Seguretat de les transaccions electròniques

PID_00269811

César Pablo Córcoles Briongos
Ismael Peña-López

Temps mínim de dedicació recomanat: 2 hores

Universitat Oberta de Catalunya

César Pablo Córcoles Briongos

Llicenciat en Matemàtiques per la Universitat Autònoma de Barcelona. És professor dels estudis d'Informàtica, Multimèdia i Telecomunicacions des del 2001. Coordina assignatures de l'àmbit del disseny i el desenvolupament web del programa de grau en Multimèdia. És director del màster universitari de Desenvolupament de llocs i Aplicacions Web. La seva àrea d'interès en recerca se centra en l'ús de recursos multimèdia (animació, visualització en 3D) i interactius per a la docència de les ciències, amb atenció especial a les matèries STEM.

Ismael Peña-López

Professor dels estudis de Dret i Ciències Polítiques (UOC) i investigador a l'Internet Interdisciplinary Institute i a l'eLearn Center, també de la UOC. És doctor en Societat de la Informació i del Coneixement, llicenciat en Ciències Econòmiques i Empresarials (Economia), màster en Ecoauditories i planificació empresarial del medi ambient i postgraduat en Gestió del coneixement. Treballa en l'impacte de les tecnologies de la informació i la comunicació en el desenvolupament. En concret, els seus interessos se centren en la mesura de l'evolució de les economies digitals i l'adopció personal del que és digital (*e-readiness*, divisòria digital), i també en l'impacte de les TIC en el desenvolupament i les seves institucions principals, especialment en l'àmbit de les TIC i l'educació i les TIC i la democràcia.

L'encàrrec i la creació d'aquest recurs d'aprenentatge UOC han estat coordinats pel professor: Iván Serrano Balaguer (2020)

Primera edició: febrer 2020

Av. Tibidabo, 39-43, 08035 Barcelona
Realització editorial: FUOC

Índex

Introducció..... 5

1. Criptografia i identitat a la xarxa..... 9

2. Certificació digital..... 12

3. Cibercrim..... 16
3.1. Atacs al sistema 16
3.2. Engany a l'usuari 18

4. Anonimització i xarxes privades virtuals (VPN)..... 21

5. Altres mesures d'autenticació..... 23

Bibliografia..... 25

Introducció

Fins ara hem vist alguns exemples d'interacció per mitjans electrònics entre l'Administració i la ciutadania. Una bona part del que significa l'Administració electrònica és la comunicació entre els diferents agents i administracions, l'intercanvi de dades i el treball compartit en línia. Igual que succeeix al món «real», hi ha el perill que certes transaccions es puguin dur a terme d'una manera incorrecta. I, al marge de la possibilitat d'errors –humans, tècnics– que puguin ocórrer en aquestes transaccions, hi ha d'haver les garanties següents:

- Que els interlocutors –tant l'Administració com l'administrat– siguin els que diuen que són de manera que no hi hagi suplantació de la identitat en cap dels dos casos, és a dir, l'**autenticació**.

- Que cap de les parts no pugui negar haver fet o haver rebut una determinada comunicació, és a dir, el **no repudi**, una vegada aquestes parts estan degudament validades formalment.

- Que la transacció que es faci sigui precisament la que es vol fer sense que hi hagi modificacions –o ingerències– en les dades que s'intercanvien, és a dir, la **integritat** d'aquestes dades.

- Que els tercers no puguin accedir a les dades ni, per descomptat, utilitzar-les en el seu profit, és a dir, la **privadesa**.

En qualsevol d'aquests casos la peça fonamental és demostrar que s'és un usuari que té accés a les dades o a les comunicacions i que hi pot operar. Operacions elementals en l'Administració electrònica, com fer consultes sobre serveis o polítiques, efectuar transaccions administratives o tributàries, o fins i tot exercir en última instància la democràcia mitjançant el **vot electrònic**, són qüestions que requereixen una correcta autenticació del ciutadà –per estar segurs que qui accedeix a les seves dades sanitàries és el pacient correcte– i també una correcta autenticació de l'Administració, per a estar segurs que paguen els impostos al departament corresponent i no a un impostor. Volem insistir en aquesta dualitat de l'autenticació: és tan important que el ciutadà s'acrediti davant l'Administració com que aquesta ho faci davant l'administrat.

Històricament, la humanitat ha resolt aquesta qüestió de l'autenticació de manera que la persona que havia d'acreditar-se convencés l'acreditador que tenia alguna cosa que, per la naturalesa de l'objecte i del propietari, creava una relació única entre tots dos, amb la qual cosa es demostrava la seva personalitat. Personar-se davant de qui ens pot reconèixer és, sens dubte, la forma

d'acreditació més antiga del món, la qual pot ser substituïda pel «sant i senya» i la contrasenya corresponent en el cas que personar-se impliqui un accés que pugui no ser desitjat.

Podem organitzar en tres categories allò que un pot demostrar que té per a acreditar-se:

- Un **coneixement**, que és el cas de la contrasenya, encara en ús als nostres dies.

- Un **objecte físic**, com una clau, sia física, per a entrar a casa o al cotxe, o electrònica, per a accedir a una determinada màquina o ordinador.

- El propi cos –**informació biomètrica**–, que serà inspeccionat i reconegut pels dispositius corresponents com qui ens reconeixia. Parlem, per descomptat, de parts del nostre cos especialment singulars, com les empremtes dactilars o l'iris dels ulls.

Com que personar-se mitjançant les TIC no és possible físicament, a diferència de trucar a la porta d'una societat secreta en la cinematografia, és necessari que la informació que ens acreditarà es converteixi en una sèrie de dades digitalitzades que viatjaran entre les diferents parts d'una transacció.

No obstant això, aquesta acreditació es pot efectuar de dues maneres diferents. La primera, més intuïtiva, és el cas de les **contrasenyes**: un usuari té una contrasenya que el sistema, o l'altre usuari, coneix. Per a demostrar la seva identitat, envia aquesta contrasenya al sistema, aquest la compara amb la que apareix en la seva base de dades i, si coincideixen, es verifica que l'usuari és autèntic.

La segona és el cas, no de la informació que es coneix que circula d'un usuari a un altre, sinó del resultat d'una operació basada en aquesta informació. Aquest cas s'anomena de **repte/resposta**, que, al seu torn, té també dues opcions:

- En la primera opció tots dos coneixen una mateixa informació. El sistema ordena a l'usuari que vol acreditar-se que faci una operació amb la informació que comparteixen, i és el resultat d'aquesta operació el que es transmet.

Exemple de repte/resposta amb informació compartida

L'Administració i l'usuari saben que el document d'identitat de l'usuari té el número 1234. En demanar l'autenticació en el sistema de pagament d'impostos, el sistema de l'Administració demana a l'usuari que introdueixi el número del seu document d'identitat multiplicat per dos (aquesta operació variarà per a cada autenticació a fi d'evitar que es pugui arribar a deduir el número en formar part sempre de la mateixa operació). Si l'usuari tecleja 2468, la seva autenticació serà vàlida sense que hagi hagut d'enviar el seu número real, el 1234. (L'operació, o sèrie d'operacions, serà naturalment molt més complexa que «multiplicar per dos» i verificarà tot un seguit de condicions per a assegurar la seguretat del procediment.)

- En la segona opció solament l'usuari coneix aquesta informació –per la qual cosa és l'opció més segura– i el sistema, encara que no pot reproduir-la, sí pot verificar-la. Entrarem més endavant en aquesta qüestió en parlar de la signatura digital.

1. Criptografia i identitat a la xarxa

Tenint en compte que aquest viatge és perillós perquè les dades es poden robar o suplantar, es fa necessari «amagar-les» d'alguna manera. La **criptografia** –disciplina plenament integrada avui dia i desenvolupada en l'àmbit de les matemàtiques– respon a aquesta necessitat.

Xifrar –de vegades s'utilitza l'anglicisme «encriptar»– és el procés de canviar la informació de manera que aparegui com a inintel·ligible per a un tercer però que els qui coneixen l'**algoritme** –o procés– de xifratge puguin fer i desfer l'operació tantes vegades com sigui necessari, tant per a deformar aquesta informació com perquè torni a ser comprensible. De fet, en sentit estricte no és necessari conèixer l'algorisme que se segueix, sinó que el nostre ordinador o algun altre dispositiu nostre el conegui, a més de determinades **claus** necessàries per a iniciar el procés, de la mateixa manera que per a traduir un text necessitem el text mateix, un traductor expert i, a més, saber en quin idioma és escrit i a quin volem traduir-lo.

Exemple de xifratge

En el número del document d'identitat de l'exemple anterior un algorisme podria ser «sumar la clau» (tenint en compte que, per a **desxifrar**, caldrà «restar la clau»). Si la clau és 3, el valor xifrat del document 1234 serà 1237.

En el cas que tant l'emissor com el receptor del missatge comparteixin la clau, el xifratge rep el nom de **xifratge simètric o de clau compartida**. Dit d'una altra manera, la clau de xifratge i la clau de desxifratge són idèntiques o bé es poden deduir l'una de l'altra. Com més gran sigui la clau major serà la seguretat del sistema. La longitud de la clau es mesura en bits, per la qual cosa un sistema de seguretat de 128 bits és més segur que un sistema de seguretat de 64 bits.

El principal desavantatge del xifratge simètric és que, en l'exemple de l'Administració electrònica, l'Administració té la nostra clau. Aquest fet implica un risc, ja que alguna persona de l'Administració pot tenir incentius per a facilitar la clau dels ciutadans a tercers. I, àdhuc suposant una incorruptibilitat total de l'Administració, sempre hi haurà el risc que els sistemes informàtics d'aquesta administració pateixin atacs amb l'objectiu de conèixer totes les claus de tots els ciutadans. Solament si el ciutadà és l'únic que coneix la seva clau corresponent, el risc disminueix considerablement.

Per a evitar que ambdues parts comparteixin una única informació, amb el risc que s'emmagatzemi per partida doble i amb l'inconvenient que en algun moment és necessari arribar a un acord per a compartir o consensuar aquesta informació –i això comporta també dificultats i riscos–, es crea el **xifratge asimètric o de clau pública**. En aquest sistema es creen un parell de claus, la pública i la privada. Com els seus noms indiquen, la clau pública és coneguda

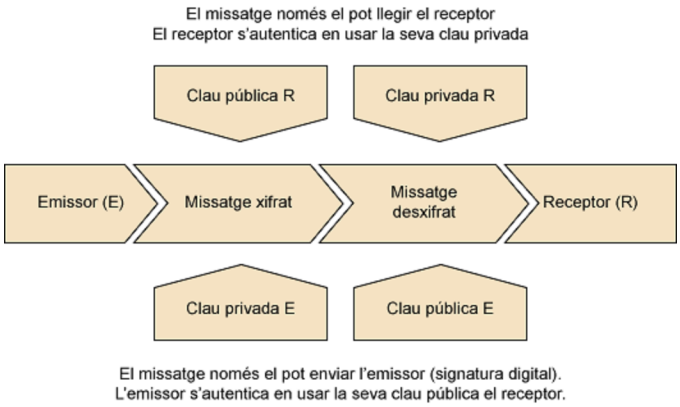
per tot el món, mentre que la clau privada queda sota custòdia d'un únic usuari. Per a establir una comunicació, un emissor utilitza la clau pública –que el receptor haurà posat a la seva disposició directament o bé facilitant-la en el seu propi lloc web– per a xifrar un missatge que solament el receptor podrà desxifrar amb la clau privada. Amb aquest procediment, hi ha dues garanties:

- que el missatge no pateix canvis per ocultar-se a tercers;
- que solament el receptor legítim pot llegir el missatge.

Queda clar, per tant, que aquest sistema aporta certes millores davant la criptografia simètrica: mentre les claus no les tenen tots dos interlocutors, amb els riscos i inconvenients que això comportaria, el missatge té una **integritat** amb la clau privada, i el seu contingut no es pot veure i, ni molt menys, modificar. El sistema és totalment vàlid per a pagar impostos, per exemple. No obstant això, queda una qüestió en l'aire: com saber si l'emissor del missatge és qui diu que és, ja que la criptografia de clau pública garanteix solament la integritat del missatge, i solament el destinatari podrà desxifrar-lo amb la seva clau privada.

La **signatura digital** soluciona aquests problemes, i ho fa, a més, utilitzant el mateix sistema: la criptografia de clau pública. Fins ara hem considerat la parella clau pública - clau privada com un sistema amb el qual la clau pública «tanca» un missatge que solament pot ser «obert» per qui tingui en el seu poder la clau privada, que és el «negatiu» de la clau pública. Si ho pensem bé, si una clau desfà allò que l'altra fa intuïm que l'ordre en què les operacions tinguin lloc hauria de ser independent. I és així almenys en aquest tipus de xifratge: la signatura digital és l'aplicació inversa del xifratge asimètric. Un emissor xifra un missatge amb la seva clau privada. Solament si és cert que l'emissor és qui diu que és, la seva clau pública –recordem, a l'abast de qualsevol persona– podrà desxifrar el missatge. Si amb la clau pública de l'emissor es pot desxifrar el missatge, el missatge s'ha xifrat amb la clau privada d'aquest emissor, que solament ell té. Podem veure un resum gràfic del funcionament del xifratge asimètric o de clau pública, inclòs el cas de la **signatura electrònica** en la imatge següent.

Figura 1. Xifratge asimètric o de clau pública



Font: elaboració pròpia.

Resumint, el **xifratge de clau pública** aporta **confidencialitat** a la comunicació. D'una banda, garanteix que el missatge arriba a qui ha d'arribar. D'altra banda, garanteix que l'origen del missatge és **autèntic**. I no solament és autèntic, sinó que és impossible repudiar aquest missatge o transacció: solament l'emissari amb la seva clau privada pot haver efectuat l'acció que desfà la seva clau pública. En l'Administració electrònica el **no repudi** és fonamental per a molts processos administratius, de la mateixa manera que ho és l'autenticació del ciutadà. Pensem, per exemple, en l'Administració electrònica de Justícia, on fer o deixar de fer alguna cosa pot tenir conseqüències diferents.

Encara que en la figura 1 hem presentat la confidencialitat del missatge i l'acreditació del receptor, d'una banda, i l'acreditació de l'emissor, de l'altra, en el fons aquestes dues qüestions es poden resoldre conjuntament amb dos xifratges seqüencials: l'emissor xifra el seu missatge amb la seva clau privada –autenticant la seva autoria, és a dir, signant el missatge electrònicament– i després el resultat amb la clau pública del receptor, de manera que garanteix que solament aquest podrà llegir el missatge. Amb aquest procediment «senzill» –elaborat pràcticament del tot pels ordinadors i tan automàticament com volem–, s'aconsegueix l'**autenticació** de les parts, el **no repudi** i la **integritat**. La **confidencialitat** queda garantida pel mateix fet que els missatges estan signats i dirigits a un receptor concret.

2. Certificació digital

Arribats en aquest punt, es posa de manifest una altra possible feblesa del sistema, una mica menys intuïtiva i en certa manera més filosòfica: el fet que la clau pública que hem creat sigui la que hem d'utilitzar per a enviar un missatge, per exemple, a l'Administració, no significa que aquesta clau pública pertanyi realment a l'Administració. Mentre que l'edifici seu de l'Agència Tributària en una determinada ciutat és difícil de suplantar –sempre ha estat al mateix lloc, en coneixem alguns dels treballadors, etc.–, el fet que algú ens enviï una clau pública dient que és l'Administració Tributària no ens hauria de merèixer cap tipus de confiança *a priori*.

- Com podem saber que una clau pública pertany sens dubte a qui diu que n'és el propietari? Suposem que algú ens dona la seva clau pública dient que és un ciutadà que vol interposar una denúncia (electrònica) a l'Administració de Justícia. Considerarem vàlids els seus missatges, tot i que sigui un impostor, perquè podrem desxifrar-los.

- Com podem saber que una clau pública és sens dubte la de qui nosaltres creiem que és? Suposem que trobem la clau pública de l'Agència Tributària en un lloc web que creiem de confiança. Els nostres missatges podran ser llegits per algú que tingui la clau privada que és parella d'aquesta pública. Aquest algú pot ser perfectament un impostor que ha simulat que la seva clau pública és la de l'Agència Tributària, de manera que els nostres impostos aniran directament al seu compte bancari personal.

Cal, doncs, que una persona o organisme s'erigeixi en acreditador de la titularitat de les claus públiques. L'organisme acreditador –com un bancs amb capacitat d'emetre moneda– certifica i garanteix, de manera directa o indirecta, tant la identitat digital de les persones i institucions com l'autenticitat dels documents que aquestes generen.

Un **certificat digital** –emès per **una entitat de certificació digital**– és un document electrònic que acredita –certifica– que el nexe que hi ha entre un determinat parell de claus pública i privada i una persona és autèntic, és a dir, que una determinada clau pública pertany realment a qui en reclama la propietat, mentre que la relació entre la clau pública i la privada no fa falta certificar-la, ja que es valida per construcció. El certificat, doncs, uneix una persona o institució amb una clau pública i, per norma general, li associa una sèrie de dades com la validesa del certificat (inclosa la data d'expiració) i la signatura digital de l'entitat acreditadora, és a dir, que el certificat digital va signat digitalment per a garantir l'autenticitat.

Per descomptat, aquí ens enfrontem amb l'antiga qüestió de qui vigila el vigilant o, en el nostre cas, qui certifica el certificador. Cal recórrer en última instància a una entitat que tingui la confiança absoluta de la població. Recorrem a entitats estatals com la Fàbrica de Moneda i Timbre –a Espanya– o bé a entitats privades d'acreditació de solvència contrastada, com l'empresa Verisign.

El certificat digital –o infraestructura de clau pública segons el seu nom tècnic– permet acreditar usuaris i les seves comunicacions, sia missatges electrònics o, el que és molt important per al cas de l'Administració electrònica, un lloc web.

En l'exemple de la figura 2 es pot apreciar que la Fàbrica Nacional de Moneda i Timbre espanyola –en les seves sigles, FNMT– ha emès un certificat per a la pàgina web w1.renfe.es garantint que es tracta efectivament del lloc de la Xarxa Nacional de Ferrocarrils Espanyols (en les seves sigles, RENFE). Ens n'indica també el període de validesa. L'ús més evident d'aquest certificat és garantir a l'usuari que les compres de bitllets de tren que faci en aquesta pàgina web són efectivament productes autèntics garantits per l'empresa de ferrocarrils RENFE, i que els seus pagaments amb targeta electrònica no aniran a parar a mans de tercers perquè la pàgina sigui un frau.

Figura 2. Certificat digital

Font: elaboració pròpia.

En aquest últim exemple l'FNMT emet a favor de RENFE un certificat digital, signat digitalment per l'FNMT –recordem que la validesa de la signatura de l'FNMT es fonamenta en una confiança total en aquesta institució per part de la resta d'agents, atès que ningú no certifica la validesa de la seva signatura–, de manera que garanteix que tot el que RENFE firma digitalment amb aquesta signatura certificada és autèntic.

Els certificats electrònics són creats per programes especials en els servidors de l'entitat certificadora i llegits per altres programes utilitzats pels clients de manera integrada en les diferents aplicacions de missatgeria electrònica o pàgines web, entre d'altres. L'emissor del missatge pot signar electrònicament amb un programa a aquest efecte o amb dispositius físics com targetes magnètiques o llapis de memòria USB preparats especialment per a això.

El **document d'identitat digital** –a Espanya anomenat DNI electrònic o digital– no és sinó una eina física per a signar digitalment. Aquest document, que pot prendre la forma d'una targeta de crèdit amb la incorporació d'un xip, emmagatzema a l'interior una sèrie de dades sobre la persona titular i tres certificats:

- El primer, més important, és el certificat de l'entitat certificadora, que garanteix que tot el conjunt és autèntic.
- El segon és un certificat d'autenticació –i la seva clau privada–, la qual cosa ens permetrà accedir a recintes o ordinadors introduint solament el document d'identitat digital. Aquest certificat substitueix altres mètodes d'autenticació digital, com els basats en biometria (vegeu el principi d'aquest apartat).
- El tercer és el certificat de signatura digital –i la seva clau privada–, per a signar documents i efectuar transaccions mitjançant sistemes informàtics.

Els sistemes informàtics que utilitzen el xifratge asimètric es basen en l'anomenada **transport layer security** (**TLS**). TLS és un protocol de xifratge asimètric que s'utilitza en diverses aplicacions, com el correu electrònic o la comunicació per la web. Utilitza els certificats electrònics –que, recordem, incorporen la clau pública– per a establir, entre altres coses, l'autoria d'una pàgina o un missatge signat amb una clau privada. Podem saber que una pàgina web ha estat acreditada perquè en el seu URL apareix el protocol HTTPS, que no és sinó el protocol HTTP habitual amb l'afegit de la tecnologia TLS, i un cadenat tancat en la barra d'estat del navegador, normalment en la part inferior, en la barra de navegació o en tots dos llocs, com es pot apreciar en la imatge següent, captura de pantalla de l'Oficina Virtual de l'Agència Tributària Espanyola.

Vegeu també

Sobre els protocols TLS, podeu veure el subapartat 2.1, «Internet i comunicació en xarxa».

Figura 3. Pàgina xifrada amb protocol SSL

Cal tenir en compte una qüestió molt important: el fet que aparegui l'esmentat cadenat en la part inferior del navegador no significa que la pàgina sigui autèntica –en el sentit de pertànyer a qui creiem que pertany–, sinó que s'ha establert una relació satisfactòria –certificada– entre la pàgina i el seu propietari. Comprovar, llegint el certificat corresponent, que la persona o organització a qui pertany aquesta pàgina és efectivament la persona o organització amb qui es vol tenir tractes correspon a tots i cadascun dels usuaris.

Vegeu també

La suplantació, generalment amb finalitats delictives, d'identitats corporatives mitjançant pàgines web falses és tractada en l'apartat 3.3.2 en parlar del *phishing*.

Pretty Good Privacy

Hi ha altres mètodes per a proveir aspectes de privadesa i autenticació, el més conegut dels quals és probablement l'anomenat Pretty Good Privacy (PGP).

3. Cibercrim

Tal com passa en la vida fora de la xarxa, mentre determinades institucions i usuaris intenten protegir la seva identitat o les seves comunicacions, hi ha terceres organitzacions i persones que persegueixen justament el contrari: violar els sistemes de seguretat establerts per accedir a dades o propietats que puguin explotar en benefici propi. En el cas d'internet, allò el criminal persegueix és apropiar-se directament o indirectament de dades que pugui utilitzar fraudulentament.

A grans trets, hi ha tres maneres genèriques d'apropiar-se de les dades d'un usuari –individual o institucional– per usar-les amb finalitats delictives:

- La primera, robar-les per la força bruta, obtenir-les en presència d'un usuari obligant-lo, per exemple, a subministrar el seu nom d'usuari i la clau secreta, o bé entrant en el sistema informàtic on es guarda aquesta informació.

- La segona, induir l'usuari a subministrar-les convencent-lo que no ho està fent, és a dir, conduint l'usuari a l'error.

- La tercera, induir l'usuari a fer una transacció en benefici d'un tercer en lloc d'en benefici del mateix usuari –de fet, no és un robatori de dades en sentit estricte.

3.1. Atacs al sistema

Per al cas que el criminal vulgui apoderar-se de les dades entrant en el sistema informàtic –no presencialment–, hi ha una sèrie de dispositius, tant màquines com programes, que reben el nom de ***firewall*** o **tallafoc**. De la mateixa manera que en el cas d'un incendi, l'objectiu del tallafoc és elevar barreres que dificultin accedir a la informació sensible per part de tercers, controlant bàsicament la manera en què té lloc, i per part de qui, el trànsit entre les diferents aplicacions i espais d'un servidor. Al moment en què un usuari no autoritzat intenta accedir a unes dades (zona) per a les quals no té permís d'accés, aquest accés és denegat i l'usuari és expulsat del sistema. La complexitat d'aquest procediment rau a detectar a temps les diferents incursions –atacs– dels criminals en el sistema, la manera en què ho estan fent i ser capaç d'expulsar-los d'aquest sistema. Es diu que un sistema té un **forat de seguretat** quan és possible accedir a una zona restringida sense que el sistema detecti la presència de l'intrús o sense que li sigui possible expulsar-lo. De vegades aquest forat de seguretat és creat deliberadament pels dissenyadors del software amb el que s'anomena **porta posterior**, que, igual que en un edifici, permet accedir al programa o a la xarxa de seguretat sense haver de passar pels processos d'autenticació ha-

bituals. Aquestes portes posteriors, a més de ser programades en origen –no tenen per què ser malintencionades, sinó que s'utilitzen sovint per a facilitar el treball als programadors en reparacions dels programes, encara que pràcticament sempre és una molt mala idea habilitar portes posteriors–, es poden crear també amb programes infiltrats que, a diferència del cas anterior, sí que pretenen obrir aquesta porta amb intencions il·legítimes.

Reben el nom de ***malware*** o ***software*** **maliciós** els programes dissenyats amb finalitats nocives. Per descomptat, per nocives podem entendre una infinitat de coses, entre les quals hi ha les que fa un ***adware*** o programes de publicitat, que ens mostra, generalment contra la nostra voluntat, ofertes o material publicitari quan funciona un determinat programa, generalment un navegador web.

No obstant això, el *software* maliciós sol tenir pitjors intencions que la mera informació sobre ofertes publicitàries, i el seu objectiu principal és robar informació de l'usuari, en el millor dels casos, o utilitzar el seu ordinador per a finalitats pròpies, en el pitjor dels casos.

El *software* maliciós o *malware* se sol classificar en dos grans grups, la diferència entre els quals, que rau en aspectes tècnics més que en les seves funcionalitats, és innòcua per a l'usuari final:

- El **virus**, que necessita «contaminar» un altre programa per a reproduir-se. La manera de «contaminar» un ordinador és afegir una porció de codi a un programa ja existent en el sistema. El principal problema a l'hora d'eliminar un virus és que, com que **infecta** un altre programa –l'**hoste** o *host*–, pot resultar molt complicat i fins i tot impossible separar el codi del virus del codi de l'hoste, per la qual cosa cal recórrer a eliminar l'hoste, amb la corresponent pèrdua de les dades d'aquest.

- El **cuc** o *worm*, que a diferència del virus no necessita infectar un altre arxiu, sinó que pot autoreplicar-se de manera independent i copiar-se en tants sistemes com li és possible. Encara que l'eliminació del cuc és molt més neta que la del virus, el principal desavantatge d'aquest tipus de *software* maliciós és que aprofita els canals de comunicacions oberts a l'exterior –correu electrònic, navegador web, compartició d'espais en una xarxa LAN– per a reproduir-se en altres sistemes enviant còpies a tants ordinadors com li és possible, amb el corresponent consum d'amplada de banda i altres recursos afegits.

Una de les principals maneres en què els cucs poden instal·lar-se en un ordinador, a més de contaminar mitjançant missatges de correu electrònic i un altre tipus de comunicacions, és mitjançant programes que l'usuari descarrega i utilitza deliberadament. Un **cavall de Troia** –o *troià*, en honor al mite– és un programa que apareix a l'usuari com una eina útil per a fer determinades funcions. L'usuari el descarrega de la xarxa, l'instal·la i l'executa. Per norma

general, sí que fa les funcions promeses, però també inclou altres funcions que pretenen, en el fons, aconseguir el control de l'ordinador per recopilar informació i dades sensibles. Sovint, el troià és la manera que el cibercriminal utilitza per a poder instal·lar el cuc en l'ordinador aliè, ja que, com que és l'usuari final el qui executa conscientment el programa, és una manera fàcil i ràpida de saltar qualsevol tipus de protecció que l'ordinador pot tenir, sia el tallafoc o un programa **antivirus**, dissenyat per a evitar les infeccions per virus o cucs.

Aquí es canvia l'enginyeria tecnològica per quelcom més subtil: l'**enginyeria social**. La dita que diu que una cadena és tan forta com la més feble de les seves baules és antiga. En aquest cas, per més que es reforci tècnicament el sistema, si l'usuari és la baula més feble, els atacs del criminal incidiran amb major força justament aquí.

En general, es coneix com a ***spyware*** o **programes espia** tot *software* maliciós que pretén monitorar allò que fa l'usuari en el seu ordinador per comunicar-ho posteriorment a un altre ordinador per la xarxa. Aquest monitoratge pot tenir un baix impacte, per concentrar-se a analitzar els hàbits de consum o de navegació de pàgines web de l'usuari, o bé tenir un major impacte en obtenir informació sobre noms d'usuari i les claus secretes associades, sia d'accés a altres xarxes privades –per a accedir a una altra informació– o d'accés a comptes bancaris o comptes de client en establiments de venda en línia.

3.2. Engany a l'usuari

En el segon i tercer cas que hem esmentat, on en lloc d'entrar per la força en el sistema s'indueix l'usuari a un error, en els últims anys s'han generalitzat dues pràctiques, amb més o menys variacions encara que sempre amb estratègies similars i, per descomptat, amb les mateixes finalitats. Ambdues pràctiques recuperen la filosofia amb què concloíem el subapartat anterior: la baula més feble en la seguretat del sistema sol ser l'usuari, sia perquè el seu baix nivell d'alfabetització digital fa que tots els aspectes tècnics li semblen secrets i insondables, o perquè acaba saltant-se les incòmodes mesures de seguretat en honor de treballar més còmodament i ràpidament. Davant l'estat d'hipnosi que comporta l'aclaparador bombardeig d'argot informàtic per a l'ignorant, aquest adopta una posició d'inèrcia basada en el «sí a tot», en la qual accepta a ulls clucs tot el que el sistema li proposa i, en el pitjor dels casos, el que un suposat expert li aconsella amb la finalitat de facilitar-li els tràmits.

El ***phishing*** –paraula composta de *password harvesting* o cultiu de claus d'usuari, que en anglès té una pronunciació semblant a la de *pescar* en anglès–, persegueix aconseguir generalment dades d'accés a xarxes o serveis en línia (com les esmentades dades bancàries o comptes de client) per a després utilitzar-les en benefici propi suplantant la identitat de l'usuari legítim. El procés més habitual és enviar un missatge de correu electrònic –o per qualsevol altra via– a un usuari en què se li sol·licita aquesta informació. Per a justificar la petició, se li explica, per exemple, que hi ha hagut un error en la base de dades i que

el seu compte s'ha de reactivar; els arguments són infinits, encara que tots solen girar al voltant del mateix eix. És sorprenent constatar que el nombre de persones que responen a aquestes sol·licituds d'informació proporcionant les seves dades secretes és espectacularment elevat.

El *phishing*, a més d'utilitzar arguments més o menys convincents, també utilitza plantilles i pàgines web amb la imatge de la institució (per exemple, la imatge de la banca virtual que es pretén suplantar) per a reforçar l'aparença de veracitat d'aquest engany. En molts casos s'arriba a replicar la pàgina original en un servidor fals, és a dir, en un servidor que no és propietat de la institució autèntica, aprofitant mínimes modificacions de l'URL per a aparèixer com a veritable: per exemple, utilitzant l'adreça www.mibanccoonline.com en lloc de la que seria l'autèntica, www.mibancoonline.com. Noteu que en el cas del primer URL, el fals, hi ha una lletra c de més. Si la rèplica és prou bona, és fàcil que aquest petit canvi en el nom de l'URL passi desapercebut, i més per a l'usuari que navega a internet només ocasionalment.

No obstant això, aquest punt no deixa de ser un cert error en el disseny de l'estratègia d'engany del cibercriminal, error que ha trobat la solució en un mètode més sofisticat, el *pharming*.

El ***pharming*** –que de vegades es confon amb la variant de *phishing* en què es replica la pàgina web del servei en línia– utilitza una vulnerabilitat del sistema DNS, de manera que es pot redirigir un domini a un altre domini o, millor dit, una adreça IP (la legítima) a una altra adreça IP (on resideix la rèplica falsa) sense que l'usuari no ho noti, fins i tot quan tecleja correctament el nom del domini en el navegador. A diferència del *phishing*, el *pharming* no solament fa una còpia falsa de la pàgina web i la fa semblar igual a l'original, sinó que emmascara la IP falsa amb el nom de domini autèntic de la pàgina original.

Per a això és necessari que hi hagi, com a mínim, dos errors en la seguretat del sistema:

- El primer és que el criminal pugui controlar el servidor DNS de la víctima, és a dir, que pugui entrar en el seu ordinador i prendre el control del programa que dirigeix un nom de domini a una determinada IP. A aquests efectes, s'empren, entre altres eines, troians i programes espia o *spyware*.

- El segon és que l'usuari no accedeix a la pàgina amb un protocol segur, a saber, amb la combinació HTTP + TLS (o HTTPS) que hem comentat al principi d'aquest apartat, o bé que, fins i tot fent-ho, no nota que ha estat redireccionat a un entorn no segur i que, entre altres coses, el cadenat tancat no apareix en la barra d'estat del seu navegador web.

Per a concloure aquest apartat, volem donar una reflexió doble.

La primera és posar de manifest els enormes avantatges que pot tenir una identitat digital certificada correctament, de manera que es possibiliti una infinitat de tràmits en línia amb tanta o més seguretat que la contrapart presencial. No hi ha cap dubte que, si l'Administració electrònica vol fer quelcom més que proporcionar informació mitjançant la xarxa, aspectes com el xifratge de clau pública, la certificació digital o el document d'identitat digital seran tecnologies d'ús comú en el seu àmbit i, per tant, serà necessària una àmplia informació en tots els nivells i a tots els agents implicats en el seu ús.

La segona reflexió, malgrat incidir sempre en el mateix aspecte, és que cal no oblidar que en aquests moments de ràpida adopció de noves tecnologies el desconeixement sumat a l'enlluernament de la passió fan que l'usuari sigui poc previngut i, en conseqüència, especialment vulnerable a enganys i mals usos d'aquesta tecnologia. Les conseqüències, però, són molt més greus que quan passen precisament al món real. Una vulnerabilitat en un sistema informàtic provocada per un descuit per un dels seus usuaris no solament posa en perill la identitat o el patrimoni d'aquest, sinó que, com que tots els sistemes estan interconnectats, posa en un seriós conflicte el sistema íntegrament i, amb això, totes i cadascuna de les dades que hi resideixen.

Molts tecnòlegs afirmen que una gran part dels defectes de seguretat dels sistemes existeixen, precisament, pel desconeixement mateix que els mateixos tècnics tenen d'aquests sistemes, no solament l'usuari final. L'argument és que, si el codi dels programes no pot ser analitzat, és impossible saber què fa exactament un programa i, per aquest motiu, fins i tot en el millor dels casos, quan es detecta una disfunció, és dificilíssim solucionar-la perquè no se sap quin procés en concret cal modificar. En conseqüència, afirmen que el *software* lliure és l'únic que pot proporcionar la seguretat deguda al sistema.

4. Anonimització i xarxes privades virtuals (VPN)

La criptografia i la certificació digital es poden utilitzar per a garantir la nostra identitat i fer-la pública, o bé per a tot el contrari: ocultar la nostra identitat i totes les operacions que efectuem a la xarxa. Els motius per a això –tant legítims com il·legítims– poden ser nombrosos, entre els quals en caldria destacar almenys dos: el primer és per a evitar que en la nostra anada i vinguda a la xarxa les nostres dades puguin ser robades; el segon és perquè la nostra identitat pugui ser traçada, la qual cosa podria significar exposar-se a la censura, la repressió i fins i tot posar en perill la pròpia vida en alguns règims autoritaris.

Una primera manera d'ocultar la pròpia identitat és a partir dels anomenats **proxy abiertos**. Tal com hem vist, el servidor intermediari és el que canalitza les peticions d'un ordinador cap a internet. Un servidor intermediari obert anònim fa aquestes mateixes funcions però oculta la IP de l'ordinador personal, de manera que la identitat d'aquest queda en el tram de comunicacions entre l'ordinador mateix i el servidor intermediari. El gran avantatge d'utilitzar aquest tipus d'eina rau en el fet que qualsevol missatge, visita a una web, recurs pujat a internet, etc. no podrà ser traçat fins al seu origen, i es preservarà la privadesa de l'usuari.

Els desavantatges dels servidors intermediaris oberts són diversos. Pel que fa a l'usuari, cada vegada és més freqüent que les pàgines web utilitzin dades emmagatzemades en l'ordinador (mitjançant *cookies*, per exemple) per a personalitzar la navegació. Això sol ser impossible de dur a terme amb anonimitzadors, per la qual cosa la navegació pot tornar-se menys usable. D'altra banda, com que l'anonimització es pot usar per a finalitats poc ètiques o fins i tot il·legals, no deixa de ser un perill arriscar-se a allotjar, en un servidor intermediari obert, activitats que puguin donar lloc a delictes. Com que la traçabilitat s'interromp en aquest servidor intermediari, és aquí on acabarà (o començarà) la recerca policial d'uns presumptes delictes.

Un pas més enllà dels servidors intermediaris oberts són les **xarxes d'anonimització**, com la popular TOR (*the onion router*), que combina una xarxa de servidors que, a més d'encaminar repetides vegades les comunicacions, encripten les dades per ocultar-ne el significat. A diferència del cas dels servidors intermediaris oberts, les xarxes d'anonimització fan opaca no solament la identitat de l'usuari sinó també el missatge per si mateix, la qual cosa augmenta la seguretat de les comunicacions.

TOR

TOR és una eina d'anonimització utilitzada popularment en situacions de comunicació de risc: http://www.torproject.org

Les **xarxes privades virtuals** (VPN segons la sigla anglesa) utilitzen mecanismes semblants a les xarxes d'anonimització, però el seu objectiu és l'oposat a aquestes: garantir la identitat dels usuaris i la integritat dels missatges. És a dir, en utilitzar una VPN l'usuari es connecta amb un servidor i es garanteix que

tant l'un com l'altre (l'usuari i el servidor) són els que diuen ser, la qual cosa és especialment útil per a connexions entre professionals (seus d'una mateixa empresa connectades per internet, treballadors itinerants que es connecten a la seu, etc.). D'altra banda, i una vegada establerta la connexió entre el client i el servidor, la comunicació es xifra perquè sigui secreta. Aquesta funcionalitat serveix, més enllà de protegir les dades que s'intercanvien a la xarxa, també per a protegir altres dades que circulen igualment per internet però que tendim a oblidar que ho fan, com noms d'usuari i contrasenyes per a accedir a comptes remots de correu electrònic o d'accés a xarxes socials. Així, fora de l'àmbit estrictament professional, és aconsellable utilitzar les VPN quan s'accedeix a internet mitjançant una connexió poc fiable o manipulable fàcilment, com la connexió wifi d'una sala de conferències o d'un hotel.

5. Altres mesures d'autenticació

L'autenticació en sistemes digitals ha consistit tradicionalment en la combinació d'un nom d'usuari i una contrasenya. Però, tal com hem vist en els casos del *phishing* i el *pharming* –i altres mecanismes d'enginyeria social–, enganyar l'usuari mitjà per obtenir-ne la contrasenya no és excessivament difícil, sobretot si les seves credencials donen accés a dades prou importants, que poden motivar un atacant per a fer tot tipus d'esforços. És per això que en entorns que requereixen nivells elevats de seguretat s'utilitzen altres mesures. Les més freqüents són la **identificació biomètrica** i l'**autenticació de doble factor**.

És més que probable que el lector hagi usat, o vist usar, algun telèfon mòbil o ordinador que podem desbloquejar usant l'empremta dactilar o bé apuntant-ne la càmera al rostre de l'usuari: la càmera reconeix a l'usuari i desbloqueja el dispositiu. Es tracta de mètodes molt populars per la seva comoditat, però s'han de tenir en compte algunes de les seves limitacions. La primera es refereix a la tecnologia que s'usa per a reconèixer empremtes o cares. Tant en l'un cas com en l'altre, hem de tenir en compte dos tipus d'error possibles. D'una banda, pot passar que el sistema no ens reconegui i, per tant, no ens hi doni accés. Afortunadament, encara que això pot ser incòmode, sempre disposarem del mecanisme convencional d'usuari i contrasenya o d'un PIN (número d'identificació personal). D'altra banda, hi ha un error més perillós: el sistema pot confondre una empremta aliena –o una reproducció, fotogràfica o d'un altre tipus, de la nostra cara– amb la nostra, i donar accés així a un atacant a totes les nostres dades. Abans d'usar un sistema d'identificació biomètrica, doncs, és essencial documentar-se sobre la tecnologia que usa i sobre les probabilitats que es produeixi aquest segon tipus d'error (per a una identificació facial que usa càmeres convencionals, per exemple, la taxa d'error pot ser tan elevada com un entre deu mil, taxa que pot ser inacceptable per a moltes finalitats).

Una altra limitació de la identificació biomètrica està molt relacionada amb aquests tipus d'errors. Hi ha un parell d'aforismes usats amb freqüència pels experts en seguretat que la il·lustren. El primer és que la identificació biomètrica hauria de ser l'equivalent del nom d'usuari, no de la contrasenya. Això és així pel segon aforisme, que diu que les contrasenyes són com la roba interior, si se'ns permet el llenguatge vulgar: s'han de canviar amb freqüència. És obvi que en cas que un atacant aconsegueixi replicar la nostra empremta dactilar o la nostra cara –quelcom més senzill del que un podria imaginar si l'atacant és prou sofisticat i té prou interès–, i el nostre sistema d'autenticació en depèn, el problema que tenim és greu perquè difícilment podrem canviar-les.

Un altre mecanisme, en aparença més rudimentari però moltes vegades més efectiu, és l'autenticació de doble factor, que ens exigeix dos factors per a accedir a un sistema: el primer pot ser l'habitual combinació d'usuari i contrasenya,

però el segon té a veure amb un objecte –físic o lògic– que obra en el nostre poder, i al qual un atacant hauria d'accedir també per a obtenir l'accés. Aquest objecte pot tenir la forma d'un petit dispositiu amb una pantalla que mostra un codi alfanumèric que canvia periòdicament d'acord amb un algorisme pràcticament impossible de desxifrar, o claus USB que exerceixen la mateixa funció de generar periòdicament codis però que, en comptes de mostrar-nos aquest codi per poder-lo teclejar nosaltres, l'introdueixen directament en el sistema. En l'actualitat aquests dispositius físics són substituïts cada vegada més per petites aplicacions mòbils que exerceixen aquesta funció. Naturalment, sempre és necessari tenir en compte que en algun moment l'usuari oblidarà la seva clau USB, o fins i tot el seu mòbil, i per tant cal donar camins alternatius per a poder accedir. És vital, per a la seguretat del sistema, que aquestes vies alternatives siguin prou segures –la qual cosa sol comportar un cert nivell d'incomoditat per a l'usuari– per a no posar-lo en risc, perquè, tal com hem dit, la seguretat d'una cadena és la de la baula més feble.

Bibliografia

INTECO (2010). *Estudio sobre el fraude a través de Internet 2009* [en línia]. Madrid: INTECO. <http://www.inteco.es/file/xk6K9xU46WM_Q1i88xyWtA>