l'iOS, el 2009 va aparèixer Ikee.A, el primer cuc per als iPhone. Aquest va tenir diverses versions. La primera versió va ser únicament una prova de concepte, que canviava el fons d'escriptori. Les versions posteriors van ser molt més perilloses, i permetien enviar la informació confidencial de l'usuari a un servidor remot o el control a distància. Aquest cuc únicament afectava els iPhones que havien obtingut permisos de *root* mitjançant el *jailbreak* i que després d'instal·lar el servei d'SSH no havien canviat la contrasenya que tenien per defecte. Després, es propagava per la xarxa buscant més víctimes.

Vegeu també

El problema de la seguretat del protocol SSH s'ha descrit en el subapartat 3.3.

Una pràctica molt comuna a l'hora de desenvolupar programari és la de reutilitzar trossos de programari d'altres desenvolupadors, com per exemple utilitzar biblioteques externes. Aquesta situació fa que els desenvolupadors puguin no conèixer el 100% del codi font del seu programa. Això fa que un programa pugui ser compromès perquè fa servir una biblioteca externa que conté codi maliciós.

Un dels pocs factors que juga a favor dels usuaris és la diversitat de tecnologies mòbils que es fan servir. Aquestes diferents tecnologies requeriran que els desenvolupadors de programari maliciós hagin d'escriure un codi per a cada plataforma, cosa que en pot frenar la velocitat de propagació.

4.1.2. Atacs al Web

A continuació veurem una petita descripció de les principals vulnerabilitats que poden afectar els navegadors web i els mecanismes de seguretat existents. D'aquesta manera és possible fer-se una idea de fins a quin punt podem ser vulnerables davant d'aquests atacs, i que s'ha d'anar amb molt de compte quan es navegui pel Web.

Vegeu també

Aquest mòdul no pretén estendre's en el funcionament del Web ni dels diversos atacs que s'hi poden fer. Per als que vulguin aprofundir en la matèria es recomana la lectura dels mòduls didàctics de l'assignatura de *Seguretat en aplicacions web*. O algun dels llibres sobre el tema que s'inclouen en la bibliografia.

Encara que hi ha una gran llista d'atacs que afecten les pàgines web, únicament ens centrarem en els dos que més rellevància tenen quan parlem de dispositius mòbils: el falsejament d'identitat (*web spoofing*) o pesca (*phishing*), i el *clickjacking*.

Falsejament d'identitat o pesca (*web spoofing* o *phishing*)

El falsejament d'identitat o pesca (*web spoofing* o *phishing*) és un tipus d'atac que consisteix a suplantar una pàgina web i a partir d'aquí intentar obtenir informació confidencial de manera fraudulenta. Aquesta informació acostumen a ser contrasenyes o informació bancària, com poden ser les targetes de crèdit.

L'estafador o atacant pot suplantar una pàgina web de moltes maneres, i la més comuna és utilitzant una adreça web molt semblant a l'original. La pàgina web fraudulenta tindrà una estructura idèntica a l'original, perquè l'usuari no pugui detectar a primer cop d'ull que està essent víctima d'aquest tipus d'atac.

A més, aquestes pàgines web fraudulentes demanaran informació confidencial de l'usuari que teòricament no haurien de demanar, com pot ser el número de la teva targeta de crèdit.

Una altra estratègia consisteix a imitar el format dels missatges del sistema operatiu o d'alguna aplicació, avisant d'una falsa actualització o d'alguna acció que s'ha de realitzar. Si l'usuari no se n'adona, pot facilitar les seves dades d'accés o bé instal·lar programari maliciós al seu dispositiu.

Per tant, per a l'usuari és difícil detectar aquest tipus d'atac, ja que podeu arribar a la pàgina web suplantada per mitjà d'un enllaç i l'única diferència que podríeu detectar a simple cop d'ull és l'adreça web. A més, el problema s'agreuja perquè els dispositius mòbils disposen d'una pantalla limitada, cosa que fa que pugui ser difícil veure l'adreça web completa.

De totes maneres, com a usuaris hem de saber que mai no hem d'introduir informació confidencial que una pàgina web no ens hauria de demanar. Per defecte hem de desconfiar sempre. En aquest tipus d'atac és clau estar totalment pendent del que es fa. Qualsevol distracció ens pot portar a ser estafats.

Exemple de pesca

Al correu electrònic ens arriba un enllaç a la nostra pàgina bancària dient-nos que hem d'actualitzar les nostres dades de la targeta de crèdit perquè han aplicat una nova política de seguretat per a evitar estafes. A la part inferior hi ha el logotip del banc, el qual, en lloc d'apuntar a http://www.bancdeprova.es apunta a http://www.bancdaprova.es. Si decidim pitjar l'enllaç, ja som un pas més a prop de ser estafats.

Un cop dins el web veiem que la pàgina és extremament similar al web original, fins al punt que és imperceptible la diferència. Un cop aquí ens demana omplir un formulari en què ens demana tant el número de seguretat de la targeta (els tres números de la part posterior) com una actualització de les nostres dades, incloent-hi la contrasenya. Suposem que no ens adonem que hem anat a una pàgina fraudulenta, i no desconfiem de les dades que ens demana. Per tant, omplim el formulari. En aquest punt ja no hi ha marxa enrere. L'atacant ha obtingut les nostres dades bancàries i intentarà treure'ns diners per tal de rendibilitzar els seus atacs.

Quan es tracta amb dades bancàries l'atenció és clau. Els atacants intentaran aprofitar que estem ocupats, amb pressa o distrets. També jugaran amb el fet que som massa crèduls. Abans de seguir cap enllaç amb el navegador mòbil, ens hem d'assegurar que enllaça al lloc correcte. Si no n'estem segurs no l'hem de seguir. Sempre que sigui possible s'ha d'accedir al web escrivint manualment l'adreça del web i sobretot vigilar els enllaços que ens arribin per correu electrònic. La petita pantalla del dispositiu sumada a la falsa sensació de seguretat en dispositius mòbils ens pot jugar una mala passada.

Clickjacking

El *clickjacking* és una tècnica que enganya l'usuari perquè aquest premi sobre elements d'un lloc web en els quals no ho faria voluntàriament. Això s'aconsegueix superposant dues pàgines. La principal és la que conté un ele-

ment que a l'atacant l'interessa que pitgem, com pot ser la confirmació de l'habilitació d'un permís. L'altra és la que ens enganya, i està superposada a l'altra. Òbviament, aquesta pàgina superposada ha de tenir elements que ens incentivin a pitjar els botons que a l'atacant l'interessa, com pot ser algun tipus de joc.

Sense entrar massa en detall, aquesta tècnica es basa en la superposició d'*iframes*. Aquests són elements HTML que permeten la inclusió d'un recurs extern dins de la nostra pàgina. I encara que tenen una sèrie de limitacions a l'hora d'accedir-hi mitjançant JavaScript, és possible utilitzar-los per a enganyar els usuaris.

4.2. Mecanismes de prevenció

En la capa d'aplicació tractarem diversos mecanismes de prevenció. Començarem veient com s'ha creat una primera capa de seguretat fent servir els mercats d'aplicacions. A continuació, veurem mecanismes de seguretat que es poden fer servir al Web. Finalment, descriurem diversos tipus d'aplicacions que poden augmentar el nivell de seguretat en els dispositius mòbils.

4.2.1. Mercat d'aplicacions

En els dispositius mòbils actuals quasi tota la seguretat s'ha centrat a crear un punt centralitzat i fiable per a baixar i gestionar les aplicacions. Això s'ha anomenat *mercat d'aplicacions*. Cada mercat d'aplicacions pot tenir polítiques més o menys restrictives, sia del tipus de contingut, o de la perillositat potencial que tenen. De totes maneres, a grans trets es poden dividir en dos grups:

- Mercats que permeten totes les aplicacions, indiferentment de qui les hagi publicat i de la funcionalitat que tinguin.
- Mercats que tenen un control per a limitar les aplicacions que seran accessibles. Això està lligat a l'existència d'un procés previ de revisió.

El primer grup crea un lloc central de distribució d'aplicacions però es desentén de les conseqüències que pugui tenir una aplicació baixada. Aquesta centralització facilita a l'usuari l'accés a aquestes aplicacions, però *a priori* no afegeix cap mesura de seguretat. De totes maneres, aquests sistemes poden tenir sistemes de valoració de les aplicacions, tant si són numèrics com en qualitat de mode de comentaris. Aquests sistemes aporten un grau de seguretat en el sentit que un cop detectada una aplicació maliciosa la comunitat mateixa la desprestigiarà i perdrà rellevància. De totes maneres, hi pot haver aplicacions malicioses que no s'hagin descobert i que, per tant, continuïn tenint una valoració positiva.

Google Play

Android pertany al grup de mercats que permeten totes les aplicacions. Té el mercat d'aplicacions Google Play, el qual permet que qualsevol desenvolupador hi pugui allotjar la seva aplicació perquè els usuaris la baixin. Abans del 2016 no es realitzava cap com-

provació per part de Google. A causa dels nombrosos abusos, Google va iniciar una sèrie de comprovacions automàtiques i en alguns casos manuals abans que l'aplicació estigui disponible. De totes maneres, totes les aplicacions han de ser signades amb un certificat, la clau pública del qual pertany al desenvolupador. Amb aquest mecanisme s'autentica d'una manera segura el desenvolupador. A més, disposa tant de valoració numèrica com de comentaris per a cada aplicació. Finalment, hi ha la possibilitat que Google retiri alguna aplicació del mercat si en algun moment arriba a coneixement seu que és maliciosa. I fins i tot, poden desinstal·lar aplicacions remotament. Addicionalment, les aplicacions que no siguin a Google Play es poden instal·lar d'una manera senzilla.

I com ja s'ha comentat abans, Android afegeix una capa de seguretat que limita els accessos que una aplicació pot fer al sistema operatiu per mitjà de permisos. Aquests permisos se sol·liciten bé en el moment de la instal·lació (versions d'Android anteriors a Marshmallow), o bé en el moment del seu ús (versions més actuals). Si una aplicació no demana els permisos corresponents, no els podrà utilitzar. Aquesta política depèn de la intervenció de l'usuari, però és molt potent a l'hora de limitar els danys que cada aplicació pot causar. Per exemple, una aplicació per a controlar la velocitat a la qual ens movem no necessita veure els nostres missatges.

En canvi, el segon grup de mercats crea un lloc central de distribució en el qual exerceix un control sobre la qualitat i el contingut. Aquest control elimina aplicacions que puguin causar un mal funcionament del sistema o que directament siguin malicioses. El problema és que cada aplicació ha de ser revisada a fons abans de ser publicada, cosa que n'alenteix la publicació. A més, no sempre és fàcil revisar una aplicació a fons, i veure si el que està fent és maliciós o no. Desafortunadament, aquesta revisió pot portar a una mena de censura i que únicament es publiquin les aplicacions que la companyia cregui que són acceptables.

AppStore

L'iOS de Apple incorpora l'AppStore, un mercat d'aplicacions basat en aquesta segona opció, el qual exerceix un control total sobre les aplicacions que poden ser baixades al dispositiu. Per això, cada aplicació és revisada a fons. Però revisar a fons una aplicació no és sempre fàcil, i de fet, s'ha trobat casos en què aplicacions que deien que feien una cosa, per sota en feien una altra d'addicional. Per exemple, una aplicació que deia que era una llanterna, per sota habilitava el *tethering*, és a dir, compartir la connexió mòbil del dispositiu per mitjà de connexió sense fils, acció no permesa per la companyia. Per tant, quan l'aplicació va ser popular, va ser eliminada de l'AppStore.

A més, per defecte l'iOS no permet instal·lar aplicacions d'altres fonts. Per a fer-ho s'ha d'habilitar l'usuari *root* al sistema per mitjà del mètode abans mencionat *jailbreak*.

Aquests mercats d'aplicacions també poden permetre fer una actualització de les aplicacions. Aquesta tasca s'ha de fer periòdicament, ja que les noves aplicacions, a banda de millores en rendiment i funcionalitat, acostumen a solucionar vulnerabilitats detectades que podrien ser explotades.

Actualització d'aplicacions Android

L'Android permet fer una actualització automàtica de les seves aplicacions mitjançant Google Play. De totes maneres, no totes les aplicacions es poden actualitzar automàticament. Per exemple, les aplicacions que han canviat els seus permisos respecte de l'aplicació anterior requeriran la interacció de l'usuari perquè aquest accepti els nous permisos.

A més, les companyies també es reserven el dret d'eliminar a distància i automàticament qualsevol aplicació considerada com a perillosa, actuació que assegura una eliminació ràpida de l'aplicació un cop s'ha trobat com a nociva.

Un cas especial són les aplicacions que ens cobren internament per determinats serveis, com pot ser desbloquejar un nou nivell a un joc. En aquest cas la seguretat estarà marcada per la manera com gestioni les dades bancàries cada aplicació i els mecanismes de prevenció que implementi internament.

4.2.2. Navegador web

Per defecte, tots els sistemes operatius porten una aplicació encarregada de la navegació web. Encara que aquest punt no ens pugui semblar crític en la seguretat del sistema, l'experiència en els ordinadors corrobora que sí que ho és.

Per tant, és molt important que tractem aquesta aplicació amb tant respecte com la tractem en l'ordinador. Això és perquè són aplicacions que poden executar codi molt complex. Els navegadors executen codi a escala d'usuari, amb el nivell de privilegis que aquest tingui establert. Els codis que s'executen són potencialment perillosos a causa de la gran quantitat de funcionalitats que s'hi poden implementar. Els llenguatges més utilitzats són HTML/DHTML i JavaScript. A més, el contingut multimèdia pot ser directament obert des d'aquí, executant altres aplicacions, les quals també poden tenir vulnerabilitats.

De totes maneres, no hi ha cap protecció a escala d'usuari que sigui infal·lible, ja que hi ha tècniques per a fer atacs de *man in the middle* (MiM), que no depenen de la intervenció de l'usuari, que, per tant, no tindrà la possibilitat d'evitar l'èxit de l'atac. Per tant, s'han de vigilar les pàgines a les quals s'accedeix i les execucions de codi, com per exemple JavaScript.

Vulnerabilitat de les BlackBerry

En el navegador web de les BlackBerry es va trobar un error de programari al motor de renderització que permetia l'execució remota de codi. Aquesta vulnerabilitat es produïa quan l'usuari accedia a un web que l'atacant havia dissenyat malintencionadament. Un cop s'havia accedit al web, l'atacant era capaç de llegir i escriure a la secció d'emmagatzematge de la memòria interna o a la targeta externa d'emmagatzematge.

A causa dels atacs de què són objecte les aplicacions web, s'han pres mesures per a intentar reduir-los, com per exemple fer servir HTTPS.

HTTPS és un protocol d'aplicació basat en HTTP, però destinat a l'accés segur a pàgines web. És utilitzat bàsicament per qualsevol servei que necessiti l'enviament de dades personals, com tendes virtuals o bancs.

Bàsicament, HTTPS pretén crear un canal segur sobre una xarxa insegura, garantint protecció contra atacs d'*eavesdropping* i *man in the middle*. Aquesta seguretat es basa a fer servir xifratge, certificats digitals i una autoritat de certificació, que actua com a tercera part de confiança[15], en la qual tant el web com l'usuari han de confiar.

(15) En anglès, *trusted third party* (TTP).

Perquè una connexió HTTPS sigui segura, s'ha de complir que:

- L'usuari confiï en l'autoritat de certificació.
- El lloc web proporcioni un certificat vàlid, signat per la mateixa autoritat de certificació en la qual confia l'usuari. I que aquest certificat identifiqui correctament el lloc web.
- El navegador web de l'usuari alerti quan detecta que hi ha un certificat invàlid.
- El protocol fet servir per al xifratge sigui de confiança.

4.2.3. Aplicacions de seguretat

Encara que fins ara hem vist les aplicacions com una font de vulnerabilitats, aquestes també poden contribuir a augmentar el nivell de seguretat del sistema. Hi ha diferents aplicacions que poden afegir noves capes de seguretat als dispositius mòbils, sia amb mètodes d'autenticació addicionals més restrictius, sistemes de còpia de seguretat[16], xifratge de les dades, aplicacions antivirus o tallafocs[17].

(16)En anglès, *backup*.

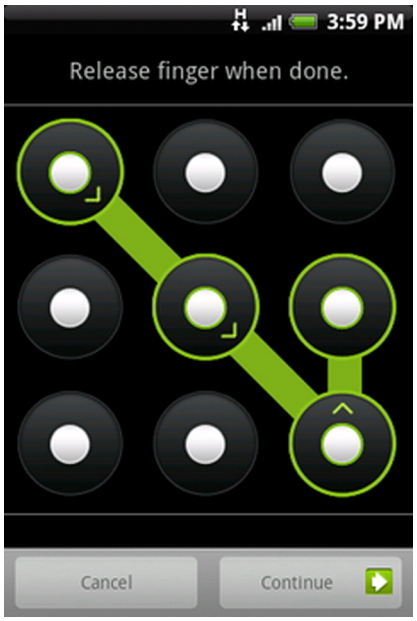
(17)En anglès, *firewall*.

Autenticació addicional

Per defecte els telèfons intel·ligents (*smartphones*) porten com a mínim una mesura d'autenticació com és el codi PIN, que s'ha d'introduir en iniciar el dispositiu. Però un cop el dispositiu està encès és comú fer servir més mètodes d'autenticació.

Algunes versions de l'Android incorporen el que anomenen *patró de desbloqueig*, que consisteix a dibuixar sobre la pantalla del dispositiu mòbil un patró que prèviament ha estat definit per a desbloquejar el mòbil. Aquesta mesura és poc intrusiva (triguem poc temps a introduir el patró). Per altra banda, els dispositius de gamma alta han incorporat control d'accés biomètric basat en empremta dactilar, reconeixement facial o escàner d'iris.

Exemple de patró de bloqueig de pantalla



Font: HTC

Exemple de control d'accés basat en empremta dactilar d'Apple (Touch ID)

Font: Kelvinsong - Own work, CC BY 3.0, https://commons.wikimedia.org/w/index.php?curid=29893016

Còpia de seguretat

Una de les accions imprescindibles quan treballem amb informació és la realització de còpies de seguretat. En els dispositius mòbils emmagatzemem molta informació, i el problema és que a vegades no és fàcil fer-ne una còpia de seguretat global, ja que cada aplicació pot emmagatzemar les dades internament, en una part concreta de la memòria. Per això, és important disposar d'una aplicació que faciliti i automatitzi aquest procés.

Titanium Backup

L'aplicació Titanium Backup de l'Android permet fer còpies de seguretat tant de les aplicacions instal·lades com de les dades que contenen. Això sí, aquesta aplicació requereix permisos de *root*.

Xifratge

Els dispositius mòbils poden emmagatzemar molta informació sensible, com poden ser documents confidencials o dades bancàries. Per això és interessant afegir una capa més de seguretat i xifrar aquestes dades. Això garanteix que en cas de pèrdua la informació sigui illegible per a algú no autoritzat.

Xifratge en l'iOS 8

Des d'iOS8, tota la informació del sistema de fitxers es troba xifrada per defecte. El nivell de xifrat de les dades d'una *app* es pot ajustar fent servir l'API[18] proporcionada per Apple. Aquest xifrat es va millorar en la versió iOS 10.3 amb el nou sistema de fitxers. L'aposta per la privacitat d'Apple li va portar molts problemes amb les autoritats dels Estats Units, que li demanaven mecanismes per a poder accedir als continguts dels seus dispositius, sobretot en casos de terrorisme.

[18] Són les sigles en anglès de *application programming interface*, que es tradueix com a interfície de programació d'aplicacions.

Antivirus

El programari maliciós ja és una realitat en els dispositius mòbils. Per tant, comencen a ser necessàries aplicacions que analitzin els fitxers per a evitar infeccions. Aquestes solucions poden heretar tota l'experiència adquirida en els ordinadors, i per tant, els antivirus més populars per als ordinadors estan traient versions per a dispositius mòbils.

AVG

AVG ha tret una versió del seu antivirus per a l'Android anomenada *AVG Anti-Virus Free*. Aquest permet escanejar el dispositiu buscant virus, revisar una aplicació a la recerca de programari maliciós abans de baixar-la i revisar el contingut d'una pàgina web, d'un correu electrònic o d'un SMS abans de baixar-lo al dispositiu.

Tallafocs

Com que els dispositius mòbils cada cop fan i reben més connexions amb dispositius externs, hi ha diverses solucions comunes als ordinadors com són els tallafocs que també es comencen a popularitzar en aquest entorn. Aquests programes permeten controlar les comunicacions.

4.3. Cas d'estudi: Zeus Man In The Mobile

El Zeus és un troià informàtic per a ordinadors que executen el Windows que té com a objectiu robar informació bancària mitjançant un enregistrador de teclat. Va ser detectat per primer cop el 2007 però la seva popularitat va augmentar el 2009, quan va infectar ordinadors de companyies importants. El Zeus ha estat usat per a crear grans xarxes de zombis (*botnet*). Bàsicament, el Zeus captura contrasenyes i dades bancàries dels ordinadors que ha infectat d'una manera oculta.

Xarxa de zombis (*botnet*)

Una xarxa de zombis (*botnet*) és un grup de dispositius connectats que un cop han estat infectats són controlats remotament per a fer tasques sense l'autorització del propietari.

Però Zeus ha avançat un pas més, i ha fet convergir el programari maliciós dels ordinadors i telèfons intel·ligents en un únic esquema, conegut com a *MITMO* (Man in the Mobile).

Actualment, molts bancs, a banda de l'autenticació tradicional d'usuari i contrasenya, ofereixen una segona autenticació que es basa a rebre un SMS amb un codi, el qual posteriorment hem d'introduir en fer una transacció, també conegut com a *TAN*[19]. I és aquí on Zeus ha vist una oportunitat per a fer un nou atac.

(19) *TAN* són les sigles de *transaction authentication number*.

Bàsicament Zeus fa servir tres tècniques per a obtenir el robatori d'informació:

- **Redirecció**: l'usuari és redirigit a un lloc web diferent de l'original, encara que visualment pugui ser una rèplica exacta. Tota la informació introduïda és emmagatzemada per l'atacant.

- **Captura**: mitjançant enregistradors de teclat o captures de pantalla.

- **Injecció**: injectant codi HTML al navegador web de l'usuari infectat, demanant dades que normalment l'entitat bancària no demanaria, com el codi de seguretat de la targeta de crèdit.

La tècnica més potent i popular és la d'injecció. Una de les últimes versions d'aquest troià utilitza la injecció de codi, un cop l'usuari ha estat autenticat al web del seu servei bancari, per a demanar-li el número de telèfon i el model del dispositiu mòbil. Aleshores, l'usuari rep al seu dispositiu mòbil un missatge amb un enllaç d'on es pot baixar una aplicació que diu que és complementària al sistema d'autenticació del seu banc.

Un cop s'instal·la l'aplicació al dispositiu mòbil, l'usuari ha estat infectat. Aquesta aplicació el primer que fa és enviar un SMS a un telèfon mòbil preestablert en què diu que l'aplicació ha estat correctament instal·lada. A continuació, monitora tots els missatges, i si vénen del número preestablert els analitza en busca d'ordres per executar i després els esborra. Les ordres permeten, entre altres coses, ignorar totes les peticions per SMS, canviar el número preestablert des d'on es controla i esborrar contactes.

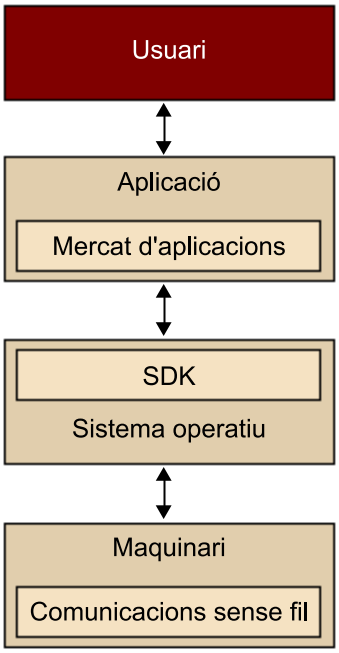
A causa d'aquest funcionament, tot el sistema és transparent a l'usuari, ja que aquest en cap moment no veu els missatges. A més, el Zeus també implementa funcionalitats per al reenviament de missatges SMS, amb la finalitat d'enviar els TAN usats com a segon factor d'autenticació per alguns bancs.

A més, com que el dispositiu infectat pot rebre ordres per SMS, produeix infeccions molt més robustes. No hi ha un punt central que pugui ser bloquejat per a parar tota la infecció. De totes maneres, cal recordar que la infecció ha estat deguda al fet que l'usuari ha instal·lat el programari maliciós a partir d'un

enllaç rebut. De fet, aquest atac no és més que un atac de pesca, però com s'ha comentat abans, la gravetat d'aquest procés s'accentua per la poca percepció per part dels usuaris dels riscos existents, i la perillositat que representen.

5. Usuari

En aquest apartat ens centrarem en les intrusions físiques al dispositiu mòbil per part d'un usuari, quan s'ha tingut accés físic al dispositiu mòbil. Quan parlem d'intrusió física ens referim al fet que algú ha tingut accés físic al dispositiu. Aquest tipus d'intrusió és la més perillosa, ja que és molt vulnerable. De totes maneres, hi ha mesures que es poden prendre per tal que les dades que emmagatzemem en el nostre dispositiu mòbil estiguin segures.



5.1. Atacs

Els atacs que es poden fer depenen bàsicament de si el dispositiu està en funcionament o no i del temps que l'atacant tingui per a comprometre el sistema. Per tal d'estructurar millor l'explicació, seguirem el segon criteri, diferenciant quan el mòbil ha estat vulnerable durant un temps reduït de quan aquest ha estat exposat a l'atacant durant molt de temps.

En el cas d'atacs momentanis, l'atacant tindrà poc temps per a efectuar accions. Si el dispositiu està apagat i protegit amb el codi PIN el podem considerar com a segur. En canvi si està encès es poden emprendre diverses accions:

- Llegir d'informació fàcilment accessible, com poden ser els contactes, SMS, correu electrònic o fotografies.

- Eliminar informació fàcilment accessible.

- Reenviar alguna informació important, com pot ser un correu electrònic que contingui la contrasenya per a algun servei web.

- Connectar el dispositiu mòbil a un ordinador i copiar part del contingut de la memòria, on hi pot haver, per exemple, documents, imatges, contrasenyes o dades d'aplicacions.

- Instal·lar codi maliciós.

En el cas d'atacs de duració indefinida, el dispositiu mòbil ha estat sostret durant un temps indeterminat. Això pot ser per pèrdua, robatori o fins i tot per una intervenció per part de la policia. En aquest cas, l'atacant disposarà de tot el temps que vulgui per a intentar trencar el sistema. Les accions que pot emprendre, a banda de les mencionades anteriorment, són:

- Còpia de tota la memòria.

- Tècniques forenses per a recuperar informació que ha estat esborrada recentment.

- Intentar trobar les contrasenyes mitjançant atacs de força bruta[20].

[20] En criptografia s'anomena *atac de força bruta* el procés de recuperar una clau provant totes les combinacions possibles fins a trobar la que permet l'accés.

5.2. Mecanismes de prevenció

Els mecanismes de prevenció els dividirem amb el mateix criteri seguit en els atacs: depenent si la protecció serà efectiva per a sostraccions momentànies o indefinides.

5.2.1. Sostracció momentània

En aquest cas, com que l'atacant tindrà poc temps per a fer accions les mesures de seguretat d'accés al dispositiu que tinguem activades seran molt efectives.

Primer de tot, s'ha d'establir una autenticació quan s'encengui el telèfon. Aquesta pot ser més segura, fent servir usuari i contrasenya, o menys, introduint el codi PIN. De totes maneres, en un accés momentani, qualsevol codi que no sigui totalment previsible, com per exemple el 0000, serà suficient.

Un cop encès, és important tant que el dispositiu es bloquegi automàticament, com que demani una autenticació per a desbloquejar-lo. Si no, un accés momentani amb el dispositiu encès permetrà el robatori de dades. L'autenticació en aquest nivell pot ser més senzilla, ja que la farem servir més sovint, però ha de continuar essent imprevisible.

Un exemple és el patró de desbloqueig que incorporen algunes versions de l'Android, del qual s'ha parlat anteriorment.

Únicament amb aquestes dues mesures podem garantir amb una gran probabilitat que les dades emmagatzemades al nostre dispositiu estaran segures enfront d'un accés al dispositiu momentani.

5.2.2. Sostracció indefinida

En el cas de sostracció indefinida, l'atacant disposarà de tot el temps que vulgui per a intentar trencar el sistema.

Les mesures inicials que s'han de prendre són les descrites a l'apartat anterior: autenticació tant a l'inici com després del desbloqueig. A més, el bloqueig del dispositiu és recomanable que es faci automàticament després d'un temps d'inactivitat. I a partir d'aquí, s'ha d'intentar dificultar qualsevol tipus d'extracció d'informació.

Com s'ha comentat, la mesura de desbloqueig del dispositiu un cop encès és fàcil que sigui menys segura que la inicial; per tant, seria interessant apagar el dispositiu remotament. Però, abans d'aquest apagament del sistema ens interessaria fer altres accions, com una eliminació del contingut emmagatzemat.

El contingut pot ser eliminat tant remotament com localment. Remotament seria produït per l'enviament d'una ordre nostra sobre el dispositiu. Localment, podria ser per una aplicació que en cas d'entrada incorrecta del codi d'autenticació un cert nombre de vegades, automàticament elimini tot el contingut del sistema.

McAfee Mobile Security

L'aplicació McAfee Mobile Security de l'Android és una eina de seguretat per al dispositiu i les dades que emmagatzemi. Aquesta permet fer copies de seguretat, bloquejar-lo remotament, bloquejar-lo en canviar el SIM i monitorar en un mapa la localització actual en la qual hi ha el dispositiu.

Però en alguns casos és possible que no sigui necessari eliminar el contingut si s'ha fet servir xifratge. A més, l'ús del xifratge també garanteix la protecció de les nostres dades contra anàlisis forenses que es puguin fer al dispositiu.

Per la manera com s'emmagatzemen les dades a les memòries, un esborrament normal no és suficient perquè les dades (o part d'aquestes) no puguin ser recuperades. Això sí, si aquestes estan xifrades, per molt que les dades puguin ser recuperades, si no es disposa de la clau correcta per a desxifrar-les aquestes es mantindran protegides.

Finalment, és important tenir sempre una còpia de seguretat de les dades. Sobretot si hem d'esborrar les dades.

Control remot

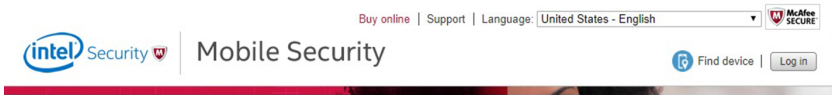
Les plataformes Android i iOS proporcionen mecanismes per a realitzar un control remot del dispositiu. En cas de pèrdua o sostracció indefinida, és possible determinar la ubicació del dispositiu, trucar-hi, bloquejar-lo o bé eliminar-ne tota la informació. Aquestes funcionalitats s'han d'activar abans de la pèrdua del dispositiu per tal de poder-les fer servir.

5.3. Cas d'estudi: McAfee Mobile Security

Una aplicació que permet garantir la privacitat de les dades emmagatzemades fins i tot després del robatori del dispositiu mòbil és el McAfee Mobile Security. D'aplicacions amb aquestes característiques n'hi ha més d'una, però revisarem aquesta perquè és una de les més esteses i de les més completes. A més, aquesta aplicació té al darrere McAfee, una companyia amb un llarg recorregut en la seguretat informàtica.

El McAfee Mobile Security consta de dues parts: la primera és el lloc web https://www.mcafeemobilesecurity.com/ i la segona una aplicació client que s'ha d'instal·lar al dispositiu mòbil. Aquesta aplicació està desenvolupada per a l'Android, el BlackBerry, el Symbian, el Windows Mobile i el Java. En aquest estudi ens centrarem en la versió de l'Android, ja que és el sistema operatiu que més s'ha tractat en aquest mòdul.

El lloc web és la interfície de control per al nostre dispositiu mòbil. Des d'aquí es poden fer diverses tasques remotament, com localitzar i bloquejar les dades del nostre dispositiu mòbil o accedir-hi. Però, abans de poder utilitzar aquest servei és necessari crear-se un compte. En aquest registre ens demana tant el nostre número de telèfon com una contrasenya. Addicionalment, també ens demana un segon número de telèfon, que serà utilitzat com a oient dels canvis produïts al nostre dispositiu mòbil. Per exemple, se li enviarà un SMS quan canviem el SIM.



Lloc web del McAfee Mobile Security

Un cop s'ha accedit al web amb el nostre número de telèfon i la contrasenya, a l'esquerra ens apareix un menú amb totes les opcions per fer. A la secció del nostre dispositiu hi ha les opcions de bloquejar, rastrejar, ubicar, còpia de seguretat, esborrament i restauració. A la secció de les nostres dades hi ha les opcions de contactes, SMS, registre de trucades i multimèdia.

En cas de robatori del nostre dispositiu mòbil, pitjant l'opció de bloqueig s'inutilitza completament el dispositiu mòbil, i es pot personalitzar el missatge que sortirà en pantalla. A més, el dispositiu podrà ser desbloquejat únicament si es disposa del codi PIN de seguretat.

Un cop bloquejat el dispositiu es pot obtenir informació d'aquest, com el número de telèfon que s'està fent servir actualment al nostre dispositiu mòbil i la localització exacta mitjançant una interfície amb el Google Maps. A més, també podem fer una còpia de seguretat de les nostres dades al web, per a poder restaurar-les posteriorment. En cas que no puguem recuperar el nostre dispositiu, per tal de garantir la privacitat de les nostres dades podem esborrar remotament totes les dades personals emmagatzemades al dispositiu.

A més, des del dispositiu mateix es poden anar fent còpies de seguretat d'una manera automàtica.

6. Pràctiques de seguretat

Com hem vist en aquest mòdul, els dispositius mòbils ja han de ser tractats com un ordinador pel que fa a la seguretat, ja que han heretat moltes de les característiques d'un ordinador. Per tant, moltes de les pràctiques de seguretat que aquí veurem seran similars a les que fem servir quan som davant d'un ordinador. Però, com que encara ho veiem com un dispositiu inferior, tenim una falsa sensació de seguretat. Per tant, és important seguir aquestes pràctiques de seguretat quan es fa servir un dispositiu mòbil:

- **Activar el control d'accés inicial**. Aquest accés pot ser mitjançant el codi PIN o usuari i contrasenya.

- **Configurar el bloqueig automàtic**. Després d'un temps d'inactivitat és convenient que el dispositiu es bloquegi.

- **Activar autenticació per a desbloquejar**. Aquesta autenticació per a desbloquejar el dispositiu pot ser més simple i ràpida que la inicial, com reconeixent un patró dibuixat a la pantalla o alguns dels sistemes biomètrics comentats anteriorment.

- **Controlar les aplicacions per instal·lar**. S'ha de tenir cura de les aplicacions que s'instal·lin al sistema, intentant baixar-les de fonts de confiança i amb una reputació positiva. També s'han de revisar els permisos que aquestes aplicacions requereixen per a funcionar (en cas que el sistema operatiu limiti les accions de les aplicacions per mitjà de permisos).

- **Mantenir tot el programari actualitzat**. Per tal de corregir els problemes de seguretat al més aviat possible, és important mantenir tant les aplicacions com el sistema operatiu actualitzat. A més, en cas de ser possible s'ha de configurar perquè faci això automàticament.

- **Fer còpies de seguretat**. És molt important que periòdicament es facin còpies de la informació important que s'emmagatzema al dispositiu. A més, les dades copiades haurien d'estar fora del dispositiu, com pot ser al Web.

- **Xifrar la informació sensible**. Aquest xifratge pot ser tant fent servir els serveis que ofereix el sistema operatiu com amb aplicacions de tercers.

- **Monitorar l'ús de recursos**. Es poden detectar anomalies fent un control de la utilització dels recursos del dispositiu mòbil per part de les aplicaci-

ons. Això inclou revisar la factura telefònica per a detectar possibles usos fraudulents.

- **Deshabilitar els sistemes de comunicació quan no s'utilitzin**. A més de reduir el consum energètic, deshabilitar els sistemes de comunicació quan no s'utilitzen pot evitar atacs. Els sistemes de comunicació únicament s'han d'utilitzar en xarxes de confiança.

- **Permetre control remot**. En cas de robatori és important tenir activat el control remot del dispositiu (iCloud.com per a dispositius iOS i la web d'administració de dispositius Android de Google). Així, es pot localitzar el dispositiu, recuperar-ne les dades emmagatzemades o esborrar les dades confidencials perquè aquestes no siguin compromeses. També es pot tenir una aplicació que esborri les dades automàticament després de diversos intents d'accés fallits.

- **Contactar amb el proveïdor de serveis en cas de pèrdua**. En cas de pèrdua del dispositiu el primer que s'ha de fer és informar el proveïdor de serveis per tal que efectuï el bloqueig del dispositiu.

- **Eliminar la informació confidencial abans de llençar el dispositiu**. En desfer-se del dispositiu no se sap en quines mans pot caure; per tant, és important eliminar tota la informació que conté aquest dispositiu.

- **Tenir sentit comú**. S'han de tenir les mateixes precaucions que es tenen amb els ordinadors quan tractem amb arxius adjunts a correus electrònics, enllaços des d'SMS, aplicacions de missatgeria instantània, xarxes socials i navegació en general per Internet.

Bibliografia

Bibliografia complementària

Felt, Adrienne Porter, et al. (2011). «A survey of mobile malware in the wild». *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*. ACM.

La Polla, Mariantonietta; Martinelli, Fabio; Sgandurra, Daniele (2013). «A survey on security for mobile devices». *IEEE communications surveys & tutorials*, 15.1: 446-471.

Enllaços d'Internet

https://www.android.com/security-center/

https://developer.apple.com/security/

https://www.apple.com/business/docs/iOS_Security_Guide.pdf

https://www.us-cert.gov/

https://www.ccn-cert.cni.es/