Administració de la seguretat

Jordi Serra Ruiz
Miquel Colobran Huguet
Josep Maria Arqués Soldevila
Eduard Marco Galindo

PID_00190184

Universitat Oberta de Catalunya

Els textos i imatges publicats en aquesta obra estan subjectes –llevat que s'indiqui el contrari– a una llicència de Reconeixement-NoComercial-SenseObraDerivada (BY-NC-ND) v.3.0 Espanya de Creative Commons. Podeu copiar-los, distribuir-los i transmetre'ls públicament sempre que en citeu l'autor i la font (FUOC. Fundació per a la Universitat Oberta de Catalunya), no en feu un ús comercial i no en feu obra derivada. La llicència completa es pot consultar a http://creativecommons.org/licenses/by-nc-nd/3.0/es/legalcode.ca

Índex

Introducció

Com veurem seguidament, el concepte de seguretat informàtica és difús i pràcticament inabastable, per la qual cosa serà preferible centrar-nos en el que podríem anomenar fiabilitat, entesa com a garantia de qualitat de servei d'un sistema informàtic. En aquest mòdul veurem els elements que poden comprometre aquesta fiabilitat, i també les eines que un administrador té a la seva disposició a l'hora d'evitar i detectar les mancances de seguretat d'un sistema informàtic. Finalment, en els darrers apartats d'aquest mòdul introduïm el concepte del mal anomenat delicte informàtic, les responsabilitats derivades d'aquest tipus d'accions, així com les bases d'una disciplina de recent creació, la informàtica forense, la qual ens pot ajudar a determinar, una vegada ha succeït un incident, què ha passat i qui n'ha estat l'autor.

Objectius

En els materials didàctics associats a aquest mòdul, l'estudiant trobarà les eines i els continguts necessaris per a assolir els objectius següents:

1. Conèixer els problemes bàsics que comporta l'administració de seguretat d'un sistema informàtic.

2. Conèixer quines són les responsabilitats que té un administrador envers els equips i les dades que es troben contingudes en un sistema informàtic, i les responsabilitats en què poden incórrer les persones que en vulneren la seguretat, així com què cal fer una vegada ha succeït un incident de seguretat per a poder determinar què ha passat i qui n'ha estat el presumpte autor.

3. Saber establir plans de recuperació del sistema en cas d'atac o pèrdua d'informació.

1. Seguretat informàtica

Encara que sigui d'una manera intuïtiva, tots entenem que un sistema informàtic es considerarà segur si es troba lliure de tot risc o dany. Tot i que no resulta gaire senzill formalitzar el concepte de seguretat informàtica, entendrem com a tal el conjunt constituït per diverses metodologies, documents, programari i maquinari que determinen que els accessos als recursos d'un sistema informàtic siguin duts a terme exclusivament pels elements autoritzats a fer-ho.

Efecte de desastres naturals

Tot i que no es tindran en consideració les mesures que cal aplicar per a prevenir o reduir l'efecte dels desastres naturals o altres tipus d'accidents (incendis, inundacions, etc.), en un estudi real poden ser d'importància vital.

Atès que és del tot impossible garantir la seguretat o inviolabilitat absoluta d'un sistema informàtic, en lloc de l'inabastable concepte de seguretat serà preferible fer servir el terme **fiabilitat**. Per tant, no es podrà entendre la seguretat informàtica com un concepte tancat conseqüència de l'aplicació mecànica d'una sèrie de mètodes, sinó com un procés que es pot veure compromès en qualsevol moment de la manera més insospitada possible.

En general, doncs, direm que un sistema informàtic és fiable quan se satisfan les tres propietats següents:

- **Confidencialitat**: només poden accedir als recursos que integren el sistema els elements autoritzats a fer-ho. Per recursos del sistema no solament s'entén la informació, sinó qualsevol recurs en general: impressores, processador, etc.

- **Integritat**: els recursos del sistema només poden ser modificats o alterats pels elements autoritzats a fer-ho. La modificació inclou diverses operacions, com ara l'esborrament i la creació, a més de totes les possibles alteracions que es puguin fer sobre un objecte.

- **Disponibilitat**: els recursos del sistema han de romandre accessibles als elements autoritzats.

Com ens podem imaginar, és molt difícil trobar un sistema informàtic que maximitzi les tres propietats. Normalment, i segons l'orientació del sistema, es prioritzarà algun dels tres vessants.

Exemple de prioritització de la confidencialitat de la informació

En un sistema que emmagatzemi dades de caràcter policial, l'element que cal prioritzar és la confidencialitat de la informació, tot i que també cal tenir molt en compte la preservació (en la mesura que es pugui) de la integritat i la disponibilitat. Observem que no serveix de res garantir la confidencialitat mitjançant algun mètode criptogràfic si permetem que un intrús pugui esborrar fàcilment la informació emmagatzemada en el disc dur del servidor (atac contra la integritat). D'altra banda, és absolutament necessari que les dades puguin ésser disponibles en el decurs d'una actuació policial, per la qual cosa tampoc podem descuidar la propietat de disponibilitat en un sistema d'aquestes característiques.

1.1. Tipus d'atacs

La protecció d'un sistema informàtic no solament s'ha d'adreçar al maquinari i al programari, sinó també a les dades, tant si es troben circulant per una xarxa com si estan emmagatzemades en un disc dur o en altres suports.

Pensem que si bé gairebé sempre és possible substituir el maquinari o el programari, les dades, objectiu primordial de tot sistema informàtic, no tenen substitut en cas que es perdin definitivament.

Els atacs que poden patir el maquinari, el programari i, d'una manera molt especial, les dades, es classifiquen en quatre grans grups:

1) Interrupció: atac contra la disponibilitat en el qual es destrueix o queda no disponible un recurs del sistema.

Exemple d'atac d'interrupció

Un exemple d'atac d'interrupció és tallar una línia de comunicació o deshabilitar el sistema de fitxers del servidor. Un altre són els atacs de denegació de servei.

2) Intercepció: atac contra la confidencialitat en el qual un element no autoritzat aconsegueix l'accés a un recurs. En aquest tipus d'atac no ens referim únicament a possibles usuaris que actuïn com a espies en la comunicació entre emissor i receptor.

Exemple d'atac d'interceptació

Un procés que s'executa subreptíciament en un ordinador i que emmagatzema en un fitxer les tecles que prem l'usuari que utilitza el terminal, constituiria un atac d'intercepció.

El programari o maquinari que enregistra l'activitat d'un teclat d'una estació de treball rep el nom genèric de *keylogger*.

Vegeu també

Sobre els atacs de denegació de servei vegeu el subapartat 3.6 d'aquest mateix mòdul.

3) Modificació: atac contra la integritat en el qual, a més d'aconseguir l'accés no autoritzat a un recurs, també s'aconsegueix modificar-lo, esborrar-lo o alterar-lo de qualsevol manera.

Exemples d'atac de modificació

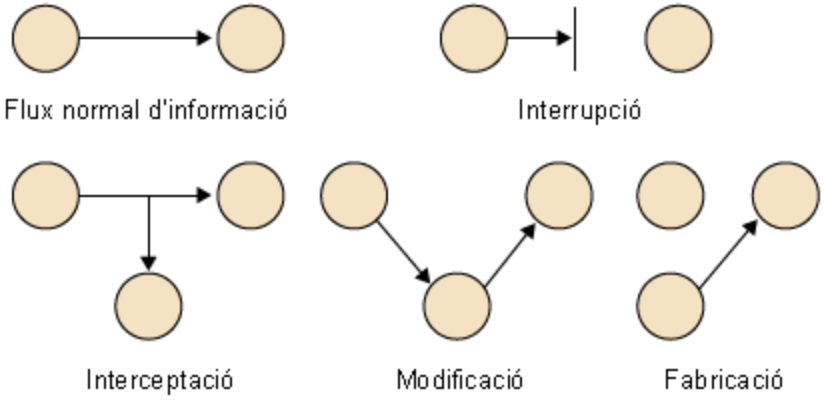
Els atacs fets pels intrusos (esborrament de bases de dades, alteració de pàgines web, etc.) són exemples típics d'aquesta modalitat d'atac.

4) Fabricació: atac contra la integritat en el qual un element aconsegueix crear o inserir objectes falsificats en el sistema.

Exemples d'atac de fabricació

Un exemple d'atac de fabricació és afegir d'una manera no autoritzada un nou usuari –i la contrasenya corresponent– al fitxer de contrasenyes.

Representació dels diferents tipus d'atacs que pot patir la comunicació entre emissor i receptor



1.2. Atacs provinents de persones

La major part dels atacs que pot patir un sistema informàtic es produeixen en mans de persones que, amb diversos objectius, intenten d'accedir a informació confidencial, destruir-la o simplement aconseguir el control absolut del sistema atacat. Conèixer els objectius dels atacants i les seves motivacions resulta, doncs, essencial per a prevenir-ne i detectar-ne les accions.

Vegeu també

Les amenaces lògiques (virus, troians, etc.) es consideraran en l'apartat 3 d'aquest mòdul, dedicat a la seguretat del sistema.

Així, doncs, els atacs provinents de persones es poden classificar en dos grans grups:

1) Atacs passius. L'atacant no modifica ni destrueix cap recurs del sistema informàtic, simplement l'observa, normalment amb la finalitat d'obtenir alguna informació confidencial. Sovint aquest atac es produeix sobre la informació que circula per una xarxa. L'atacant no altera la comunicació, sinó que senzillament l'escolta i obté la informació que es transmet entre l'emissor i el receptor. Com que la informació que es transmet no resulta alterada, la detecció d'aquest tipus d'atac no és una tasca senzilla, perquè l'escolta no té cap efecte sobre la informació circulant. Una solució molt eficaç que permet de resoldre aquest tipus de problema consisteix en l'ús de tècniques criptogràfiques per a fer que la informació no es transmeti en clar i no pugui ser comprensible per als espies.

Vegeu també

Una eina criptogràfica que es fa servir molt és el PGP (*pretty good privacy*). Sobre aquesta eina podeu veure l'apartat 2 d'aquest mateix mòdul.

2) Atacs actius. En una acció d'aquest tipus, l'atacant altera o destrueix algun recurs del sistema. Per exemple, en el cas d'un espia que monitoritza una xarxa, es podrien donar problemes molt seriosos, com els que exposem a continuació:

- **Suplantació d'identitat**: l'espia pot suplantar la identitat d'una persona i enviar missatges en nom seu.

- **Reactuació**: un o diversos missatges legítims són interceptats i reenviats diverses vegades per a produir un efecte no desitjat (per exemple, intentar repetir diverses vegades un ingrés en un compte bancari).

- **Degradació fraudulenta del servei**: l'espia evita el funcionament normal dels recursos del sistema informàtic. Per exemple, podria interceptar i eliminar tots els missatges que s'adrecen a un usuari determinat.

- **Modificació de missatges**: es modifica una part del missatge interceptat i es reenvia a la persona a qui anava adreçat originalment.

Com ja s'ha indicat prèviament, conèixer les motivacions que poden tenir les persones per a atacar els sistemes informàtics pot ser vital a l'hora de prevenir tota mena d'intrusions. Vegem, doncs, el perfil dels possibles atacants d'un sistema informàtic:

- **Personal de la mateixa organització**: tot i que per defecte el personal intern gaudeix de la confiança de l'organització, cal tenir en compte que alguns atacs es poden produir des de dins mateix de la institució. Sovint no cal que aquests atacs siguin intencionats (tot i que, quan ho són, són els més devastadors que es poden produir), poden ser accidents provocats pel desconeixement del personal (per exemple, el format accidental d'un disc dur).

Desinformació

Una política de seguretat adequada pot evitar els problemes provocats per la desinformació o falta de coneixement.

- **Antics treballadors**: una part molt important dels atacs a sistemes informàtics són els fets per antics treballadors que, abans de deixar l'organització, instal·len tota mena de programaris destructius com, per exemple, virus o bombes lògiques que s'activen en absència del treballador que, acomiadat o descontent per les condicions de treball, ha decidit canviar de feina. La presència d'aquest tipus de programari no sempre és fàcil de detectar, però almenys sí que es poden evitar els atacs que l'antic treballador pugui dur a terme des de fora amb el nom d'usuari i la contrasenya de què disposava quan encara treballava a l'organització. Per tant, com a norma general, cal donar de baixa tots els comptes de l'extreballador i canviar-ne les contrasenyes d'accés al sistema com més ràpid millor.

Nom dels usuaris

Els noms dels usuaris es poden deduir fàcilment dins d'una organització perquè sovint es troben normalitzats sota algun criteri (per exemple, l'usuari Pere Joan podria tenir el nom d'usuari *pjoan*).

- ***Hackers*** (**intrusos informàtics**): aquestes persones duran a terme normalment atacs passius orientats a obtenir informació confidencial (per exemple, un examen d'un curs universitari), o simplement amb la finalitat de posar-se a prova per a obtenir el control del sistema atacat. A més, si l'atacant és prou hàbil, fins i tot podria esborrar les empremtes de les seves accions en els fitxers que les enregistren (anomenats genèricament fitxers *log*). Com que aquest tipus d'accions no produeixen cap efecte "visible", no són fàcilment detectables. Els intrusos solen aprofitar les vulnerabilitats conegudes de sistemes operatius i programaris per a aconseguir el control de tot el sistema informàtic. Per a dur a terme aquest tipus d'accions n'hi ha prou d'executar diversos programaris que es poden obtenir a Internet

Vegeu també

En l'apartat 3 descriurem algunes de les tècniques que poden fer servir els intrusos per a dur a terme les seves accions.

i que automatitzen els atacs als sistemes informàtics sense que l'intrús necessiti disposar de gaires coneixements tècnics.

A més de les eines que hem esmentat, els intrusos disposen d'altres tècniques més senzilles (almenys des del punt de vista informàtic), però igual d'efectives. Per exemple, pot resultar molt productiu fer una senzilla recerca de contrasenyes escrites en papers entre la brossa continguda en una paperera (*trashing*), o d'una manera més enginyosa l'intrús podria suplantar la identitat d'una altra persona per a esbrinar-ne la contrasenya (*mascarada*). Així mateix, un intrús que volgués obtenir una contrasenya en un sistema determinat, podria trucar per telèfon a l'administrador, fer-se passar per una altra persona i demanar la contrasenya amb l'excusa que l'ha oblidat o perdut. En un excés de bona fe, l'administrador podria canviar la contrasenya i lliurar la nova a l'intrús en la mateixa comunicació telefònica. Les variants d'aquest tipus d'atacs són múltiples i moltes s'inclouen dins el que es denomina *enginyeria social*, és a dir, la manipulació de les persones per tal que facin determinades accions que en realitat no volen fer.

Altres finalitats il·lícites

Altres finalitats il·lícites que cal considerar: utilització del sistema atacat com a servidor de còpies no autoritzades de programari o com a trampolí per a atacar altres màquines.

Delicte de danys

Les accions dels intrusos (*hackers*) poden ser constitutives de delicte de danys –entre d'altres– i poden implicar responsabilitats civils i penals.

- **Intrusos remunerats**: tot i no ser un tipus d'atac gaire freqüent, també val la pena tenir-lo en compte. En aquest cas, els intrusos es troben perfectament organitzats (poden ser en diferents localitzacions geogràfiques i tot) i ataquen d'una manera conjunta el sistema d'una organització determinada. Disposen de molts mitjans tècnics i reben remuneracions molt elevades de l'organització rival que dirigeix l'atac, sovint amb l'ànim d'accedir a informació confidencial (un nou disseny, un nou programari, etc.) o bé amb la intenció de provocar un dany important en la imatge de l'organització atacada.

1.3. Mecanismes de seguretat

La seguretat global d'un sistema informàtic depèn en bona part del disseny acurat de les mesures següents:

- **Mesures de prevenció**: augmenten la seguretat del sistema durant el seu funcionament.
- **Mesures de detecció**: s'utilitzen per a detectar violacions de la seguretat d'un sistema.
- **Mesures de recuperació**: permeten la recuperació del funcionament correcte del sistema una vegada s'ha produït l'atac.

Exemples de mesures de prevenció, detecció i recuperació

Alguns exemples de mesures de seguretat són:

1) Mesures de prevenció: l'ús de tallafoc per a evitar els intrusos.
2) Mesures de detecció: ús de l'eina de seguretat i integritat de dades *Tripwire*.
3) Mesures de recuperació: a més dels mecanismes de còpia de seguretat, també entren dins d'aquesta categoria els programaris d'anàlisi forense (com l'eina *Encase*, per exemple), els quals permeten d'esbrinar quina ha estat la porta d'entrada al sistema i també les activitats que ha dut a terme l'intrús.

Atès que el desenvolupament en profunditat d'aquests tres punts no és possible per motius obvis d'espai, en aquest mòdul ens limitarem a exposar els problemes bàsics que comporta l'administració d'un sistema pel que fa a la prevenció i detecció de violacions de la seguretat.

Vegeu també

Vegeu els plans de contingència i d'anàlisi de riscos en el mòdul "El sistema informàtic dins l'organització".

En cas de caiguda del sistema, ens pot ser útil tenir en consideració el protocol d'actuació següent:

1) Desconnexió de l'equip atacat de la xarxa. Amb aquesta acció evitem que l'intrús causi més danys i que pugui eliminar (si encara no ho ha fet) les empremtes de les seves accions.

2) Fer una còpia de seguretat a baix nivell que s'utilitzarà posteriorment per a analitzar l'atac.

3) Analitzar i compilar tota la informació possible sobre l'atac: *logs*, programari instal·lat per l'atacant (troians, per exemple), porta d'entrada que ha fet servir, etc.

4) Restaurar el sistema i aplicar les actualitzacions del programari instal·lat (o *patch*) per a solucionar la vulnerabilitat de què s'ha servit l'atacant per a introduir-se en el sistema. A més, cal notificar l'atac als usuaris amb la finalitat que canviïn les contrasenyes dels comptes com més aviat millor.

Adreça recomanada

Hi ha moltes llistes de correu de seguretat que aporten informació de vulnerabilitats i actualitzacions diàriament. Per exemple, http://www.hispasec.com.

5) Si es detecta que la màquina ha estat utilitzada com a trampolí per a atacar altres màquines, cal avisar els responsables d'aquests sistemes. També cal notificar l'atac al cap de l'organització del sistema atacat i, en cas que es consideri necessari, denunciar-ho a la policia (tots els cossos policíacs de l'Estat disposen d'unitats especialitzades en aquest tipus de delicte) i notificar-ho al Computer Emergency Response Team (CERT). Finalment, també és possible sol·licitar informes pericials als col·legis d'enginyers informàtics i a empreses especialitzades del sector.

Els CERT són equips de resposta als incidents de seguretat dels sistemes informàtics. Cada país disposa dels seus propis CERT, els quals ofereixen serveis d'assistència tècnica, anàlisi i documentació sobre els incidents de seguretat que es produeixen.

Adreça recomanada

Podeu accedir a l'IRIS-CERT a l'adreça http://www.rediris.es/cert.

2. Seguretat de l'entorn

En aquest apartat veurem algunes mesures de protecció física que es poden fer servir per a evitar els accessos no autoritzats als sistemes informàtics. Una organització pot invertir molts diners en programari que eviti i detecti els accessos il·lícits als seus sistemes, però tota aquesta inversió no servirà de res si els recursos físics del sistema es troben a l'abast de tothom.

El maquinari sol ser l'element més car d'un sistema informàtic i, per tant, cal tenir especial cura amb les persones que hi tenen accés material. Una persona no autoritzada que accedís al sistema podria causar enormes pèrdues: robatori d'ordinadors, introducció de programari maliciós en el servidor (per exemple, un troià o un *keylogger*), destrucció de dades, etc.

Per a evitar aquest problema hi ha diverses mesures de prevenció com, per exemple, les següents:

Vegeu també

Vegeu les polítiques de còpies de seguretat en el mòdul "Administració de servidors".

- Mantenir els servidors i tots els elements centrals del sistema en una zona d'accés físic restringit.
- Mantenir els dispositius d'emmagatzemament en un lloc diferent de la resta del maquinari.
- Dur a terme inventaris o registres de tots els elements del sistema informàtic (útil en casos de robatori).
- Protegir i aïllar el cablatge de la xarxa (tant per a protegir-lo de danys físics com de l'espionatge).
- Instal·lació de càmeres de videovigilància.
- Utilització de contrasenyes en els protectors de pantalla.
- Utilització de contrasenyes de BIOS.
- Desactivar les opcions d'autocompletar i recordar contrasenyes dels navegadors d'Internet.
- Triar una topologia de xarxa adequada a les nostres necessitats de seguretat.
- Garantir la seguretat del maquinari de xarxa (encaminadors, connectors, concentradors i mòdems).

- Mecanismes d'autenticació dels usuaris que volen accedir al sistema.

S'anomena **autenticació** el procés de verificació de la identitat d'una persona o d'un procés que vol accedir als recursos d'un sistema informàtic.

Vegeu també

Sobre la topologia de xarxa segura i sobre la seguretat del maquinari de xarxa vegeu el mòdul "Administració de la xarxa".

De mecanismes d'autenticació n'hi ha de molts tipus diferents, des dels més barats i senzills (com, per exemple, un nom d'usuari i una contrasenya) fins als més cars i complexos (com, per exemple, un analitzador de retina). Com sempre, segons els objectius i el pressupost de l'organització, cal triar el que més s'ajusti a les nostres necessitats. També cal tenir en compte que molts d'aquests mecanismes són complementaris i es poden utilitzar alhora.

Situació d'un mecanisme d'autenticació

Hi ha diversos nivells en els quals situar un mecanisme d'autenticació:

- Instal·lat en la BIOS.
- Instal·lat en el sector d'arrencada de l'equip.
- Sol·licitat pel sistema operatiu.
- Sol·licitat per un programari.

2.1. Mecanismes d'autenticació d'usuaris

Hi ha diversos mecanismes d'autenticació d'usuaris. Els podem classificar de la següent manera:

1) Sistemes basats en elements coneguts per l'usuari

El principal mecanisme dins d'aquests tipus d'autenticació són els sistemes basats en **contrasenyes**. És un dels mètodes que es fan servir més sovint per a autenticar un usuari que vol accedir a un sistema. Òbviament és el mètode més barat, però també és el més vulnerable, ja que encara que la paraula de pas o contrasenya hauria de ser personal i intransferible, sovint acaba en poder de persones no autoritzades. D'altra banda, encara que les contrasenyes s'emmagatzemin xifrades en un fitxer, és possible desxifrar-les amb múltiples tècniques (per exemple, un atac de diccionari).

Tot i que l'assignació de les contrasenyes als usuaris es basa en el sentit comú, no és sobrer recordar els aspectes següents:

- Memoritzar-la i no portar-la escrita.
- Canviar-la periòdicament (amb caràcter mensual, per exemple).
- No repetir la mateixa contrasenya en comptes diferents.
- Evitar d'introduir-la en presència d'altres persones.
- No llençar documents amb contrasenyes a la paperera.
- Evitar utilitzar paraules de diccionari.
- Evitar utilitzar dades que poden ser conegudes per altres persones (per exemple, nom i cognom de l'usuari, *login*, DNI, número de mòbil, etc.).
- Fer servir contrasenyes d'un mínim de vuit caràcters.
- Evitar la reutilització de contrasenyes antigues.
- No utilitzar contrasenyes exclusivament 1èriques.
- Afavorir l'aparició de caràcters especials (¡, *, ¿, etc.).
- No utilitzar seqüències de teclat del tipus "qwerty".

Vegeu també

Sobre l'ús de diccionaris als atacs a contrasenya vegeu el subapartat 3.2 d'aquest mòdul.

- Fer servir mnemotècnics per a recordar la contrasenya.

Encara que com a usuaris d'un sistema informàtic pensem que no és necessari prendre precaucions amb la nostra contrasenya perquè no emmagatzemem cap informació important en el sistema, val la pena aturar-se a pensar que una persona prou hàbil podria obtenir el control de tot el sistema a partir de l'obtenció d'un compte sense cap privilegi especial.

A tall d'exemple, a l'article "Observing Reusable Password Choices", publicat al principi dels anys noranta, segons Eugene H. Spafford el 30% dels comptes dels sistemes Unix de la mostra analitzada tenien contrasenyes que es podien desxifrar en només uns minuts de temps de CPU[1]. Tenint en compte que els ordinadors actuals són molt més ràpids, si la política d'assignació de contrasenyes (i l'educació dels usuaris en el seu ús) no ha variat, el problema s'haurà agreujat encara més.

[(1)]CPU és la sigla de l'expressió anglesa corresponent a *unitat de control de procés*.

Lectura complementària

Eugene H. Spafford. "Observing Reusable Password Choices". A: *Usenix Security III Proceedings* (pàg. 299-312).

2) Sistemes basats en elements que posseeix l'usuari

A diferència dels mètodes anteriors, aquests sistemes no es basen en el que coneix l'usuari, sinó en el que posseeix. Podem distingir:

a) Sistemes basats en targetes intel·ligents i *tokens* de seguretat

Una targeta intel·ligent[2] és similar a una targeta de crèdit, però a diferència d'aquesta les targetes intel·ligents allotgen un microprocessador (i memòria) que les dota de les característiques següents:

[(2)]En anglès, *smartcard.*

- Capacitat per a fer càlculs criptogràfics sobre la informació que emmagatzemen (algoritmes DES, Triple DES, DSS, RSA, etc.).

Vegeu també

Els algoritmes DES, Triple DES, DSS, RSA es descriuen al subapartat 2.2 d'aquest mòdul.

- Emmagatzematge xifrat de la informació.
- Protecció física i lògica (clau d'accés) a la informació emmagatzemada.

Vegeu també

Sobre les claus de signatura i xifratge vegeu el subapartat 2.2 d'aquest mateix mòdul.

- Capacitat per a emmagatzemar claus de signatura i xifratge.

És un mètode d'autenticació que cada vegada fan servir més les organitzacions, tot i el cost d'adaptació de la infraestructura als dispositius que permeten la lectura de les targetes.

A més, les targetes poden ser de contacte (és a dir, han de ser inserides en la ranura d'un lector perquè puguin ser llegides), o sense contacte. Per exemple, aquest segon tipus s'ha començat a emprar amb èxit en diversos països com a sistema de pagament en el transport públic.

Una altra solució per a resoldre el problema de l'autenticació, força popular en el sector empresarial, consisteix en l'anomenat *token* de seguretat. Solen ser dispositius físics de mida reduïda (alguns inclouen un teclat per a introduir un PIN), similars a un clauer, que calculen contrasenyes d'un únic ús (canvien a cada *login* o cada cert temps). Poden emmagatzemar claus criptogràfiques, com per exemple la signatura digital o mesures biomètriques.

b) Sistemes biomètrics

Els sistemes biomètrics es basen en les característiques físiques de l'usuari que s'ha d'autenticar (o en patrons característics que puguin ser reconeguts com, per exemple, la signatura). Com a principal avantatge, l'usuari no ha de recordar cap contrasenya ni cal que porti cap targeta al damunt. Solen ser molt més cars que els mètodes anteriors, motiu pel qual encara no es fan servir gaire, tot i que alguns d'aquests mètodes ofereixen un alt nivell de seguretat (per exemple, el reconeixement dactilar). Entre les diferents característiques que es poden utilitzar per a reconèixer un usuari mitjançant mesures biomètriques destaquem els següents:

Seguretat dels sistemes biomètrics

Tot i que aparentment aquests sistemes són molt difícils de falsificar, cal veure els treballs realitzats pel Netherlands Forensics Institute, sobre la seguretat real que presenten els sistemes biomètrics.

Vegeu també

Vegeu en l'apartat 4 d'aquest mòdul com s'ha de fer l'emmagatzemament de les dades personals.

- Veu.
- Olor corporal.
- Escriptura.
- Empremtes dactilars (probablement és el mètode més utilitzat i de menys cost).
- Patrons de la retina o de l'iris.
- Geometria de la mà.
- Traçat de les venes.
- Estructura facial.

2.2. Protecció de les dades

Per a evitar els atacs contra la confidencialitat i les tècniques d'espiament es poden fer servir diversos mètodes criptogràfics. A continuació definirem els criptosistemes de clau privada i clau pública, les funcions resum i la signatura digital, i estudiarem les implicacions que poden tenir aquests elements en la seguretat global del sistema informàtic.

Vegeu també

Sobre tècniques d'espiament vegeu el subapartat 1.2. d'aquest mòdul.

Una *xifra* o *criptosistema* és un mètode secret d'escriptura, mitjançant el qual un text en clar es transforma en un text xifrat o **criptograma**. El procés de transformar un text en clar en text xifrat s'anomena **xifratge**, i el procés invers, és a dir, la transformació del text xifrat en text en clar, s'anomena **desxifratge**. Tant el xifratge com el desxifratge són controlats per una o més **claus criptogràfiques**.

S'anomena **criptografia**[3] la ciència i estudi de l'escriptura secreta. Juntament amb la **criptoanàlisi** (tècnica que té com a objectiu esbrinar la clau d'un criptograma a partir del text en clar i del text xifrat) formen el que es coneix amb el nom de **criptologia**.

(3)El mot *criptografia* prové dels mots grecs *krypto* (`amagat') i *graphia* ('escriptura').

Per a protegir la confidencialitat de les dades (emmagatzemades o circulant per la xarxa) es poden fer servir criptosistemes de clau privada (simètrics) o de clau pública (asimètrics).

2.2.1. Criptosistemes de clau privada

Els **criptosistemes de clau compartida** són criptosistemes en els quals emissor i receptor comparteixen una única clau. És a dir, el receptor podrà desxifrar el missatge rebut si i només si coneix la clau amb la qual l'emissor ha xifrat el missatge.

L'algorisme més representatiu dels criptosistemes de clau privada és el *Data Encryption Standard* (DES), de l'any 1977. Aquest algorisme xifra la informació en blocs de 64 bits de llargada fent servir claus de 56 bits. Actualment es troba en desús, ja que no és segur. En lloc del DES s'utilitza una variant anomenada Triple DES, o altres algorismes com, per exemple, IDEA, CAST, Blowfish, etc. No obstant això, l'actual estàndard (des de l'any 2002), adoptat com a tal pel Govern dels Estats Units, és l'anomenat *Advanced Encryption Standard* (AES), representat per l'algorisme *Rijndael*. Les especificacions de l'AES (que no coincideixen exactament amb el seu representant, l'algorisme *Rijndael*), determinen una mida de bloc fix de 128 bits i mides de clau de 128, 192 o 256 bits. A continuació veurem un criptosistema veritablement enginyós i conceptualment molt elegant.

2.2.2. Criptosistemes de clau pública

La criptografia de clau pública va ser introduïda per Diffie i Hellman l'any 1976.

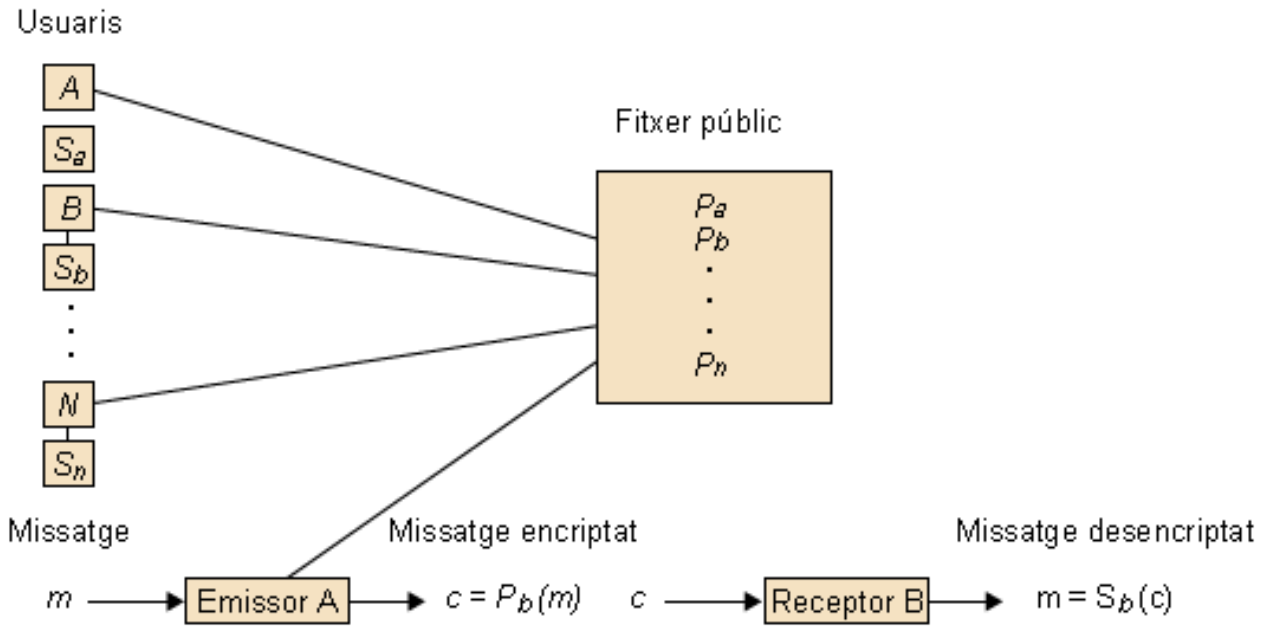
Els **criptosistemes de clau pública** són un tipus de criptosistemes on cada usuari u té associada una parella de claus $<P_u , S_u>$. La clau pública, P_u, és accessible per a tots els usuaris de la xarxa i apareix en un directori públic, mentre que la clau privada, S_u, tan sols és coneguda per l'usuari u.

Observació

Donada qualsevol clau del parell $<P_u , S_u>$, no és possible esbrinar-ne una a partir de l'altra.

Quan un usuari *A* vol enviar un missatge a un usuari *B*, xifra el missatge fent servir la clau pública de *B* (recordem que aquesta clau és accessible per tothom). Quan el receptor rebi el missatge únicament el podrà desxifrar utilitzant la seva clau privada (la qual es troba exclusivament en poder seu).

Xifratge d'un missatge en un criptosistema de clau pública



El criptosistema de clau pública més conegut és l'anomenat RSA[4], però n'hi ha d'altres com, per exemple, el criptosistema *Digital Signature Algorithm* (DSA). Aquests tipus de criptosistemes es basen en funcions matemàtiques unidireccionals (no utilitzen substitucions o transposicions) i són lents si es comparen amb els de clau privada, motiu pel qual se solen fer servir per a intercanviar claus simètriques en els protocols de comunicació, però no per a xifrar informació.

Un avantatge molt important d'aquest tipus de criptosistema és que permet la incorporació de **signatura digital**. Cada usuari podrà signar digitalment el seu missatge amb la seva clau privada i aquesta signatura podrà ser verificada més tard de manera que l'usuari que l'ha originat no pugui negar que s'ha produït (propietat de *no-repudi*).

Per a poder explicar el mecanisme de signatura digital, caldrà definir prèviament el concepte de funció *hash*.

(4)El criptosistema RSA va ser ideat el 1978 per Rivest, Shamir i Adleman.

DSS

El *Digital Signature Standard* (DSS) és un sistema de signatura digital adoptat com a estàndard per l'NIST. Utilitza la funció resum SHA i l'algorisme DSA.

Vegeu també

Com veurem al subapartat 4.2.3 la signatura digital té jurídicament la mateixa validesa que la convencional.

Una funció ***hash*** (o **funció resum**) és una funció matemàtica que fa correspondre una representació de mida fixa a un missatge *m* de mida variable. Aquesta representació té de 128 a 160 bits –els nous algorismes poden arribar als 256, 384 i 512 bits–) i s'anomena *valor resum del missatge*.

Per exemple, el que es pot veure a continuació és el resultat d'aplicar una funció resum a un fitxer anomenat MD5.TXT:

```
MD5.txt 89736DF30DC47A7D5AC22662DC3B5E9C
```

Les funcions resum han de ser unidireccionals.

Una funció resum o funció *hash* (*H*) és **unidireccional** si per a qualsevol missatge *m*' del recorregut de *H*, és "difícil" (des del punt de vista computacional) trobar *m* tal que *m*' = *H* (*m*).

Paper de les funcions resum

Les funcions resum o funcions *hash* tenen un paper molt important en la verificació de la integritat del sistema (detecció de troians, virus, etc.).

Els programaris P2P, per exemple, usen funcions *hash* a efectes d'identificació dels arxius compartits entre els diferents usuaris de la xarxa.

Els algorismes **MD5**[5] i **SHA-1**[6] són els que es fan servir més per a implementar les funcions resum. A més de l'algorismes SHA-0 (el precursor) i SHA-1, hi ha diverses variants (SHA-224, SHA-256, SHA-384 i SHA-512), tots ells identificats com a SHA-2. En l'actualitat encara no s'ha pogut trobar cap atac efectiu sobre l'algorisme SHA-1, tot i que s'han publicat resultats compromesos sobre funcions similars a SHA-1.

(5)MD5 és la sigla de *message digest*.

(6)SHA-1 és la sigla de *secure hash algorithm*.

Origen dels algoritmes MD5 i SHA-1

L'algoritme MD5 va ser desenvolupat per Ron Rivest i amb resums de 128 bits. Està qüestionat des de l'any 2004.

L'algoritme SHA-1 va ser desenvolupat per l'Agència de Seguretat Nord-americana i amb resums de 160 bits.

A continuació descriurem el funcionament del protocol de signatura digital amb funcions resum. Suposem que l'usuari *A* vol signar el missatge *m* i enviar-lo a l'usuari *B*.

1) L'usuari *A* calcula el resum de *m*.

2) A continuació, l'usuari *A* signa el resum, *m*, amb la seva clau privada i obté *s*. L'usuari B rebrà el missatge *m* i el resum signat *s*. Quan l'usuari *B* volgués verificar l'origen del missatge rebut faria les accions següents.

3) L'usuari *B* calcula el resum de *m*.

4) A continuació, l'usuari *B* desxifra el resum signat, *s*, fent servir la clau pública de l'usuari *A*. Si aquest valor coincideix amb el calculat en el pas 3, aleshores *s* és una signatura digital vàlida per al valor resum de *m*.

Certificat digital

A l'hora d'utilitzar la clau pública d'un usuari, com podem saber que és autèntica? Per a resoldre aquest problema es requereix la participació d'una tercera part (anomenada autoritat de certificació) que confirmi l'autenticitat de la clau pública d'un usuari amb l'expedició d'un certificat digital.

L'eina criptogràfica PGP

El programari *Pretty Good Privacy* (PGP) va ser desenvolupat per Phil Zimmermann l'any 1991 i en l'actualitat encara és una de les eines que més es fan servir mundialment per a preservar la confidencialitat de la informació i signar les comunicacions que s'han fet per correu electrònic, tot i les sospites que han originat les seves presumptes *backdoors*.

Backdoors

Les *backdoors* són portes d'entrada a sistemes operatius i programaris, inserides pels mateixos dissenyadors o programadors, que els permeten d'accedir a l'aplicació evitant tots els mecanismes d'autenticació.

PGP[7] és un programari híbrid que utilitza tant tècniques de criptografia de clau privada com de clau pública. A més de gestionar les claus i permetre diversos algorismes de xifratge, també permet l'esborrament segur de fitxers.

(7)PGP són les sigles que identifiquen el tipus de programari *pretty good privacy*.

Un tret essencial que va convertir el PGP en una eina molt atractiva arreu del món és que el seu codi font era de lliure distribució (fins a la versió 6.5.8), motiu pel qual Zimmermann va patir seriosos problemes amb els serveis secrets nord-americans, ja que als Estats Units, l'exportació d'eines criptogràfiques era considerada una pràctica similar al contraban d'armes. La venda del PGP a una empresa nord-americana i la dificultat per a accedir al seu codi font, han provocat que els seus usuaris sospitessin de l'existència de portes de darrere o *backdoors* (tot i que Zimmerman afirma que la versió 7.0.3 es va desenvolupar sota la seva supervisió i no té portes de darrere). Per aquest motiu, l'any 1999 va aparèixer un nou programari, anomenat *Gnu Privacy Guard* (GnuPG), obra de l'alemany Werner Koch i que, com el seu nom indica, és un programa lliure sota llicència GNU, el qual desenvolupa els estàndards d'implementació de l'OpenPGP.

Observació

Un usuari pot signar digitalment els fitxers que conté el seu propi disc dur per a evitar que siguin modificats sense el seu consentiment.

Adreces recomanades

Podeu obtenir els programaris PGP i GnuPGP als webs respectius d'aquestes organitzacions

Esteganografia

S'anomena *esteganografia*[8] el conjunt de tècniques que permeten d'ocultar o amagar qualsevol tipus de dada. A diferència de la criptografia, l'esteganografia amaga les dades entre altres dades, però no les modifica de manera que no siguin llegibles.

(8)Esteganografia prové del mot grec *stegos* ("coberta") i literalment significa "escriptura oculta".

A tall d'exemple, mitjançant l'ús de tècniques esteganogràfiques, un fitxer d'una imatge digitalitzada podria ocultar dins seu un fitxer de text amb totes les contrasenyes dels usuaris d'un sistema informàtic. Des del punt de vista de l'usuari que examina la imatge, no es podria apreciar cap diferència entre la imatge original i la imatge que oculta les dades confidencials; els dos fitxers tindrien la mateixa mida i tot.

En general, qualsevol fitxer, tant si és una imatge com un document o fins i tot un fitxer de so, és susceptible d'amagar algun tipus d'informació. Encara que les diferències entre el fitxer original i el fitxer *esteganografiat* siguin pràcticament inapreciables, òbviament hi són. Una de les tècniques que es poden fer servir per a ocultar informació en un fitxer consisteix a alterar els bits menys significatius del fitxer original, de manera que en aquestes altera-

S-Tools

Podeu cercar a Internet el programari S-Tools per a fer proves esteganogràfiques.

cions s'emmagatzemi precisament la informació que es vol ocultar. La mida del fitxer *esteganografiat* serà exactament la mateixa que la del fitxer original, però el contingut serà lleugerament i inapreciablement *diferent*.

No hi ha cap mena de dubte que, si la criptografia pot tenir usos delictius, de l'esteganografia encara se'n pot fer un ús més il·legítim. Si es localitza un fitxer xifrat es pot pensar que s'hi amaga alguna cosa confidencial (encara que desxifrar-ho sigui molt complex o gairebé impossible), però en el cas de l'esteganografia, l'anàlisi superficial de les dades ni tan sols pot arribar a crear sospites que algun fitxer contingui informació rellevant. Una tècnica que es pot fer servir per a localitzar fitxers que continguin informació oculta consisteix en la comparació dels valors resum dels fitxers sospitosos amb els valors resum dels fitxers originals. Per exemple, en cas que els fitxers sospitosos siguin fitxers de sistema operatiu, és relativament senzill obtenir els valors resum dels fitxers originals del sistema, els quals es compararan posteriorment amb els valors resum dels fitxers sospitosos per a determinar si han estat tractats amb tècniques esteganogràfiques.

Observació

L'esteganografia és una tècnica de detecció similar a la que es fa servir per a detectar els problemes d'integritat dels fitxers d'un sistema informàtic.

3. Seguretat del sistema

L'objectiu d'aquest mòdul se centrarà en l'estudi de les intrusions i atacs dels quals pot ser objecte un sistema informàtic. Algunes de les tècniques descrites poden semblar obsoletes, però al nostre parer són didàcticament interessants i poden servir de fonament per a comprendre processos més complexos. Així mateix, molts dels sistemes actuals encara funcionen amb sistemes operatius antics, o amb sistemes no actualitzats que, molt probablement, són susceptibles de patir molts dels problemes que es descriuran tot seguit.

Les fases o etapes de les quals sol constar una intrusió són les següents:

1) Etapa prèvia a l'atac: recollida d'informació.

2) Atac inicial.

3) Accés complet al sistema.

4) Instal·lació de *backdoors*, *key loggers*, troians, etc. per a obtenir informació i facilitar futurs accessos de l'atacant.

5) Eliminació d'empremtes.

Hi ha moltíssims sistemes informàtics que, un cop instal·lats, ja no s'actualitzen més, molts cops per por que deixin de funcionar correctament o simplement per desconeixement. És molt important fer les actualitzacions del sistema. En sistemes complexos –on es poden tenir problemes de compatibilitats amb altres equips– o amb programari ja instal·lat, és convenient disposar d'un equip de reserva idèntic al de producció on poder fer les actualitzacions a mode de prova.

Els procediments i eines que s'estudiaran en aquest mòdul es poden utilitzar per a prevenir i detectar les intrusions en un sistema informàtic, si bé també poden ser utilitzades maliciosament per a produir l'efecte contrari.

3.1. Seguretat en el sistema de fitxers

En aquest subapartat considerarem que l'administració d'usuaris, grups i els seus privilegis, i també la de fitxers i directoris, s'ha fet correctament. Tot i que tampoc no en parlarem a fons, també cal tenir en compte les llistes de control d'accés (ACL[9]). Mitjançant les ACL és possible l'assignació de permisos a usu-

[9]ACL són les sigles d'*access control lists*.

Vegeu també

Vegeu els mòduls "Administració de servidors" i "Administració d'usuaris".

aris o grups concrets. Això pot ser útil en cas que dos usuaris que pertanyen a grups diferents necessitin els mateixos permisos a l'hora d'accedir a uns determinats directoris.

Exemple de llistes de control d'accés

En un projecte interdisciplinari entre professors del departament d'informàtica i el de filosofia (tots dos grups d'usuaris amb perfils perfectament definits dins de cada departament), podria requerir que els components del projecte haguessin d'accedir als mateixos directoris, necessitat que es podria satisfer amb la creació de l'ACL corresponent.

3.2. Atacs a contrasenya

Malgrat l'existència de molts mecanismes d'autenticació, el cert és que avui en dia la via d'entrada més comuna per accedir a un sistema informàtic és l'ús del nom d'usuari acompanyat de la corresponent contrasenya. En conseqüència, la política de gestió i manteniment de contrasenyes és vital per a garantir la seguretat del sistema.

En aquest subapartat estudiarem amb cert detall el fitxer de contrasenyes de sistemes Unix/Linux. Malgrat la seva especificitat, molts dels conceptes que apareixen en aquest subapartat són fàcilment extrapolables a altres sistemes operatius i útils per a comprendre com funcionen els atacs a contrasenya.

3.2.1. El fitxer */etc/passwd* en Unix/Linux

La finalitat d'aquest tipus d'atac consisteix a esbrinar o desxifrar, esborrar, modificar o inserir contrasenyes en el fitxer que les emmagatzema. En els sistemes Unix cada nom d'usuari (*login name*) té una entrada, juntament amb la contrasenya xifrada respectiva, en el fitxer */etc/passwd*. Per al bon funcionament del sistema aquest fitxer ha de tenir permisos de lectura per a tots els usuaris.

Observació

El fitxer */etc/passwd* també conté comptes d'usuaris *no reals*, relatius a diversos serveis del sistema. Cal eliminar els que no s'han d'utilitzar.

Les entrades del fitxer */etc/passwd* tenen el format que es pot veure en l'exemple següent (el símbol ":" actua d'element separador entre els diferents camps):

```
Pere:HGY89fgf801we:UID:GID:informació d'usuari:directori de treball de l'usuari:
<i>shell</i> per defecte de l'usuari
```

Els camps que ens interessen són, bàsicament, el primer camp (nom de *login* de l'usuari), i el segon, la contrasenya xifrada de l'usuari. Els camps UID i GID representen, respectivament, l'identificador (únic) de l'usuari i l'identificador del grup de l'usuari.

Quan un usuari entra al sistema, la contrasenya del fitxer */etc/passwd* no es desxifra (ja que l'algorisme de xifratge és unidireccional), sinó que es xifra la contrasenya introduïda per l'usuari fent servir el mateix algorisme de xifrat simètric i es compara amb la contrasenya xifrada del fitxer */etc/passwd*. En cas que coincideixin, l'usuari estarà autoritzat a entrar. Atès el caràcter unidireccional de l'algorisme de xifrat, la manera més evident de trencar les contrasenyes del fitxer */etc/passwd* serà l'ús de tècniques de força bruta (explorant tot l'arbre de possibilitats i, per tant, en general molt lent). A més, però, també es poden utilitzar els anomenats **atacs de diccionari.**

Atacs de força bruta

Les contrasenyes de longitud curta poden ser desxifrades ràpidament amb atacs de força bruta.

Com ja s'ha esmentat anteriorment, el fitxer */etc/passwd* ha de romandre amb permisos de lectura per a tots els usuaris, de manera que resulta relativament senzill visualitzar o obtenir el contingut del fitxer */etc/passwd*, localment o remotament. Una vegada es disposa d'aquest fitxer, es podran mirar d'esbrinar les contrasenyes, simplement xifrant totes les paraules contingudes en un fitxer de diccionari (s'anomenen d'aquesta manera els fitxers ASCII que contenen molts mots d'un idioma determinat o d'un tema concret: esports, música, etc.) i comparant el resultat amb les contrasenyes xifrades del fitxer */etc/passwd*. Si alguna de les contrasenyes xifrades coincideix amb el resultat de xifrar un mot del diccionari, haurem obtingut una clau d'accés al sistema d'una manera no autoritzada.

En realitat, el procés de xifrar tots els mots d'un diccionari és més complex del que s'ha explicat, ja que no hi ha un únic xifratge per a cada mot. A l'hora de xifrar un mot (és a dir, en el moment en què es va crear o bé es va canviar la contrasenya), cal tenir en compte 12 bits (anomenats *salt* en anglès) que proporcionen 4.096 codificacions diferents per a cada mot (el valor del rang de 0 a 4.095 es tria segons l'hora del sistema).

Així, doncs, cada mot del diccionari haurà de ser codificat 4.096 vegades per a assegurar que no ens deixem cap possibilitat per explorar. Val a dir, però, que la presència dels bits de *salt* no dificulta (computacionalment no representa un cost insalvable) el trencament de les contrasenyes, però permet que dos usuaris que tinguin la mateixa contrasenya apareguin xifrats d'una manera diferent en el fitxer */etc/passwd*.

La creació de contrasenyes fortes dificulta en gran manera els atacs basats en l'ús de diccionaris. En aquest sentit, l'administrador disposa de diverses eines que permeten de comprovar la qualitat de les contrasenyes dels usuaris del sistema. Per exemple, les aplicacions *npasswd* o *passwd+* (entre d'altres) permeten l'anomenada *comprovació proactiva de contrasenyes*, la qual permetrà d'eliminar

Vegeu també

Recordeu que al subapartat 2.1 hem vist algunes recomanacions per a la creació de contrasenyes.

les contrasenyes que, segons una sèrie de criteris, siguin considerades febles. Així, doncs, en cas que un usuari esculli una contrasenya que no satisfà aquests criteris, es veurà obligat a triar-ne una altra.

Rebuig de contrasenyes

Es poden rebutjar, per exemple, les contrasenyes que:

- No tinguin com a mínim un cert nombre de caràcters.
- Les que es basin en dades conegudes de l'usuari o de l'organització (tant si estan del dret com a l'inrevés).
- Les que no barregin minúscules i majúscules.
- Les formades per paraules de diccionaris, etc.

A més, l'administrador també pot executar amb una certa periodicitat (i amb l'autorització per a fer-ho), eines com per exemple *Crack* o *John the Ripper* per a fer atacs de diccionari sobre el mateix fitxer de contrasenyes i poder comprovar-ne d'aquesta manera la robustesa. Aquestes eines automatitzen el procediment d'atac basat en diccionaris i fins i tot permeten de dur a terme atacs de força bruta, efectius quan les contrasenyes tenen un nombre de caràcters molt reduït.

3.2.2. Ocultació de contrasenyes en Unix: el fitxer */etc/shadow*

Mitjançant la tècnica d'ocultació de contrasenyes[10], les contrasenyes xifrades que abans es podien localitzar al fitxer */etc/passwd* (amb permís de lectura per a tots els usuaris), ara passen a localitzar-se al fitxer */etc/shadow*, el qual únicament podrà ser llegit per l'usuari *root*. Les entrades del fitxer de contrasenyes */etc/passwd* són idèntiques a les que hem vist anteriorment, amb l'excepció que ara el camp de la contrasenya contindrà un símbol (generalment una *x*) que indicarà la localització de la contrasenya en el fitxer */etc/shadow* als programes que ho requereixin:

(10)La tècnica d'ocultació de contrasenyes rep en anglès el nom de *shadowing*.

```
Pere:<b>x</b>:500:100:Pere Joan:/export/home:/bin/bash
```

A més, cada usuari tindrà una entrada en el fitxer */etc/shadow* que contindrà el nom d'usuari, la contrasenya xifrada i una sèrie de camps que serveixen per a implementar mecanismes d'envelliment de contrasenyes (*agin password*), els quals no es detallaran, ja que excedeixen els propòsits d'aquests materials:

```
Pere:<b>HGY89fgf801we</b>:120078:0::7:10::
```

En l'actualitat, en moltes distribucions de Linux l'opció de *shawdowing* es troba activada per defecte i, de vegades, ni tan sols es pot desactivar.

3.3. Codi maliciós i amenaces lògiques

S'anomena *codi maliciós*[11] qualsevol fitxer que pugui resultar perniciós per a un sistema informàtic.

(11)En anglès, *malware*.

Algunes vegades, el codi maliciós es pot inserir dins d'un programa "autoritzat". El codi maliciós també pot estar ocult i provocar tota mena de danys com, per exemple, l'esborrament de dades o l'enviament d'informació confidencial de l'usuari per correu electrònic. En altres ocasions, el codi maliciós no s'insereix dins d'un programa autoritzat, sinó que apareix com un nou pro-

gramari que desenvolupa alguna funció útil. L'usuari l'executa amb una finalitat i el programa, en virtut del codi maliciós que conté, duu a terme accions desconegudes per l'usuari.

El codi maliciós, en totes les seves múltiples variants, es pot enquadrar dins el que s'anomenen les *amenaces lògiques* (de les quals, els virus i els troians són els elements més representatius):

- **Programari incorrecte**. Consisteix en l'aprofitament de vulnerabilitats accidentals del programari (errors de programació) amb finalitats destructives. Dit d'una altra manera, consisteix a utilitzar el programari amb un objectiu diferent de l'objectiu amb què va ser concebut. Aquestes vulnerabilitats reben el nom genèric d'errors[12] i el programari que s'utilitza per a aprofitar-les s'anomena *exploit*. Per a evitar aquest tipus de problema és fonamental estar al dia de tots els forats de seguretat que presenta el nostre programari mitjançant una subscripció en llistes o fòrums de seguretat que publiquen aquestes vulnerabilitats i expliquen on es poden trobar les actualitzacions del programari que les solucionen.

[12]En anglès, *bug*.

Adreça recomanada

Hi ha moltes llistes de correu de seguretat que aporten informació de vulnerabilitats i actualitzacions diàriament. Per exemple, a Hispasec Sistemas.

- **Eines de seguretat mal emprades**. Escàners, detectors[13], programari per a atacar contrasenyes, etc.

[13]Detector en anglès s'expressa com a *sniffer*.

Vegeu també

Els escàners i els detectors s'estudien als subapartats 3.4 i 3.5.

- **Bombes lògiques**. Són parts de codi d'un programari que es manté inert fins que no es produeix una certa condició que l'activa (una data, una seqüència de tecles, etc.). Alguns programadors maliciosos insereixen aquestes parts de codi en els seus programaris amb la intenció d'activar-les si són acomiadats de l'organització en què treballen.

- **Virus**. Habitualment, els virus són seqüències de codi que s'insereixen en un fitxer executable (anomenat *hoste*) de manera que quan s'executa també ho fa el virus. La principal qualitat és l'autoreplicació, és a dir, la capacitat d'inserir-se en altres programaris del sistema informàtic atacat. Poden tenir efectes summament destructius (o simplement perseguir la replicació): format d'un disc dur, esborrament de fitxers, disminució del rendiment del sistema, etc. Els virus constitueixen un dels problemes de codi maliciós més importants en sistemes informàtics basats en Windows.

  Pel que fa als programaris antivirus, a més dels basats en la recerca de patrons vírics dins els fitxers infectats, també hi ha diversos productes que sota la denominació d'antivirus actuen en realitat com a programaris protectors de la integritat del sistema, i permeten tan sols la instal·lació de programari autoritzat (signat digitalment pel fabricant).

Tipus de virus

Hi ha molts tipus de virus: de sector d'inici, de macro, multiplataforma, multiprocés, de compressió (com a forma d'ocultació), interpretat, sobreescrits (destrueixen el fitxer) o afegits (el conserven), etc.

- **Cucs**. Similars al virus, un cuc és un programa que és capaç d'autoexecutar-se amb la finalitat de propagar-se per la xarxa i col·lapsar l'amplada de banda dels sistemes atacats o danyar-ne els ordinadors (poden anar acompanyats de virus).

Observació

Un dels incidents de seguretat més importants que han tingut lloc a Internet va ser producte d'un cuc l'any 1988 i va provocar la caiguda de milers de màquines.

- **Troians**. Són parts de codi inserides en el programari que habitualment s'utilitza en el sistema. Aquest codi es manté ocult i duu a terme tasques diverses sense que l'usuari o l'administrador se n'adonin. Camuflat sota l'aparença d'un programari útil o habitual, no solen ocasionar efectes destructius. Generalment capturen contrasenyes i altres dades confidencials i les envien per correu electrònic a la persona que ha introduït el troià dins el sistema atacat. També poden obrir forats de seguretat que posteriorment podran ser aprofitats per l'atacant. Realment, els efectes dels troians poden arribar a ser molt perniciosos i el seu ús pot ser font de delictes. Per exemple, mitjançant un troià és possible activar remotament una càmera web (*webcam*) i gravar l'usuari destí amb total desconeixement per part d'aquest.

Exemple de troià

Un exemple molt conegut de troià és el programari *BackOrifice*, una eina d'administració remota per a sistemes Windows 95/98.

- ***Backdoors***. Són portes d'entrada a sistemes operatius i programaris, inserides pels mateixos dissenyadors o programadors, que els permeten d'accedir a l'aplicació i evitar tots els mecanismes d'autenticació.

Vegeu també

Vegeu el subapartat 2.2.2. relatiu al PGP.

- ***Phishing***. Pràcticament tots els usuaris d'Internet hem hagut de patir la recepció de correus electrònics que, fent-se passar com a "fiables" i procedents d'entitats bancàries reals, ens sol·liciten informació confidencial que una veritable entitat bancària mai sol·licitaria a través del correu electrònic. Els *links* o vincles d'aquests correus ens remeten a llocs web falsos i que no corresponen a l'entitat bancària real.

Pharming

El *pharming,* en el qual s'explota una vulnerabilitat en el programari dels servidors o dels usuaris, permet que l'atacant redirigeixi un nom de domini a una altra màquina diferent. És una variant molt tècnica d'efectes similars al *phishing.*

- ***Hoax***. Tant "popular" com el *phishing* o l'*spam*, un *hoax* no és més que un correu electrònic en què s'avisa de l'existència de virus (naturalment falsos) d'efectes devastadors contra els quals no existeix cap antivirus que els pugui detectar.

- ***Adware***. És un programari que mostra publicitat diversa. Habitualment s'instal·la sense el consentiment de l'usuari.

- ***Spyware* o programari espia**. És un programari que envia dades a empreses sobre els nostres hàbits d'Internet. Com de costum, solen instal·lar-se sense el permís de l'usuari. Hi ha múltiples solucions per a "netejar" els nostres sistemes d'aquesta mena de programaris.

A continuació estudiarem les diferents tècniques que es poden fer servir per a detectar i prevenir la presència de codi maliciós en el nostre sistema informàtic. Segons la configuració del sistema, la detecció del codi maliciós (normalment fitxers compilats) serà una tasca més o menys complicada. Per exemple, si es coneix la darrera data d'actualització del sistema i es localitza algun fitxer

de sistema *posterior* a aquesta data, es pot pensar en la presència de codi maliciós. En aquest sentit, pot resultar de molta ajuda l'observació dels paràmetres següents:

- Darrera data de modificació dels fitxers.
- Data de creació dels fitxers.
- Mida dels fitxers.

Malauradament, les dates i mides dels fitxers es poden alterar amb facilitat i, per tant, no són una font d'informació segura. Una vegada més, les funcions resum ens poden ser de molta utilitat per a garantir la integritat de tot el sistema. Aquestes funcions resum permeten d'obtenir el que podríem anomenar una "empremta" única d'un fitxer o conjunt de fitxers. Així, doncs, l'administrador pot obtenir en qualsevol moment una instantània o empremta "única" del sistema informàtic fent servir funcions resum.

Vegeu també

Recordeu que les funcions resum s'han estudiat a l'apartat 2 d'aquest mòdul.

Qualsevol alteració d'un fitxer, per mínima que sigui, provocarà que quan l'administrador torni a calcular la funció resum, obtingui un resultat diferent. L'eina més coneguda per a dur a terme aquesta funció rep el nom de *Tripwire* (hi ha versions per Linux, Unix i Windows). És configurable, inclou un llenguatge de macros per a poder automatitzar tasques i fa servir diversos algorismes de resum (entre els quals l'algorisme MD5[14]). El funcionament de *Tripwire* és el següent: una vegada s'ha instal·lat el sistema, s'obté un resum de cada fitxer rellevant i s'emmagatzema en una base de dades.

(14)Recordeu que MD5 són les sigles de *message digest*.

Quan l'administrador vol comprovar la integritat del sistema, executa *Tripwire* i si s'ha produït algun canvi en algun fitxer, es generarà el senyal d'avís corresponent en el fitxer de sortida de l'aplicació. El funcionament correcte d'aquest procediment només es pot garantir si la base de dades on es guarden les sortides resum no és modificable per cap usuari. Això es pot aconseguir fent que la base de dades tingui atribut de només lectura, o millor encara, emmagatzemant-la en un medi que no admeti reescriptures com, per exemple, un CD-ROM.

Com que hi ha alguns fitxers del sistema que poden variar sovint (per exemple, el fitxer de contrasenyes), *Tripwire* permet d'actualitzar la base de dades sense tornar a calcular el resum sencer de tot el sistema. Tingueu present que convé obtenir el primer resum del sistema abans d'obrir-lo als usuaris.

3.4. Detectors

S'anomenen *detectors*[15] els programes que permeten la captura i l'enregistrament de la informació que circula per una xarxa.

(15)Detector en anglès s'expressa com a *sniffers*.

El seu funcionament es basa en l'activació del mode promiscu de les interfícies de xarxa de les estacions de treball. Amb l'activació d'aquest mode, l'estació de treball podrà monitoritzar, a més dels paquets d'informació que s'hi adrecen d'una manera explícita, el trànsit sencer de la xarxa. Això inclou, per exemple, la captura de noms d'usuari i contrasenyes, o fins i tot la intercepció de correus electrònics (o qualsevol altre document confidencial).

Carnivore

El programari Carnivore (DCS 1000) és una aplicació semblant a un *sniffer*. S'instal·la en els proveïdors de serveis d'Internet i permet la vigilància i interceptació de les comunicacions a través de la xarxa.

L'activitat dels detectors és difícilment detectable perquè no en queden empremtes enlloc. No podem tenir constància de la informació que pot haver estat interceptada per l'acció dels detectors (si no és de manera indirecta, per mitjà dels atacs que pot patir el sistema informàtic).

No obstant això, es poden fer servir mesures de protecció d'abast més general. Per exemple, si es xifren els documents que s'envien per la xarxa amb PGP, encara que puguin ser interceptats, molt difícilment podran ser desxifrats per l'espia. Malauradament, les eines criptogràfiques protegeixen la informació que circula, però no permeten d'establir connexions segures.

Wireshark

El detector per excel·lència s'anomena Wireshark (conegut com a Ethereal fins a l'any 2006) i té versions per a Unix i Windows.

Per aquest motiu, és de vital importància la instal·lació d'altres eines com, per exemple, un servidor de Secure Shell (SSH) i les respectives utilitats dels clients. Secure Shell permet l'establiment d'inicis de sessió segurs i es pot fer servir com a substitut de la comanda Telnet. Una vegada instal·lat, configurat i iniciat el servidor, l'ús de les diferents utilitats dels clients es pot executar d'una manera molt senzilla i similar a l'habitual *Telnet*, motiu pel qual la utilització de Secure Shell no necessita cap fase d'aprenentatge.

Finalment, notem que els detectors tenen molts avantatges per a l'administrador del sistema, no només per monitoritzar, per exemple, el flux d'informació que circula per la xarxa, sinó per protegir-se de moltes amenaces. Per exemple, si sospitem que el nostre sistema ha estat **troianitzat**, podem monitoritzar-lo amb un detector per esbrinar-ne els efectes.

3.5. Escàners

Els escàners són eines de seguretat que serveixen per a detectar les vulnerabilitats d'un sistema informàtic. En general, es poden dividir en dues categories: els escàners de sistema i els escàners de xarxa.

Els **escàners de sistema** s'utilitzen per a detectar les vulnerabilitats del sistema informàtic local: problemes de configuració, permisos erronis, contrasenyes febles, etc.

Els **escàners de xarxa** analitzen els serveis i ports disponibles d'*hostes* remots a la recerca de debilitats conegudes que puguin aprofitar els atacants (en certa manera, doncs, automatitzen les tasques que duria a terme un intrús remot).

Un **port** indica un punt pel qual entra o surt la informació d'un ordinador. Els protocols relatius a Internet (FTP, Telnet, etc.) utilitzen, emissor i receptor, un port de sortida i recepció comú en ambdós extrems de la comunicació. L'anomenat **escaneig de ports** consisteix a esbrinar els ports TCP/UDP[16] que estan oberts en una màquina remota pertanyent a una xarxa determinada. Els ports oberts constitueixen una informació molt interessant per als possibles intrusos, ja que les vulnerabilitats dels serveis que es troben oberts o en funcionament poden permetre, en ser aprofitades o "explotades", l'accés no autoritzat al sistema. L'assignació dels ports no és arbitrària i és determinada per la Internet Assigned 1bers Authority (IANA).

[16]TCP és la sigla de *transmission control protocol* i UDP, de *user datagram protocol*.

Altres funcions de la IANA

La Internet Assigned 1bers Authority també és responsable de la coordinació i manteniment del Sistema de Noms de Domini (DNS).

Exemples d'assignació de ports a serveis d'Internet

```
Port TCP/UDP 20: FTP (dades)
Port TCP/UDP 21: FTP (control)
Port TCP/UDP 23: Telnet
Port TCP/UDP 25: SMTP
Port TCP/UDP 53: DNS
Port TCP/UDP 80: HTTP
Port TCP/UDP 110: POP3
Port TCP/UDP 194: IRC
```

Comanda NETSTAT

La comanda *NETSTAT* (vàlid tant per a sistemes Windows com Unix) pot oferir informació sobre les connexions establertes i els números de port que s'estan emprant.

Els ports situats a partir del 1024 fins al 65535 s'anomenen **ports registrats**, no es troben sota el control de la IANA[17] i poden ser utilitzats per determinades aplicacions. Per exemple, una aplicació client d'una eina de control remot podria utilitzar un port d'aquest rang per realitzar les seves tasques i passar desapercebut per l'usuari local o l'administrador del sistema.

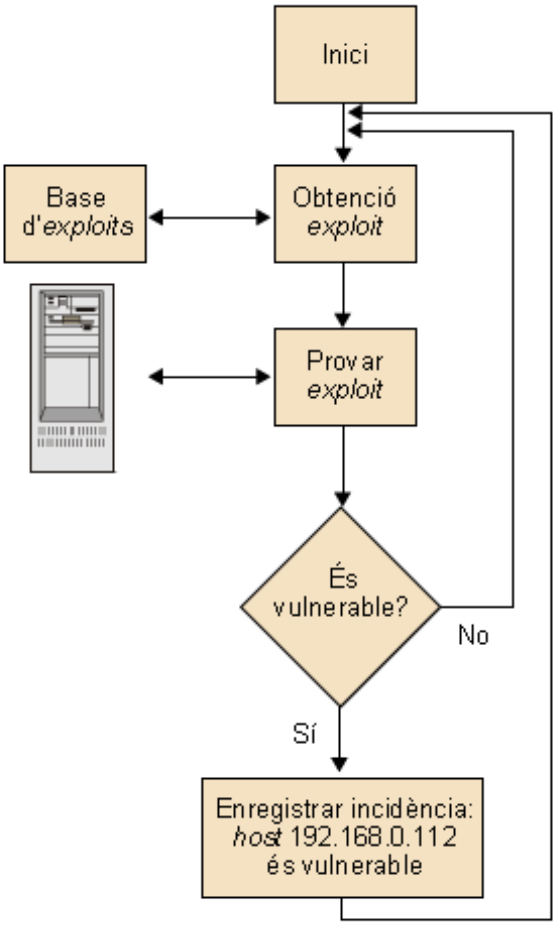
[17]Recordeu que IANA són les sigles de la Internet Assigned 1bers Authority.

Tots els escàners, tant si són de sistema com de xarxa, comparteixen en trets generals un esquema de funcionament similar. Per exemple, el diagrama de flux següent representa l'algorisme, a grans trets, que seguiria un escàner de xarxa:

Vegeu també

Vegeu l'aspecte legal de l'ús dels escàners en l'apartat 4 d'aquest mòdul.

Algorisme d'un escàner de xarxa



Tot i que els escàners són eines de molta utilitat per als administradors dels sistemes informàtics, val a dir que els intrusos també en poden fer un ús maliciós. Els escàners permeten l'automatització de centenars de proves per a localitzar les vulnerabilitats d'un sistema. D'altra banda, el possible intrús no cal que conegui amb precisió les vulnerabilitats del sistema; simplement utilitza la informació que li proporciona l'escàner, sense necessitat de ser un expert informàtic.

L'anàlisi de les vulnerabilitats d'una xarxa o sistema informàtic, en definitiva, l'estudi de la seva seguretat, des del punt de vista del que faria un intrús, rep el nom de **test de penetració**.

Tot i que al començament els escàners només analitzaven entorns Unix, en l'actualitat n'hi ha per a tot tipus de plataformes. Per exemple, l'eina Nessus és capaç d'avaluar tant entorns Windows com Unix.

3.6. Atacs de denegació de servei

S'anomenen **atacs de denegació de servei** (DoS[18], per *denial of service*) tota acció iniciada per una persona o per altres causes, que inutilitza el maquinari i/o programari, de manera que els recursos del sistema no siguin accessibles des de la xarxa.

[18]DoS és acrònim de l'expressió anglesa per a atac de denegació de servei (*denial of service*).

[19]En anglès, *distributed denial of service*.

Els atacs de denegació de servei poden atacar el maquinari de la xarxa, el sistema operatiu, i fins i tot les aplicacions del sistema. Els atacs DoS[18] poden implicar altres ordinadors intermediaris (fins i tot milers), amb la qual cosa s'aconsegueix un dany encara més gran. A més, l'atacant pot ocultar la seva adreça IP gràcies als ordinadors pont (anomenats **zombies**). Aquests tipus d'atacs s'anomenen atacs de denegació de servei distribuïts[19] (DDoS).

Exemples d'atacs DoS

Hi ha altres tipus d'atacs DoS: Smurf, Fraggle, Ping of death, Teardrop, etc.

Exemple d'atac DoS: l'atac SYN

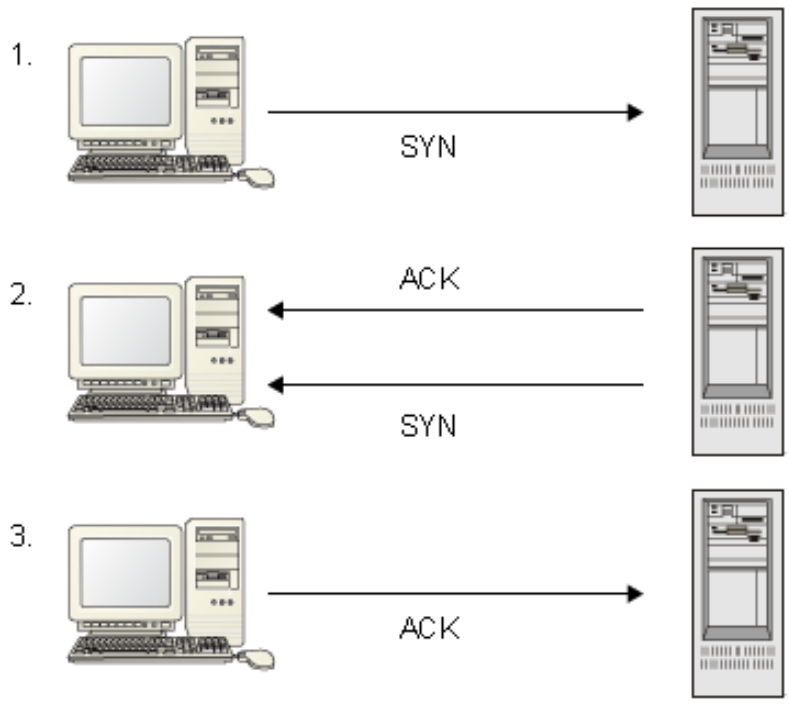
Aquest atac consisteix en l'enviament, per part del sistema atacant, d'un gran nombre de sol·licituds de connexió per segon. El sistema atacat respon correctament les sol·licituds de connexió, però en no obtenir resposta del sistema atacant, es col·lapsa i no pot atendre les sol·licituds de connexió legítimes. Aquest atac es basa en el *modus operandi* del protocol d'establiment de sessió entre client i servidor (vegeu la figura):

1) L'ordinador client envia una sol·licitud de sincronització (SYN) al servidor.

2) El servidor respon amb un missatge ACK (*acknowledgement*) i un missatge de sincronització al client.

3) En resposta a la sol·licitud de sincronització, l'ordinador client envia una resposta ACK al servidor.

Protocol d'establiment de sessió en 3 passos



El servidor manté en cua d'espera tots els paquets SYN/ACK que va rebent, fins que són cancel·lats per l'enviament del corresponent ACK per part del client (o bé expira un temporitzador que regula el temps d'espera). L'atac SYN es produeix quan els paquets enviats per l'emissor contenen adreces IP errònies i, en conseqüència, el servidor mai podrà rebre el paquet ACK que deslliuraria la cua de recepció. Així, quan aquesta s'omple, les noves i legítimes sol·licituds de connexió no es podran servir.

3.7. Auditoria i fitxers *log*

S'anomena *logging* el procediment mitjançant el qual s'enregistren en un fitxer les activitats que succeeixen en un sistema operatiu o en una aplicació. Aquest fitxer, anomenat genèricament *log*, recull, per dir-ho d'alguna manera, les "empremtes" de tot el que ha succeït en un sistema informàtic, incloent-hi l'origen dels possibles atacs de què hagi estat objecte.

3.7.1. Els fitxers de *log* d'Unix/Linux

A diferència d'altres sistemes operatius (com, per exemple, Windows), Unix/Linux presenta un gran nombre de comandes i fitxers relacionats amb les tasques de *logging*:

- ***syslog***: fitxer de text que emmagatzema (segons un fitxer de configuració anomenat *syslog.conf*) informació diversa relativa a la seguretat del sistema com, per exemple, els accessos a determinats serveis, l'adreça IP d'origen, etc. És el fitxer *log* més important del sistema Unix.

Seguretat dels fitxers *log*

Molts fitxers *log* són fitxers de text i, per tant, poden ser fàcilment modificats i/o esborrats pels intrusos amb la finalitat d'esborrar o canviar els indicis de la seva activitat.

- ***lastlog***: aquesta comanda informa del darrer inici de sessió[20] dels usuaris continguts en */etc/passwd*. Aquesta informació es troba en el fitxer */var/log/lastlog*. Els intrusos utilitzen programaris especialitzats per a esborrar les empremtes en aquest fitxer (és un fitxer binari i, per tant, no es pot reescriure fàcilment).

[20]Inici de sessió en anglès s'expressa com a *login*.

Localització dels fitxers *log*

La localització dels fitxers *log* pot variar sensiblement segons l'Unix –o segons la distribució de Linux que es faci servir. Normalment es troben a */var/log*.

- ***last***: la comanda *last* proporciona informació relativa a cada connexió i desconnexió al sistema. Aquesta informació es troba emmagatzemada en el fitxer */var/log/wtmp*. Les mateixes observacions que s'han fet per a la comanda *lastlog* són aplicables en aquest cas.

Comanda *last*

La comanda *last* proporciona la següent informació: usuaris, terminal o servei utilitzat en el login, adreça IP, data i hora, durada de la sessió, etc.

- ***utmp***: fitxer que emmagatzema els usuaris que es troben connectats al sistema informàtic en un moment determinat. La comanda *who* cerca els usuaris en aquest fitxer. També és un fitxer binari.

- ***messages***: fitxer que enregistra activitats diverses del sistema (usuaris connectats, la seva adreça IP, missatges de nucli[21], etc. –és possible configurar

[21]Nucli en àngles s'expressa com a *kernel*.

la informació que es vol emmagatzemar). És un fitxer de text i, per tant, es pot visualitzar amb la comanda *cat* o modificar-lo d'una manera molt senzilla amb la comanda *grep* o un editor de text qualsevol.

Una bona estratègia per a evitar que els intrusos puguin esborrar les empremtes en els fitxers *log*, consisteix en l'ús d'eines de *logging* diferents de les proporcionades pel sistema operatiu que mantinguin els seus propis fitxers d'activitat, independentment dels que pugui fer servir el sistema operatiu.

No són les úniques comandes i fitxers de què disposa Unix per a dur a terme les tasques de *logging*. D'altra banda, el volum d'informació que pot generar l'activitat d'un sistema informàtic és tan enorme que calen eines especialitzades a dur a terme tasques d'auditoria. Per exemple, *logrotate* serveix per a establir sistemes de rotació de *logs* (configurable a partir del fitxer */etc/logrotate.conf*), la qual cosa consisteix en comprimir cada cert temps els *logs* objecte d'interès i emmagazemar-los només fins a una certa antiguitat.

3.7.2. Els fitxers *log* i la investigació de delictes informàtics

De tot el que s'ha vist fins ara es desprèn fàcilment que la informació continguda en els fitxers *log* (tant locals al nostre sistema, com els remots, allotjats, per exemple, en els proveïdors de serveis d'Internet o altres sistemes) és molt important en la investigació de qualsevol incident de seguretat. Els proveïdors de serveis d'Internet, segons la Llei de serveis de la societat de la informació i comerç electrònic (LSSICE), només tenen l'obligació de mantenir el fitxer de *log* durant un temps màxim de 12 mesos, però no hi ha cap mínim exigible, motiu pel qual és necessari actuar ràpidament en cas de presumpte delicte.

De tot això es desprèn que la seguretat és molt important i s'ha de tenir en compte des del primer moment en què es dissenyen l'estructura de la xarxa de l'empresa i l'estructura del departament d'informàtica. Hi ha empreses en què el departament de seguretat depèn directament de la direcció i en d'altres està dins el departament d'informàtica o en el de sistemes.

La seguretat, en molts casos, passarà per sobre d'altres requisits, però en general s'ha d'arribar a un conveni entre seguretat i usabilitat.

El director d'informàtica ha de veure la seguretat com una part molt important, i per això ha de tenir una partida en el pressupost directe per a temes que hi estiguin relacionats.

4. Aspectes legals de la seguretat informàtica. Marc jurídic penal i extrapenal. El "delicte informàtic"

El "delicte informàtic" no apareix explícitament definit en l'actual codi penal (1995) ni a les reformes posteriors que se n'han realitzat i, per tant, no es podrà parlar de "delicte informàtic" pròpiament dit, sinó de delictes fets amb el concurs de la informàtica o les noves tecnologies, en els quals l'ordinador s'erigeix com a mitjà d'execució del delicte, o bé com a objectiu d'aquesta activitat (per exemple, una intrusió en un sistema informàtic). L'objectiu d'aquest apartat no és alliçonar els administradors o directors d'un sistema informàtic, sinó tan sols fer-los conèixer les responsabilitats en què poden incórrer a causa del seu treball i, com a fita principal, dotar-los de mecanismes que, en cas d'accions delictives que tenen per objecte els sistemes que administren dels quals són responsables, els permetin de denunciar els delictes dels quals han estat víctimes i sol·licitar les actuacions legals pertinents.

D'altra banda, tampoc no es pretén fer un recull excessivament generós en llenguatge jurídic, ni aprofundir en possibles sentències relacionades amb els delictes que s'explicaran en aquest mòdul. La legislació actual encara presenta buits pel que fa als mal anomenats "delictes informàtics", de manera que tan sols s'oferiran directrius bàsiques, més aviat relacionades amb el sentit comú i els articles del codi penal (entre altres normes), que no pas amb la complexa normativa que es va generant entorn d'aquesta nova problemàtica.

El vessant tecnològic o científic dels estudis d'enginyeria sovint deixa de banda el vessant social de l'aplicació dels avenços que es van produint en aquestes disciplines. Consegüentment, l'administrador d'un sistema pot ser molt competent en el treball tècnic, però és possible que tingui molts dubtes a l'hora de tractar problemes com els següents:

- Si el meu cap em demana que li mostri el contingut de la bústia de correu personal d'un treballador, tinc l'obligació de fer-ho?

- S'ha produït un accés no autoritzat al servidor i els intrusos han modificat la pàgina web del departament. Aquest fet és denunciable? A qui ho he de denunciar?

- El servidor emmagatzema dades de caràcter personal. S'han de protegir amb algunes mesures de seguretat determinades?

- És legal la utilització d'escàners (entesos com a eines d'administració de sistemes)?

- Puc penjar a Internet una pàgina web amb les fotografies i logotips del meu grup de música preferit?
- Com puc denunciar l'ús de còpies no autoritzades de programari?
- Puc fer servir eines criptogràfiques per a protegir la informació?
- Els administradors de sistemes d'hostatge[22] són responsables dels continguts que allotgen les pàgines web dels clients?

[22]En anglès, *hosting*.

En aquest apartat intentarem orientar-vos en relació amb els dubtes que s'han expressat, si bé cal ser conscient que no hi ha una línia d'actuació única i que les particularitats de cada cas fan que calgui ser molt prudent a l'hora d'enfrontar-se amb aquest tipus de problemes. En definitiva, cal tenir molt present que no tot allò que és tècnicament possible és legal, i que el desconeixement de les normes no exonera de responsabilitat (penal o no) el treballador informàtic.

4.1. Marc jurídic penal de les conductes il·lícites vinculades a la informàtica

En aquest subapartat s'estudiaran les sancions previstes pel codi penal (en moltes ocasions, penes privatives de llibertat). Com es veurà, algunes de les accions plantejades pels dubtes de l'apartat anterior poden originar responsabilitat penal. Altres, però, tindran la consideració d'**extrapenals**, entenent amb aquest nom, la branca de l'ordenament jurídic que conté sancions menys greus que les previstes pel dret penal (dret administratiu, dret civil, dret laboral, etc.).

4.1.1. Delictes contra la intimitat

L'article 197.1 de l'actual Codi penal (a partir d'ara CP) assimila la intercepció del correu electrònic amb la violació de la correspondència.

Dret a la intimitat

La Constitució espanyola reconeix el dret a la intimitat en l'article 18.

Així, doncs, seran constitutives de delicte les conductes següents:

- L'apoderament de papers, cartes, missatges de correu electrònic o qualsevol altre document o efectes personals.
- La intercepció de les telecomunicacions.
- La utilització d'artificis tècnics d'escolta, transmissió, gravació o reproducció de so, o de qualsevol altre senyal de comunicació.

Detecció i monitorització

La detecció (*sniffing*) és una activitat que es podria emmarcar dins l'article 197.

La utilització d'eines de monitorització de l'activitat d'un sistema en el terminal d'un treballador (sense el seu consentiment) també es podria incloure en l'article 197.

Per a ser constitutives de delicte, aquestes activitats s'han de produir sense el consentiment de l'afectat (ni autorització judicial motivada) i amb la intenció de descobrir-ne els secrets o vulnerar-ne la intimitat.

Per tant, obrir la bústia d'un correu electrònic que no sigui el nostre propi i llegir els missatges que s'hi emmagatzemen podria esdevenir una conducta constitutiva de delicte. Cal anar amb molt de compte amb aquest tipus d'accions i, com a norma general, mai no s'ha de llegir cap correu electrònic que no vagi adreçat a nosaltres mateixos.

El rerefons de la intercepció empresarial del correu electrònic és gairebé sempre el mateix: el dret de les organitzacions a controlar els seus mitjans de producció. En aquest sentit, diverses sentències que s'han dictat en els tribunals en relació amb l'ús dels mitjans de l'empresa amb finalitats personals, s'han pronunciat a favor de l'empresa, ja que s'entén que els mitjans pertanyen a l'empresa i que aquest no és un lloc adient per a enviar i rebre missatges de caràcter privat (o fer altres activitats personals, com ara l'ús dels jocs que s'inclouen en els sistemes operatius).

Sentències a favor de l'empresa

Hi ha diverses sentències que s'han dictat a favor de l'empresa en relació amb l'ús dels mitjans de l'empresa amb finalitats personals. Per exemple, la sentència del Tribunal Superior de Justícia de Catalunya (TSJC) núm. 9382/2000, de 14 de novembre, en relació amb l'acomiadament d'un treballador d'una entitat bancària.

També hi ha els casos de les sentències de la Sala Social del TSJC de data 29-01-2001 i el cas de la Sala Social del TSJC de data 23-10-2000.

Una manera útil per a fer saber als usuaris d'una organització quins són els usos correctes dels mitjans de l'empresa, i les seves limitacions, consisteix en l'ús de contractes en els quals s'especifica, per exemple, quines obligacions i responsabilitats té un usuari d'un compte de correu electrònic. D'altra banda, també és important que els sindicats en tinguin coneixement i que, per tant, els treballadors sàpiguen que se'ls pot sotmetre a certes mesures de control, les quals, més que basar-se en l'obertura dels correus electrònics, ho haurien de fer en l'ús de controls menys lesius, com per exemple, l'estudi del nombre de bytes transmesos, entre altres.

Usurpació i cessió de dades reservades de caràcter personal

La resta d'apartats de l'article 197 CP[23] (i els articles 198, 199 i 200 CP) tipifiquen com a conductes delictives l'accés, utilització, modificació, revelació, difusió o cessió de dades reservades de caràcter personal que es trobin emmagatzemades en fitxers, suports informàtics, electrònics o telemàtics, sempre que aquestes conductes siguin fetes per persones no autoritzades (conductes anomenades, genèricament, abusos informàtics sobre dades personals).

[23]CP és l'abreviatura de Codi penal.

Explícitament es fa esment de l'agreujant d'aquestes conductes quan les dades objecte del delicte són de caràcter personal que revelin ideologia, religió, creences, salut, origen racial o vida sexual. Altres agreujants que cal tenir en compte es produeixen quan la víctima és un menor d'edat o incapaç, o bé la persona que comet el delicte és el responsable dels fitxers que hi estan involucrats. Mereix una especial consideració l'article 199.2, en el qual es castiga la conducta del professional que, incomplint l'obligació de reserva, divulga els secrets d'una altra persona.

4.1.2. Delicte de frau informàtic

En l'article 248.2 CP es castiga la conducta de qui, emprant qualsevol manipulació informàtica, aconsegueixi la transferència no consentida de qualsevol actiu patrimonial, amb ànim de lucre i perjudici sobre tercer. La Llei 15/2003, per la qual es va aprovar la reforma del codi penal de l'any 1995, s'introdueix el càstig per a les conductes preparatòries per a la comissió de delictes de frau informàtic. Així doncs, també es castiga la fabricació, facilitació o la mera possessió de programari específic destinat a la comissió del delicte de frau informàtic.

Falsificació de targetes

L'article 387 CP considera moneda les targetes de crèdit, de dèbit, o les altres que es puguin fer servir com a mitjans de pagament. Per tant, la clonació o duplicació de targetes de banda magnètica es considera un delicte de falsificació de moneda.

4.1.3. Delicte d'ús abusiu d'equipaments

L'article 256 CP castiga l'ús de qualsevol equipament terminal de telecomunicacions sense el consentiment del seu titular, sempre que li ocasioni un perjudici superior a 400 euros. Aquesta quantitat va ser establerta per la Llei 15/2003.

Wi-fi

Notem que l'aprofitament no consentit d'una connexió *wi-fi* podria tenir la tipificació de delicte d'ús abusiu d'equipaments, sempre i que es produïssin els requisits exigits pel CP.

4.1.4. Delicte de danys

Segons l'article 264.2 CP el delicte de danys consisteix en la destrucció, l'alteració, la inutilització o qualsevol altra modalitat que impliqui el dany de dades, programari o documents electrònics emmagatzemats en xarxes, suports o sistemes informàtics.

El delicte de danys és un dels delictes "informàtics" més freqüents i sovint té repercussions econòmiques molt importants en les organitzacions afectades.

Els danys produïts en un sistema informàtic s'han de poder valorar i és essencial adjuntar una valoració d'aquests danys en denunciar l'acció delictiva davant d'un cos policíac. La valoració dels danys és un procés complex de dur a terme i pot abastar diferents aspectes: cost de restauració d'una pàgina web, pèrdues en concepte de publicitat no emesa (lucre cessant) o per serveis que no s'han pogut prestar, etc.

Val a dir que si bé la intrusió en un sistema informàtic de moment no és en si mateixa constitutiva de delicte (tot i que en breu tindrà aquesta consideració), aquests tipus de conductes se solen trobar vinculades a altres conductes que sí que són delictives com, per exemple, els delictes contra la intimitat, els danys en un sistema informàtic o els mitjans que s'hagin fet servir per a dur a terme l'accés no autoritzat (intercepció de correus electrònics, detecció o *sniffing* de contrasenyes, etc.).

Exemples de danys

L'alteració d'una pàgina web per una persona no autoritzada es tipifica com a delicte de danys.

L'enviament de virus (amb la clara voluntat de causar danys), els atacs DOS, entre altres de similars, també podrien tipificar-se com a delictes de danys.

Tingueu present, però, que la quantitat de 400 euros marca el llindar entre la falta i el delicte.

4.1.5. Delictes contra la propietat intel·lectual

Segons l'article 270 CP, les conductes relatives als delictes contra la propietat intel·lectual són aquelles en què es reprodueix, plagia, distribueix o comunica públicament, tant d'una manera total com parcial, una obra literària, artística o científica sense l'autorització dels titulars dels drets de propietat intel·lectual de l'obra.

Llei de propietat intel·lectual

Dins del marc jurídic extrapenal, la Llei de propietat intel·lectual (RD legislatiu 1/96, de 12 abril, pel qual quedava el Text refós de la Llei de propietat intel·lectual), regula la protecció de les obres literàries, artístiques o científiques, amb independència del suport en què siguin plasmades.

Aquestes condicions s'apliquen independentment del suport en què s'hagi enregistrat l'obra –textos, programaris, vídeos, sons, gràfics o qualsevol altre fitxer relacionat. És a dir, els delictes relatius a la venda, distribució o fabricació de còpies no autoritzades de programari són delictes contra la propietat intel·lectual.

Permís dels titulars

No podem fer un ús lliure de la informació que es pugui trobar a Internet com, per exemple, gràfics, animacions, logotips, etc., sense el permís dels titulars dels drets de propietat intel·lectual.

Exemples de delictes contra la propietat intel·lectual

Vegem alguns exemples delictes contra la propietat intel·lectual:

- Reproducció íntegra de programari i venda al marge dels drets de llicència.
- Instal·lació de còpies no autoritzades de programari en un ordinador en el moment de la seva compra.
- Publicació del codi font de programari, programari divers (servidors de *warez*, programari piratejat) o altres fitxers (MP3, llibres, etc.) a Internet, al marge dels drets de llicència d'aquestes obres.
- Utilització d'una llicència de programari per només un sol ordinador per a donar servei a tota la xarxa.
- Trencament dels mecanismes de protecció que permeten el funcionament correcte del programari (motxilles, contrasenyes i altres elements de seguretat). Aquestes tècniques reben el nom genèric de *cracking* (en català, pirateria).

El mateix article 270 CP preveu penes per a qui faci circular o disposi de qualsevol mitjà específicament dissenyat per a anul·lar qualsevol dispositiu tècnic de protecció del programari.

Acció d'ofici

Actuar d'ofici implica que els cossos policials poden actuar sense necessitar la denúncia de les persones o dels seus representants legals.

Amb la reforma de la Llei 15/2003, els cossos policials poden actuar d'ofici en la persecució d'aquest tipus de delicte. D'altra banda, un particular, atès que normalment no disposa dels drets de propietat intel·lectual, no pot denunciar directament aquests tipus de delicte; no obstant això, és possible fer-ho de manera indirecta a través d'organitzacions com la Bussiness Software Alliance (BSA).

Pel que fa a la creació de programari, també hi ha algunes consideracions que cal tenir en compte. Segons el tipus de contracte al qual es trobi subjecte el treballador, el programari que desenvolupi per a una organització pertany a l'empresa i, en conseqüència, si el treballador abandona l'organització, no es pot emportar el programari que ha creat en el seu antic lloc de treball. Com en el cas de la utilització del correu electrònic, seria recomanable que el contracte de treball especifiqués aquesta qüestió.

4.1.6. Delicte de revelació de secrets d'empresa

Segons l'article 278.1 CP, fa revelació de secrets d'empresa qui, amb la finalitat de descobrir un secret d'empresa, intercepti qualsevol tipus de telecomunicació o utilitzi artificis tècnics d'escolta, transmissió, gravació o enregistrament del so, imatge o de qualsevol altre senyal de comunicació.

Exemple

Hi ha diversos casos de delicte de revelació de secrets d'empresa, per exemple l'espionatge industrial. Podeu veure el cas Lear (sentència 53/07 del Jutjat Penal de Lleida, 18 de febrer de 2008).

4.1.7. Delicte de defraudació dels interessos econòmics dels prestadors de serveis

La defraudació dels interessos econòmics dels prestadors de serveis és un nou delicte, introduït arran de la reforma 15/2003 del codi penal. L'article 286 CP conté quatre modalitats de comissió:

1) Es castiga la facilitació de l'accés "intel·ligible" a serveis de radiodifusió sonora o televisiva, prestats a distància per via electrònica, mitjançant la facilitació, importació, distribució, possessió de programes o equipaments informàtics, destinats a fer possible l'esmentat accés. Aquesta modalitat inclou la instal·lació, manteniment o substitució d'aquests equipaments amb finalitats comercials.

2) Es castiga l'alteració o duplicació del número d'identificació de l'equip de telecomunicacions, amb ànim de lucre.

3) Es castiga la facilitació de l'esmentat accés a una pluralitat de persones per mitjà de qualsevol publicació pública, encara que sigui sense ànim de lucre.

4) Finalment, també es castiga la utilització dels equipaments o programaris que permeten l'accés, així com la utilització dels equipaments alterats, independentment de la quantia de la defraudació.

4.1.8. Altres delictes

A més dels delictes que hem descrit, és evident que molts altres delictes també es poden dur a terme amb el concurs de la tecnologia:

- amenaces i coaccions (per xats o mitjançant correu electrònic),
- estafes electròniques,
- falsedat documental (alteracions i simulacions de documents públics o privats) o
- difusió de pornografia infantil a Internet.

En relació amb aquest últim delicte (article 189.1 CP), la Llei 15/2003 ha ampliat notablement el tipus delictiu. Així, la mera possessió (encara que no estigui destinada a la venda) de pornografia infantil ja es troba castigada (la difusió, creació i venda ja ho estaven). A més, s'introdueixen certs agreujants, com per exemple, la utilització de menors de 13 anys, entre altres. Així mateix, també es castiga la producció, venda, distribució i exhibició, de material en què, tot i que no hi apareguin directament menors d'edat, s'hagi modificat la veu o la imatge amb la finalitat que el contingut sigui relatiu a la pornografia infantil.

Si un sistema informàtic és víctima de qualsevol d'aquests delictes, o bé, per exemple, es descobreix que el sistema és utilitzat com a plataforma de distribució de còpies de programari no autoritzades o de pornografia infantil, s'ha de denunciar immediatament a la comissaria de policia més pròxima, tenint en compte el protocol d'actuació següent:

1) Adjunció dels fitxers *log* (locals) relacionats amb el delicte comès.

2) En cas que s'hagi produït un delicte de danys, cal adjuntar una valoració dels danys ocasionats.

3) Actuar amb rapidesa (els proveïdors d'Internet no emmagatzemen indefinidament els fitxers *log* dels seus servidors).

4) En cas que aquesta acció delictiva s'hagi produït per correu electrònic, cal adjuntar les capçaleres completes del correu rebut.

5) Si l'administrador ho considera necessari (per exemple, descobreix pornografia infantil en un servidor de la seva responsabilitat), pot clonar el disc dur del servidor per a preservar l'evidència digital i reinstal·lar el sistema per a evitar que el delicte es continuï produint.

Condemna per compartir pornografia infantil

La primera condemna per compartir pornografia infantil a Internet mitjançant el programari *E-mule* es va produir l'abril de 2008 a l'Audiència Provincial de Canàries.

4.1.9. Ús d'eines de seguretat

Hi ha diverses eines de seguretat disponibles:

- **Escàners de xarxa o de sistema**. Tot i la possibilitat de dotar els escàners d'un ús maliciós, els seus beneficis són evidents pel que fa a les tasques que ha de fer l'administrador. La fiabilitat d'un sistema informàtic no es pot basar en la ignorància dels defectes que presenta i, per tant, els escàners esdevenen eines de gran valor en mans dels administradors. Ara bé, des del punt de vista legal, es poden fer servir? No hi ha cap llei en contra de l'ús dels escàners, si bé s'ha generat una interessant polèmica al seu entorn. Algunes opinions consideren que l'ús dels escàners és equivalent a anar a un domicili particular i fer servir la força per a obrir la porta.

D'altres creuen que pel sol fet de tenir una ubicació a Internet, ja es dóna el consentiment implícit per a "escanejar" la localització.

- **Eines criptogràfiques**. Pel que fa a la criptografia, tampoc no hi ha cap llei que en prohibeixi l'ús en el nostre país. Segons l'article 52 de la Llei general de telecomunicacions, Espanya disposa d'un règim de llibertat de xifratge per a protegir qualsevol dada que circuli per una xarxa. D'altra banda, aquest mateix article deixa la porta oberta a la definició de mecanismes de control com, per exemple, l'obligació de notificar a l'Estat els algorismes criptogràfics que es facin servir.

S'ha de tenir en compte, però, que en alguns països com, per exemple, els Estats Units, l'exportació d'eines criptogràfiques s'assimilava (fins al final de l'any 1999) al contraban d'armes. Recordeu els problemes que va tenir Zimmermann amb la publicació del codi del PGP. Com a norma general, mai no "s'escanejarà" un *host* sense autorització.

4.2. Marc jurídic extrapenal

Hi ha un seguit de lleis que delimiten el marc jurídic que és d'aplicació a l'àmbit informàtica: la Llei orgànica de protecció de dades personals, la Llei de serveis de la societat de la informació i comerç electrònic i la legislació que s'aplica a la signatura digital.

4.2.1. Llei orgànica de protecció de dades personals

La Llei orgànica 15/1999, de 13 de desembre, de protecció de dades personals (LOPDP) té per objectiu la protecció de la intimitat de les persones físiques, pel que fa al tractament de les seves dades personals. Per dades personals s'entén qualsevol informació relativa a persones físiques identificades o identificables. Pel tractament s'entendrà el conjunt d'operacions i procediments tècnics de caràcter automatitzat o no que permetin la recollida, gravació, conservació, elaboració, modificació, bloquejament i cancel·lació de dades. A més, també hi ha un reglament relacionat amb aquesta llei que regula les mesures de seguretat que han de satisfer els fitxers que continguin dades de caràcter personal. Aquestes mesures es disposen en els tres nivells següents:

Tractament de l'adreça IP

L'adreça IP permet, de manera indirecta, la identificació d'un titular telefònic. És, en conseqüència, una dada personal i, com a tal, s'ha de sotmetre a les mesures indicades per la LOPDP.

Fitxers amb dades personals

Les mesures de seguretat que han de satisfer els fitxers que continguin dades de caràcter personal es refereixen d'una manera genèrica a tots els fitxers que continguin aquestes dades personals, no tan sols aquells als quals es pot accedir des d'Internet.

- **Nivell bàsic**. Consisteix en la implantació de mesures d'autenticació i control d'accés per als usuaris que han d'accedir al fitxer amb contingut sensible, i també en l'elaboració de protocols d'actuació sobre el fitxer que permetin la identificació de possibles responsables en les incidències que es produeixin en la manipulació de les dades. Aquest nivell és exigible en la gestió de tots els fitxers que emmagatzemen dades de caràcter personal.

- **Nivell mitjà**. En aquest nivell de seguretat, l'administrador ha d'elaborar un catàleg sobre les mesures de seguretat genèriques que s'han de dur a terme i implementar mecanismes d'autenticació remota segurs. A més, aquestes mesures s'han de sotmetre, com a mínim cada dos anys, a una auditoria externa que certifiqui l'eficàcia de les mesures de seguretat que s'han pres. Són mesures exigibles per a tots els fitxers que emmagatzemin dades relatives a la comissió de delictes o infraccions administratives, hisenda pública, serveis financers i els relatius a la solvència patrimonial i el crèdit.

- **Nivell alt**. Per a protegir els fitxers situats en aquest nivell cal l'ús de mètodes criptogràfics per a evitar que les dades sensibles siguin intel·ligibles i no puguin ser alterades o capturades mentre circulen per una xarxa. Pertanyen a aquest nivell les dades relatives a ideologia, creences, origen racial, salut, vida sexual o les obtingudes amb finalitats policíaques.

Lectura recomanada

El Reial decret 1720/2007, de 21 de desembre, aprova el Reglament de desenvolupament de la Llei 15/1999. Els tres nivells de mesures de seguretat per a protegir els fitxers amb dades personals es desenvolupen en aquest reglament.

La LOPDP[24] distingeix entre el **responsable dels fitxers** i el **responsable de la seguretat dels fitxers**. A la vegada, el responsable dels fitxers es desdobla en dues figures que no han de ser pas coincidents: el **responsable del fitxer** o tractament (per exemple, l'empresa X) i l'**encarregat del tractament** (per exemple, una altra empresa, contractada per l'empresa X, amb la finalitat d'efectuar el tractament de les dades).

[24]LOPDP és l'abreviatura de la Llei orgànica de protecció de dades personals.

Secret professional

La LOPDP determina el deure de secret professional a tots els encarregats del tractament de dades personals.

Finalment, el responsable de la seguretat dels fitxers seria qualsevol empresa que es responsabilitzés d'aquesta seguretat (habitualment, l'encarregat del tractament i el responsable de seguretat són figures coincidents). Per acabar, cal tenir present que la llei obliga que totes les empreses que tenen fitxers amb dades personals els notifiquin a l'Agència de Protecció de Dades.

4.2.2. Llei de serveis de la societat de la informació i comerç electrònic

La Llei 34/2002, d'11 de juliol, de serveis de la societat d'informació i comerç electrònic (LSSICE) representa el desenvolupament al nostre país de la directiva comunitària sobre comerç electrònic. L'LSSICE regula els serveis oferts pels operadors de telecomunicacions, els proveïdors d'accés a Internet, portals i inclou, entre altres, el comerç electrònic. Alguns trets característiques que la defineixen són els següents:

- Prohibició del correu electrònic no sol·licitat o no consentit (*spam*). L'incompliment d'aquesta prohibició pot comportar sancions de fins a 150.000 euros.

- Regulació de qualsevol activitat que generi ingressos o permeti l'obtenció de beneficis econòmics (inclusió de cibertires publicitàries o bàners en una pàgina web, botigues virtuals, patrocinis, etc.).

- Sancions (aplicades per l'Agència de Protecció de Dades) econòmiques de fins a 600.000 euros per a les infraccions considerades molt greus.

- Obligatorietat de denunciar fets il·lícits i suspensió de la transmissió i allotjament de continguts il·lícits (mitjançant sol·licitud).

- Definició de les responsabilitats dels proveïdors d'Internet. Per exemple, en el cas d'hostatge i *linking*, els proveïdors no tindran cap responsabilitat sobre la informació emmagatzemada, sempre que no tinguin coneixement que aquesta informació sigui il·lícita, o be, si en tenen coneixement, han d'actuar amb la màxima diligència per a impossibilitar l'accés o eliminar el contingut il·lícit.

- Obligació d'emmagatzemar els fitxers de *log*, per part dels proveïdors de serveis, com a molt durant un període de 12 mesos (observem que no s'estableix cap període mínim).

4.2.3. Signatura electrònica o digital

La signatura electrònica és una matèria que queda regulada a l'Estat espanyol mitjançant el Reial decret llei 14/1999, de 17 de setembre, basat en la directiva europea que estableix el marc comunitari per a la signatura electrònica. Aquest decret llei determina l'eficàcia jurídica de la signatura digital a l'Estat espanyol, i l'establiment de les condicions dels serveis de certificació.

Hi ha dos tipus diferents de signatura:

- **Signatura electrònica o digital avançada**. Permet identificar la persona que signa i detectar qualsevol canvi que es pugui produir de forma posterior a la signatura de les dades.

- **Signatura electrònica o digital reconeguda**. Consisteix en la firma electrònica avançada, basada en un certificat reconegut i generat mitjançant un dispositiu segur de creació de signatura (els prestadors de serveis de certificació). És equiparable a la signatura manuscrita.

5. Informàtica forense

Una vegada descrit el marc jurídic en el qual s'ajusten les conductes il·lícites relacionades amb l'ús de les tecnologies de la informació, s'estudiaran breument les metodologies de treball que es poden emprar, una vegada ha succeït l'incident, amb la finalitat d'esbrinar què ha ocorregut i qui n'ha estat el presumpte autor. Aquestes tècniques es recullen en una disciplina de recent creació, situada a cavall entre el marc jurídic i la tecnologia, anomenada **informàtica forense**. Les empremtes que permeten reconstruir l'execució d'un fet (el qual no ha de ser necessàriament constitutiu de delicte) es troben emmagatzemades en suports digitals i s'anomenen genèricament **evidències digitals**.

L'evidència digital presenta, bàsicament, les propietats següents:

- Es pot modificar o eliminar fàcilment.
- És possible obtenir una còpia exacta d'un arxiu sense deixar cap empremta d'aquesta acció.
- L'adquisició de l'evidència pot suposar l'alteració dels suports digitals originals.

L'**anàlisi forense informàtica** va aparèixer a causa de la necessitat d'aportar elements rellevants en els processos judicials en què les noves tecnologies es trobaven presents, ja sigui com a objectius finals (per exemple, una intrusió amb danys en un sistema informàtic), o bé com a mitjà (per exemple, l'enviament d'amenaces a través del correu electrònic a un personatge públic). La finalitat, en qualsevol cas, consisteix en respondre a la clàssica línia argumental policíaca: **què**, **quan**, **on**, **qui**, **com** i **perquè**.

Més precisament, es podria definir l'anàlisi forense informàtic com el procés d'aplicar el mètode científic als sistemes informàtics amb la finalitat d'assegurar, identificar, preservar, analitzar i presentar l'evidència digital, de forma que sigui acceptada en un procés judicial.

Naturalment, la informàtica forense va més enllà dels processos judicials i, en moltes ocasions, els informes elaborats pels experts analistes no tindran com a objectiu final la seva presentació davant dels tribunals, sinó l'empresa privada.

5.1. Assegurament de l'escena de l'esdeveniment

Aquesta fase únicament serà preceptiva en el decurs d'una actuació policíaca. No obstant això, les recomanacions que es donaran poden ser de molta utilitat per a qualsevol pèrit que hagi d'intervenir en el lloc dels fets. La finalitat d'aquesta etapa consisteix a assegurar l'escena de l'esdeveniment i restringir-ne l'accés perquè ningú pugui alterar-la. Els referents policíacs són evidents, encara que seguir les recomanacions que ara es descriuran permetrà preservar, en qualsevol cas, l'evidència, així com facilitar-ne l'anàlisi posterior:

Adreça recomanada

Podeu veure un "codi de bones pràctiques forenses" a http://cp4df.sourceforge.net.

- Identificar l'escena on s'ha produït el fet a investigar i establir un perímetre de seguretat.

- Realitzar una llista amb els sistemes involucrats en el succés.

- Restringir l'accés de persones i equipaments informàtics a l'interior del perímetre.

- Fotografiar i/o enregistrar en vídeo l'escena del succés. També pot ser molt útil representar esquemàticament la topografia de la xarxa d'ordinadors.

- Mantenir l'estat dels dispositius. En algunes ocasions pot ser molt important fotografiar o enregistrar el contingut dels monitors en funcionament, així com la identificació i adquisició de les evidències volàtils, per exemple, l'extracció del contingut de la memòria per a saber quins processos es trobaven en execució en aquell moment.

- Desconnectar les connexions de xarxa.

- En cas d'existir, comprovar i desconnectar les connexions sense fil, ja que podrien permetre connexions remotes als equips objecte d'investigació.

- Si hi ha impressores en funcionament, permetre que acabin la impressió.

- Anotar la data i hora del sistema abans d'apagar-lo. Aquestes dades també es poden fotografiar i/o enregistrar en vídeo.

- Apagar els dispositius en funcionament, o bé traient el cable d'alimentació, o bé mitjançant el procediment d'apagat normal. L'expert haurà d'avaluar en cada cas quin és el mètode més adequat que ofereix més garanties de preservació de la prova.

- Etiquetar cables i components. A més, cal tenir present que alguns dispositius requereixen cablatge molt específic, sense el qual no serà possible analitzar l'aparell al laboratori, ja que no es podrà posar en funcionament.

En algunes ocasions, l'assegurament de l'escena es produeix en el decurs d'una entrada i perquisició en el lloc dels fets en presència de membres de les Forces i Cossos de Seguretat de l'Estat. En aquest cas, l'entrada comptarà amb la presència del secretari judicial, amb la qual cosa es pot fer constar en acta la data i hora del sistema, entre altres comprovacions de les quals el secretari judicial podria donar fe i, per tant, podria estalviar a l'analista alguns processos de documentació, fotografies i/o enregistraments de vídeo.

Data i hora d'un sistema informàtic

La data i hora d'un sistema informàtic no ha de coincidir pas amb la data i hora real. Aquest desfasament pot ser vital a l'hora de l'anàlisi i cal ferlo constar en acta.

5.2. Identificació de l'evidència digital

S'anomena així el procés d'identificació i localització de les evidències que s'han de recollir per a ser analitzades posteriorment. Aquest procés no és tan trivial com pot semblar a primera vista ja que, tot sovint, l'expert es trobarà amb configuracions de sistemes complexos amb molts dispositius (locutoris, empreses, etc.) o, simplement, amb usuaris que guarden molts suports susceptibles de ser analitzats (per exemple, un particular addicte a emmagatzemar qualsevol programari descarregat d'Internet en milers de CD i DVD). En conseqüència, l'analista haurà de trobar una solució de compromís entre la qualitat, la validesa de la prova i el temps de què disposa per a recollir les evidències.

En primer lloc, l'expert haurà d'identificar el sistema informàtic (un únic PC, una xarxa local, un sistema IBM AS/400, un RAID, etc.) amb la finalitat de saber on s'emmagatzemen les evidències digitals que poden ser d'utilitat per a l'anàlisi. Aquestes es poden trobar en ordinadors locals, en suports com CD o DVD, en servidors remots, o fins i tot en la memòria RAM dels equipaments en funcionament. Aquest tipus d'evidències, les volàtils (en essència, aquelles que desapareixen en absència d'alimentació elèctrica), són les que haurà d'intentar preservar en primera instància, en els casos en què sigui necessari.

També, en aquest instant, convindrà valorar la possibilitat de realitzar una "anàlisi en calent" a la recerca d'evidències que d'altra forma es perdrien a l'aturar el sistema. No obstant això, cal tenir present que aquesta mena d'anàlisi pot comportar la pèrdua d'altres evidències, així com la invalidació de la prova en un procediment judicial, ja que l'anàlisi en calent implica la manipulació del dispositiu original i si no es fa amb les eines forenses adequades es pot alterar l'evidència.

5.3. Preservació de les evidències digitals

Atesa la facilitat amb què les evidències digitals es poden modificar i/o eliminar, aquesta fase es converteix en la baula més crítica de tot el procediment. És evident que és del tot impossible obtenir una "instantània" completa de tot un sistema informàtic en un moment concret (la naturalesa intrínseca de les evidències volàtils així ho determina), encara que sortosament per a l'analista,

Localització d'evidències digitals

Podem localitzar evidències digitals en impressores, gravadors de targetes de banda magnètica, discs USB, telèfons i PDA, targetes de memòria, tokens, etc.

en la gran majoria d'ocasions, les proves determinants es troben emmagatzemades en el sistema de fitxers, el qual continuarà conservant l'evidència malgrat la manca d'alimentació elèctrica.

A diferència d'altres proves (per exemple, una anàlisi biològica d'ADN), l'evidència digital es pot duplicar o clonar de manera exacta (a nivell de bits), incloent-hi els arxius ocults, eliminats i no sobreescrits, i fins i tot l'anomenat *slack file* (al qual ens referirem posteriorment), possibles particions ocultes, o l'espai no assignat del disc dur. Així, en virtut d'aquesta característica, i també com a garantia de preservació de la prova, l'analista actuant acabarà realitzant un clon de l'evidència, ja sigui en l'escena del succés, o a les dependències del laboratori.

Obertura d'un fitxer

L'obertura d'un fitxer implica, si no s'utilitzen eines d'anàlisi forense, l'alteració de la darrera data d'accés a l'arxiu. La simple observació de la prova, en anàlisi forense, pot implicar la seva alteració.

A primera vista resulta temptador ajornar la clonació dels suports informàtics al moment en què aquests arribin al laboratori (ja que és on es podrà fer el procés amb tota mena de garanties i sense presses), però això no sempre serà possible. Si, per exemple, les evidències es localitzen en el servidor d'una empresa, no és possible precintar l'equipament perquè aleshores l'empresa hauria d'aturar la seva activitat. En aquests casos és preferible aturar momentàniament l'activitat de l'empresa i obtenir un clon allà mateix, per a reprendre tot seguit l'activitat empresarial, o bé realitzar una anàlisi en calent, amb els inconvenients que ja s'han explicat.

Observació

Si ens trobem un disc dur submergit en un líquid cal conservar-lo, sempre que sigui possible, en el medi on s'ha trobat.

La còpia o clon s'efectuarà, normalment, sobre dispositius (CD, DVD, discs durs, etc.) aportats per l'analista. L'elecció d'un o altre mitjà dependrà de la quantitat d'informació continguda en els suports originals. Finalment, el programari o maquinari emprat per a l'obtenció del clon calcularà un CRC (codi de redundància cíclica) o un valor *hash*, que haurà de ser el mateix, tant pel disc dur d'origen, com pel destí, amb la qual cosa es garantirà que el procés de còpia ha funcionat correctament.

Eines per a fer un clon

Hi ha diverses eines per a obtenir un clon:

- Mitjançant programari: la comanda dd de Linux, Encase, Ilook, etc.
- Mitjançant maquinari: Logicube, etc.

A més de l'adquisició de l'evidència, en aquesta etapa també cal documentar **qui** va preservar l'evidència, **on** i **com** es va fer i **quan**. Tot seguit caldrà empaquetar les evidències, identificant-les de manera unívoca. Aquest procés es du a terme embalant els paquets amb material protector que pugui protegir les evidències de cops, pluja o qualsevol altre element pugui malmetre els suports. Aquesta fase posarà fi al transport de les evidències a un lloc segur o a les dependències del laboratori on hagin de ser analitzades. L'embalatge i el transport de les evidències és l'inici de la denominada **cadena de custòdia**, la qual permet garantir la integritat de les proves, des de la seva obtenció, fins a la seva disposició a l'autoritat judicial o al laboratori on hagin de ser analitzades. La documentació de la cadena de custòdia permet saber, en qualsevol moment del procés, on han estat emmagatzemades les evidències i qui hi ha tingut accés.

5.4. Anàlisi de les evidències digitals

En aquesta fase, l'expert haurà de respondre les preguntes "policíaques" introduïdes a l'inici d'aquest apartat 5. Aquest estudi es fonamentarà, sobretot, en l'anàlisi del contingut dels arxius (dades) i de la informació sobre aquests fitxers (metadades).

Exemple de metadada

El contingut del camp *autor* que apareix en tots els arxius de Microsoft Word és un bon exemple de metadada.

Normalment no es realitzen anàlisis exhaustives dels suports objecte d'interès (seria una tasca inabastable), sinó que els informes pericials es limiten a respondre aquelles qüestions plantejades en els extrems de l'anàlisi.

Els extrems en un cas d'intrusió

En un cas d'intrusió, els extrems podrien ser: "Esbrinar l'usuari o usuaris que varen realitzar els accessos no autoritzats en les dates especificades".

En general hi ha quatre categories diferents de dades que són susceptibles de ser analitzades:

- **Dades lògicament accessibles**. És a dir, les dades contingudes en arxius directament accessibles. Aquesta anàlisi, no exempta de dificultats, pot no ser gaire senzilla a causa de l'enorme dificultat que pot existir a l'hora de discriminar la informació rellevant d'entre molts milers de fitxers, l'existència d'arxius xifrats, o la presència de fitxers troianitzats, l'execució dels quals podria produir conseqüències inesperades.

- **Dades localitzades en l'anomenat *ambient data***. És a dir, aquelles dades que apareixen en localitzacions no directament visibles i que requereixen de l'ús de programaris específics per a ser recuperats. Un bon exemple d'aquest tipus de dades és la informació residual que es pot trobar en clústers actualment no assignats a cap arxiu, o aquella informació localitzada en l'*slack file* (espai entre el final lògic d'un fitxer i el final físic d'aquest mateix).

- **Dades que han estat esborrades o eliminades**, però que encara no han estat sobreescrites per altres fitxers i que, per tant, són susceptibles de ser recuperades emprant les eines adients a aquesta finalitat.

- **Dades ocultes mitjançant esteganografia**, les quals són molt més difícils de detectar que els arxius xifrats.

Per a realitzar l'anàlisi de les evidències es poden emprar diverses eines, algunes de les quals ja s'han descrit prèviament. Possiblement, una de les més conegudes és l'eina EnCase, de codi propietari, la qual abasta, amb una interfície molt amigable, totes les fases de l'anàlisi forense, des de l'adquisició dels suports originals i l'anàlisi, fins a la generació automàtica de l'informe final. Altres eines, també molt conegudes, són l'eina Ilook (de moment gratuïta per a Forces i Cossos de Seguretat de l'Estat), la distribució de Linux Backtrack o la col·lecció de programes *Coroner's Toolkit* (TCT), desenvolupada per Dan Farmer i Wietse Venema.

5.5. Presentació i informe

En l'informe elaborat per l'expert es presentaran les evidències relacionades amb el cas, la justificació del procediment emprat i, el més important, les conclusions. En moltes ocasions, l'informe serà ratificat en presència del jutge, o bé serà lliurat a empreses i advocats. No obstant això, en cap cas els destinataris de les perícies han de disposar necessàriament de coneixements informàtics per a poder comprendre l'informe en profunditat. Per tant, en general mai no s'ha d'emprar un llenguatge excessivament tècnic i, quan calgui fer-ho, caldrà afegir notes aclaridores a peu de pàgina, o fins i tot redactar glossaris tècnics, sovint afegits a l'annex de l'informe. En els casos en què els informes hagin de ser defensats davant del jutge, l'analista, a més del rigor tècnic, ha de ser prou hàbil per a comunicar el resultat de l'anàlisi de forma concisa i clara.

Resum

En aquest mòdul hem estudiat els principis bàsics de l'administració de seguretat d'un sistema informàtic i els hem relacionat amb les possibles responsabilitats que es poden derivar de la vulneració d'aquesta seguretat. Hem dividit el mòdul en els cinc apartats següents:

- Apartat 1: dedicat a les definicions bàsiques relatives a la seguretat informàtica.

- Apartat 2: en aquest apartat hem estudiat les condicions de seguretat de l'entorn (control d'accés), i també les eines criptogràfiques que pot fer servir un administrador per a protegir la informació.

- Apartat 3: el tercer apartat estudia la seguretat del sistema en el sentit més general del terme. S'ha triat el sistema operatiu Unix per a explicar els conceptes d'aquest apartat perquè creiem que les possibilitats i la flexibilitat del Unix fan que sigui senzill extrapolar els problemes de la seguretat del sistema (i les seves solucions) a qualsevol altre sistema operatiu i a les xarxes d'ordinadors en general.

- Apartat 4: descriu les responsabilitats en què pot incórrer l'administrador d'un sistema informàtic (tant pel que fa a la responsabilitat que adquireix envers el sistema –maquinari i programari– com per les dades que s'hi emmagatzemen. D'altra banda, també e1erem els possibles delictes de què pot ser víctima en l'entorn del seu treball, i la manera de denunciar-los. La legislació encara presenta molts buits pel que fa a aquesta matèria, per la qual cosa som conscients que la lectura de l'apartat pot generar (i ho ha de fer) moltes preguntes que no tenen una resposta clara. Finalment, s'ha d'entendre que la seguretat d'un sistema informàtic no és conseqüència de l'aplicació de cap fórmula magistral, sinó d'un seguit de mesures que cal millorar i adaptar a les noves necessitats dia a dia.

- Apartat 5: descriu què es pot fer una vegada ha succeït un problema de seguretat (o fins i tot un delicte) per a poder esbrinar què ha passat i qui ha estat el presumpte autor. Es defineix el concepte d'informàtica forense, una nova disciplina situada a cavall entre la informàtica i la normativa legal.

Activitats

1. Dissenyeu un pla de seguretat física per a una organització que vosaltres conegueu (un centre de càlcul, l'organització en què treballeu, l'aula d'informàtica d'una facultat, etc.). Per a fer-ho us podeu orientar en l'esquema següent:

- Descripció dels recursos físics que es volen protegir.
- Descripció de l'espai físic on es localitzen els recursos.
- Descripció del perímetre de seguretat.
- E1eració de les amenaces que poden comprometre la seguretat del sistema.
- Possibles mesures de seguretat contra les amenaces anteriors.
- Manera d'implementar les mesures anteriors.
- Càlcul del cost estimat de la implementació de les mesures o millores que cal fer, i també del cost de les dades que cal protegir i la probabilitat que es produeixi un atac (accidental o no).

2. Cerqueu informació sobre les associacions següents, relacionades amb la informàtica forense:

- International Association of Computer Investigative Specialist (IACIS). Aquesta associació ofereix una certificació internacional (CFEC, Computer Forensic External), adreçada a analistes que no formin part dels cossos policials o judicials.
- European Network of Forensic Science Institute (ENFSI).
- International Organisation on Computer Evidence (IOCE).
- Equipo de Seguridad para la Coordinación de Emergencias en Redes Telemáticas (es-CERT).

3. La funció d'un pèrit judicial consisteix a proporcionar al jutge la informació necessària per a ajudar-lo a determinar què ha succeït en el cas que s'investiga. La figura del pèrit judicial s'introdueix a l'article 456 (i següents) de la Llei d'enjudiciament criminal. Cerqueu els articles que defineixen aquesta figura i raoneu les qüestions següents:

a) Creieu que és necessari disposar de la titulació universitària en Informàtica per a poder exercir de pèrit?
b) Quins són els drets i deures del pèrit?

Exercicis d'autoavaluació

1. Raoneu breument quina de les tres propietats que ha de satisfer tot sistema informàtic "segur" és prioritària en els sistemes següents:

- Una organització de defensa nacional.
- Un sistema de transferència electrònica de diners.
- Un departament de la universitat.

2. Relacioneu correctament els conceptes següents:

	DES	CAST	DSA	SHA-1	IDEA	RSA	MD5
C. PRIVAT							
C. PÚBLIC							
HASH							

3. La pàgina web del servidor del departament que administreu ha estat víctima d'un atac i ha estat substituïda per una altra pàgina amb un contingut completament diferent. Quines són les accions que haureu de fer per a denunciar el fet davant d'un cos policíac?

4. Determineu si els següents enunciats són o no correctes:

a) L'enviament de correu no sol·licitat (*spam*) és una conducta que apareix tipificada en el Codi penal.
b) La signatura electrònica avançada té la mateixa consideració que la signatura manuscrita.

c) La intrusió en un sistema informàtic, en si mateixa, no és una conducta tipificada en el Codi penal.
d) La LSSICE obliga els proveïdors de serveis d'Internet a mantenir els fitxers de *log* durant un *mínim* de temps.
e) La figura del responsable del fitxer o tractament és la mateixa que la del tractament del fitxer.

Solucionari

Exercicis d'autoavaluació

1. Confidencialitat, integritat i disponibilitat, respectivament.

2. Relacioneu correctament els conceptes següents:

	DES	CAST	DSA	SHA-1	IDEA	RSA	MD5
C. PRIVAT	*	*			*		
C. PÚBLIC			*			*	
HASH				*			*

3. Accions que cal fer en el cas d'un delicte de danys.

- Desconnexió de la xarxa.
- Fer una còpia de seguretat a baix nivell.
- Compilar tota la informació possible sobre l'atac (especialment els fitxers log relatius a l'adreça IP des de la qual presumptament s'ha originat l'atac –o per mitjà d'aquesta adreça).
- Restaurar el sistema i aplicar les actualitzacions de programari (per exemple, una actualització que resolgui el problema de la vulnerabilitat de les CGI).
- Notificar-ho a qui es consideri convenient i segons l'atac (al nostre cap, al CERT, a altres administradors d'altres sistemes implicats, als usuaris del nostre sistema, etc.).
- Sol·licitar una valoració dels danys produïts.
- Denunciar el fet a la comissaria de policia més pròxima i adjuntar a la denúncia tota la informació possible sobre l'atac i la valoració dels danys produïts (feta per la mateixa organització o bé per un pèrit extern).

4.a) incorrecte.

b) correcte.

c) correcte.

d) incorrecte.

e) incorrecte.

Glossari

autenticació *f* Verificació de la identitat d'una persona o procés a l'hora d'accedir a un recurs o poder fer una acció determinada.

anàlisi forense informàtica *f* Procés d'aplicació del mètode científic als sistemes informàtics amb la finalitat d'assegurar, identificar, preservar, analitzar i presentar l'evidència digital de forma que sigui acceptada en un procés judicial.

certificat digital *m* Document electrònic signat per una tercera part o autoritat de certificació que associa una clau pública a una persona.

cracking *m* Vegeu **pirateria**.

criptosistemes de clau compartida *m pl* Criptosistemes en els quals emissor i receptor comparteixen una única clau. És a dir, el receptor podrà desxifrar el missatge rebut únicament si coneix la clau amb la qual ha xifrat el missatge l'emissor.

criptosistemes de clau pública *m pl* Criptosistemes en què cada usuari *u* té associada una parella de claus <*Pu* , *Su*>. La clau pública, *Pu*, és accessible per tots els usuaris de la xarxa i apareix en un directori públic, mentre que la clau privada, *Su*, tan sols és coneguda per l'usuari *u*.

dada de caràcter personal *f* Qualsevol informació relativa a les persones. En concret, tota informació numèrica, alfabètica, gràfica, fotogràfica, acústica o de qualsevol altre tipus, susceptible de ser recollida, enregistrada, tractada o transmesa i que concerneix una persona física identificada o identificable.

fitxer automatitzat *m* Conjunt organitzat de dades que és objecte de tractament automatitzat.

footprinting *m* Vegeu **tècnica de l'empremta**.

funció *hash* *f* Funció matemàtica que fa correspondre una representació de mida fixa a un missatge m de mida variable.
sin. **funció resum**.

National Institute of Standards and Technology *m* Organisme creat el 1901 per a proveir la indústria nord-americana amb les mesures i la tecnologia per a mantenir la competitivitat en els mercats mundials i el comerç, avui ofereix serveis que cobreixen un ampli ventall d'activitats tecnològiques i comercials (normes, transferència de tecnologies, bases de dades, materials de referència, etc.). Vegeu *els algorismes SHA i AES*.
sigla: **NIST**.

NIST *m* Vegeu **National Institute of Standards and Technology**.

pirateria *f* Atac de força bruta dirigida a trencar una clau d'accés a un programa o servei.
en cracking.

pla de contingència *m* Protocol d'actuació establert que s'ha d'iniciar quan es produeix una emergència o desastre.

política de seguretat *f* Conjunt de directrius o estratègies que han de seguir els usuaris en relació amb la seguretat global del sistema informàtic.

responsable del fitxer *m i f* Persona física o jurídica, pública o privada, i òrgan administratiu que decideix sobre la finalitat, el contingut i l'ús del tractament.

seguretat informàtica *f* Conjunt constituït per diverses metodologies, documents, programari i maquinari, que determinen que els accessos als recursos d'un sistema informàtic siguin duts a terme exclusivament pels elements autoritzats a fer-ho.

spoofing *f* Tècnica d'atac a un sistema informàtic en què l'intrús simula una adreça IP d'origen, diferent de l'adreça IP real de l'atacant.

tècnica de l'empremta *f* Activitat consistent en la recollida d'informació sobre l'objectiu que es vol atacar utilitzant mètodes indirectes: determinació dels dominis i adreces IP dels sistemes objectiu (cerca d'informació als servidors *whois* o a les bases de dades *Arin* o *Ripe*, etc.).
en footprinting.

tractament de dades *m* Operacions i procediments que permeten la recollida, l'enregistrament, la conservació, l'elaboració, la modificació, el bloqueig i la cancel·lació i les cessions de dades.

Bibliografia

Bibliografia bàsica

Anònim. (2000). *Linux máxima seguridad*. Prentice Hall.

Colobran Huguet, M.; Morón Lerma, E. (2004). *Introducción a la seguridad informática*. Planeta UOC, S.L.

Dhanjani, N. (2008). *Claves hackers en Linux y Unix*. Mc Graw-Hill.

Jimeno García, M. T.; Míguez Pérez, C.; Matas García, A. M.; Pérez Agudín, J. (2008). *Guía práctica hacker*. Ediciones Anaya Multimedia.

Nemeth, E.; Snyder, G.; Hein, T. (2008). *Administración de sistemas Linux, Edición 2008*. Ediciones Anaya Multimedia.

Villalón Huerta, A. (2002). *Seguridad en Unix y redes. Version 2.1*.

Bibliografia complementària

Domingo i Ferrer, J. (1999). *Criptografia*. Barcelona: Universitat Oberta de Catalunya.

Guasch Petit, A.; Martínez de Carvajal Hedrich, E.; Peiró Mir, M.; Ríos Boutin, J.; Roca i Marimon, J. (2005). *Auditoria, peritatges i aspectes legals per a informàtics*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.

López Sánchez-Montañés, J.; Belles Ramos, S.; Aulí Llinàs, F.; Baig Viñas, R. (2008). *Sistema operatiu GNU/Linux bàsic*. Barcelona: Fundació per a la Universitat Oberta de Catalunya.