Introducció a les vulnerabilitats

Guillermo Navarro Arribas

PID_00178947

Universitat Oberta de Catalunya
www.uoc.edu

Índex

Introducció

Avui dia ningú no dubta de la importància que té la seguretat informàtica en les nostres vides. Vivim, cada vegada més, envoltats de dispositius informàtics que ens faciliten el dia a dia. Reservar entrades o fer la compra per Internet, un cotxe amb un alt grau d'automatització i capacitat de comunicació, un telèfon mòbil en el qual parlar sembla una funció secundària, la digitalització de pràcticament totes les dades relacionades amb nosaltres (l'Administració pública, les empreses, o les nostres dades personals, com agenda, correu electrònic, documents, etc.), són coses amb les quals ens hem acostumat a viure. De la mateixa manera, també hem començat a percebre la importància de la seguretat informàtica. Avui dia són freqüents les notícies en la premsa no especialitzada sobre incidents de seguretat en el món digital, com el robatori de targetes de crèdit, la suplantació d'identitat, el robatori de dades confidencials, o fins i tot atacs dirigits sobre infraestructures crítiques.

Aquesta assignatura introdueix la problemàtica de la seguretat informàtica i ho fa descrivint-ne i estudiant-ne una part concreta: les vulnerabilitats que presenten els sistemes d'informació. L'existència d'una vulnerabilitat en un sistema d'informació és el que possibilita que aquest sistema pugui ser atacat. Per això, en fer un repàs de les vulnerabilitats estem donant una introducció al problema de la seguretat informàtica per la seva base. Dit d'una altra manera, veurem el perquè de la seguretat informàtica.

Aquest mòdul introdueix els conceptes bàsics sobre els quals es desenvoluparà l'assignatura. Veurem què és una vulnerabilitat, per què són importants, com es classifiquen i com es gestionen.

Objectius

Els objectius que l'estudiant ha d'haver aconseguit després d'estudiar els continguts d'aquest mòdul són els següents:

1. Entendre el concepte de vulnerabilitat de seguretat i el seu context.
2. Conèixer com s'identifiquen i cataloguen les vulnerabilitats.
3. Conèixer com es gestionen les vulnerabilitats, i l'existència d'equips especialitzats.

1. Nocions bàsiques

Una **vulnerabilitat** de seguretat es pot veure com el punt de partida de tot el procés que implica la seguretat en general. Per exemple, un atac informàtic sobre un servidor web generalment parteix d'una vulnerabilitat en algun dels sistemes que implementen o donen suport al servidor: errors en la implementació del servidor o sistema operatiu mateix, fallades en el disseny de protocols de comunicació, errors propiciats per la inexperiència del personal encarregat d'utilitzar o administrar el servidor, etc. La dificultat de preveure aquests errors i, per tant, els possibles atacs que es derivin porta a la implantació de mesures preventives i reactives, com l'ús de tallafocs, sistemes de detecció d'anomalies o intrusions, realització d'auditories de seguretat, plans de contingència, o educació a usuaris i administradors.

Definir què és una vulnerabilitat no és senzill i per a això és necessari dotar de context aquesta definició. En aquest sentit, ens centrarem en vulnerabilitats de seguretat en sistemes d'informació.

Considerem els sistemes d'informació (SI) de manera molt general com qualsevol sistema destinat a recollir, emmagatzemar, processar o distribuir conjunts d'informació. Encara que generalment s'associa el concepte de sistema d'informació al món empresarial, adoptem el sentit més ampli d'SI abastant l'ús tant personal com dins d'una organització. En general, en parlar d'SI ens referirem a un sistema informàtic, encara que no tots els SI són informàtics. És important fer ressaltar que l'estudi de la seguretat dels SI i les seves vulnerabilitats abasta no solament els SI pròpiament, sinó també l'estudi de totes les entitats i els fenòmens que poden afectar directament o indirectament els SI. Aquesta és una visió molt àmplia d'SI que pot comprendre, entre altres: ordinadors d'ús personal, telèfons mòbils, servidors de correu electrònic, servidors web, sistemes d'emmagatzematge de dades, sistemes de comunicació d'informació, xarxes telemàtiques, als usuaris d'aquests sistemes, etc.

Vegeu també

Veurem algun exemple de vulnerabilitats dels sistemes d'informació no informàtics en el mòdul "Enginyeria social".

La seguretat en els SI comença a partir de l'existència de vulnerabilitats relatives a aquests sistemes. Una vulnerabilitat no tindria sentit si després no pogués ser explotada per un atac amb l'objectiu de violar la seguretat del sistema. És molt comú associar el concepte de vulnerabilitat al d'*error*, encara que aquesta equivalència convé matisar-la adequadament. En aquesta línia, adoptem la definició següent de vulnerabilitat.

Una **vulnerabilitat de seguretat** és una fallada o debilitat en el disseny, la implementació, l'operació o la gestió d'un sistema, que pot ser explotat amb la finalitat de violar la política de seguretat del sistema.

A continuació detallem alguns dels conceptes relacionats.

Lectura complementària

Les definicions bàsiques d'aquest apartat estan basades en aquestes obres: **R. Shirey** *Internet Security Glossary*, RFC 2828, IETF. Disponible en línia a: http://www.ietf.org/rfc/rfc2828.txt

Una **política de seguretat** és el conjunt de regles i pràctiques que defineixen i regulen els serveis de seguretat d'una organització o sistema amb el propòsit de protegir-ne els recursos crítics i sensibles. En altres termes, és la declaració del que està permès i el que no està permès fer.

La política de seguretat és la base de la seguretat d'un sistema. S'hi detallen els serveis de seguretat del sistema, es determina qui o què es pot fer o no amb els recursos del sistema, i generalment s'especifica com s'implementen aquests serveis. La implementació concreta d'una política de seguretat es du a terme mitjançant **mecanismes de seguretat**. La política no ha de ser necessàriament una declaració formal; de vegades es tracta de simples directrius sobre la seguretat del sistema en llenguatge informal.

En general, parlem d'incident de seguretat per a referir-nos a qualsevol fet que representa una violació de la seguretat del sistema. En el cas que l'incident sigui intencionat, ens hi referim com a atac.

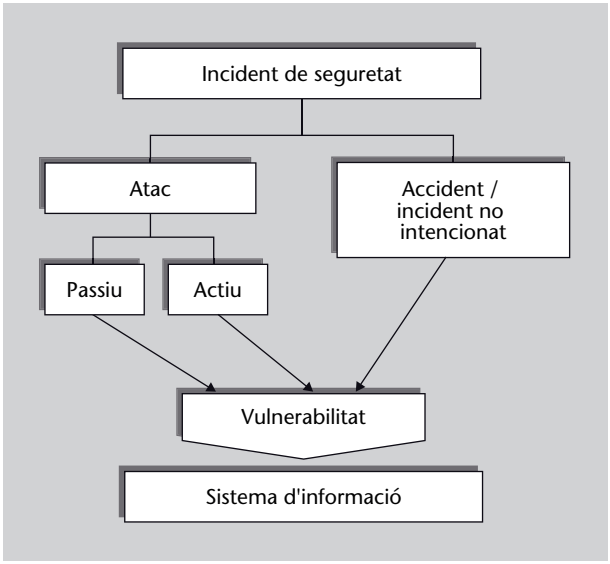
Un **atac** és una agressió a la seguretat d'un sistema fruit d'un acte intencionat i deliberat que viola la política de seguretat d'un sistema.

Un atac pot ser actiu o passiu. Un **atac actiu** intenta alterar el sistema, els seus recursos o operacions. Un **atac passiu** intenta aprendre o utilitzar informació del sistema però no afecta el sistema mateix, ni al seu funcionament. En la figura 1 es mostren els conceptes vistos fins ara.

Un altre aspecte important que tractarem en aquest mòdul és el de risc i amenaça. Tota vulnerabilitat implica una amenaça al sistema i, per tant, comporta un risc.

Una **amenaça** és una violació de la seguretat en potència, que existeix a partir d'unes circumstàncies, capacitat, acció o esdeveniment que pugui arribar a causar una infracció de la seguretat o causar algun dany en el sistema.

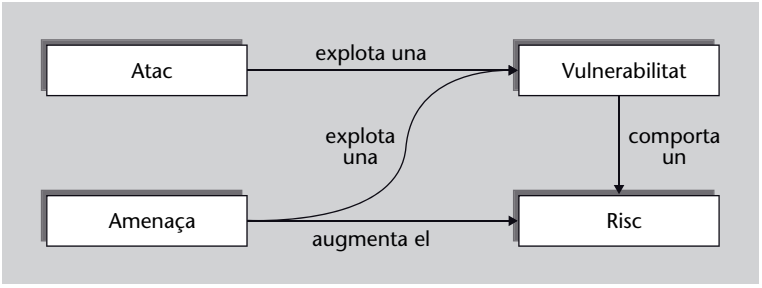
Figura 1. Relació entre conceptes de seguretat



És important distingir entre **atac** i **amenaça**. Un atac és una acció intencionada feta directament o indirectament per un atacant al qual s'atribueix certa capacitat d'acció intel·ligent. Per contra, una amenaça és la possibilitat que ocorri una violació de la política de seguretat. Aquesta violació pot ser provocada per un atac o per incidents no deliberats causats de manera fortuïta, com desastres naturals.

Una part important en la seguretat informàtica és avaluar el risc associat a un servei o sistema. Aquest risc sol ser directament proporcional a l'existència de vulnerabilitats i amenaces. Encara que cal tenir en compte que no sempre com més vulnerabilitats més gran és el risc associat a un sistema. El risc estarà determinat també per la criticitat o gravetat de la vulnerabilitat. En la figura 2 es mostren els principals conceptes vistos fins ara.

Figura 2. Relació entre conceptes de seguretat

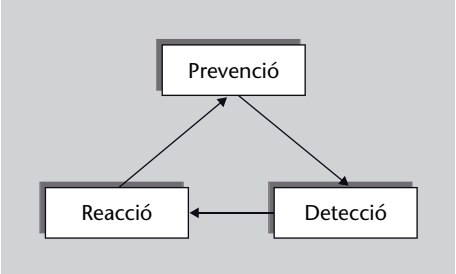


El **risc** és una expectativa de pèrdua expressada com la probabilitat que una amenaça particular exploti una vulnerabilitat particular amb resultats especialment perjudicials.

Una vegada avaluat el risc, considerant les possibles amenaces al sistema, el treball dels experts en seguretat consisteix a desenvolupar contramesures amb

l'objectiu de mitigar aquest risc. És important tenir en compte que, atesa l'actual complexitat dels sistemes informàtics, resulta pràcticament impossible disposar d'un sistema lliure de vulnerabilitats i amenaces. En aquesta línia, el procés de seguretat se sol percebre com un cicle, en què s'apliquen mesures de prevenció, detecció i reacció (podeu veure la figura 3).

Figura 3. Cicle de la seguretat

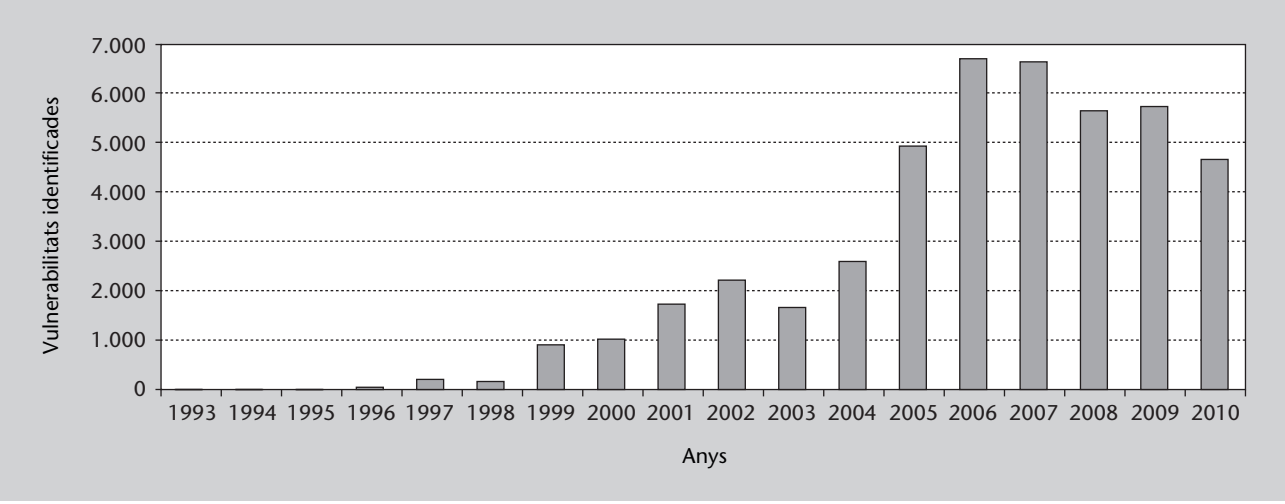


En aquesta assignatura ens centrem en l'origen de la seguretat informàtica en preveure la problemàtica des del punt de vista de les vulnerabilitats. Moltes vegades serà necessari veure els possibles atacs que poden explotar certa vulnerabilitat per a entendre aquesta vulnerabilitat. En aquest sentit, ens centrem en processos de prevenció, en intentar preveure possibles atacs o amenaces al sistema. Poques vegades es detallaran mesures de detecció, com la detecció d'intrusos, o reacció, com a resposta en temps real a atacs, ja que aquests mecanismes s'analitzaran en altres assignatures.

1.1. Exemples de vulnerabilitats

La proliferació de sistemes informàtics i especialment d'Internet ha fet créixer dràsticament el nombre de vulnerabilitats. Estimar el nombre de vulnerabilitats existents és difícil, però hi ha dades, per exemple, del nombre de vulnerabilitats diferents catalogades, com les mostrades en la figura 4. Noteu que no es mostra el nombre de vulnerabilitats, sinó el de vulnerabilitats diferents identificades. El fet que una vulnerabilitat en concret tingui més o menys presència no es mostra en aquest gràfic.

Figura 4. Nombre de vulnerabilitats diferents per any



Font: National Vulnerability Database, http://nvd.nist.gov.

Els següents són alguns exemples de vulnerabilitats:

- **Sony PSN** (*PlayStation Network*): un atac al maig del 2011 a la xarxa d'usuaris PSN de Sony va acabar amb el possible robatori d'informació personal dels seus prop de 70 milions d'usuaris, que incloïa informació de targetes de crèdit. En aquest atac es va explotar una vulnerabilitat coneguda (no s'ha revelat quins sistemes afecta).

- **Stuxnet**: cuc que infecta sistemes industrials i especialment sistemes SCADA (*supervisory control and data acquisition*) de Siemens per a la configuració i el control de processos industrials. Va ser descobert el juliol del 2010 i una particularitat d'aquest cuc és que els seus objectius semblaven molt concrets: centres d'enriquiment d'urani d'Iran. El cuc explota un total de 4 vulnerabilitats del sistema operatiu Windows de Microsoft (2 eren conegudes, i 2 eren vulnerabilitats de *zero-day*).

Lectura complementària

Podeu trobar més informació sobre Stuxnet a: N. Falliere; L. Murchu; E. Chien (2011). W32.Stuxnet Dossier. Symantec Security Response, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Vegeu també

El tipus de vulnerabilitats que explota Stuxnet s'estudien en el mòdul "Vulnerabilitats de baix nivell i programari maliciós".

- **Atac de Mitnick**: el 1994 es va produir un dels atacs informàtics més publicitats i documentats, mitjançant el qual un intrús informàtic anomenat Kevin Mitnick va aconseguir accedir als ordinadors de Tsutomu Shimomura, situats a la Universitat de Califòrnia, per robar el codi font d'un telèfon mòbil. Mitnick va explotar vulnerabilitats en el protocol TCP de denegació de servei i de segrest de sessió.

Vegeu també

En el mòdul "Vulnerabilitats en xarxes" s'estudien el tipus de vulnerabilitats que va explotar Kevin Mitnick.

Lectura complementària

Podeu trobar més informació sobre el cas Mitnick-Shimomura en els llibres:

T. Shimomura; J. Markoff (1996). *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw-By the Man Who Did It*. Hyperion Books.

J. Littman (1997). *The Fugitive Game: Online with Kevin Mitnick*. Little, Brown and Company publishers.

J. Goodell (1996). *The Cyberthief and the Samurai: The True Story of Kevin Mitnick-And the Man Who Hunted Him Down*. Dell publishers.

Hi ha maneres de poder identificar i classificar vulnerabilitats, que es poden fer públiques perquè tothom pugui aplicar mesures preventives. Molts problemes de seguretat vénen per no tenir els sistemes informàtics actualitzats amb els últims pegats de seguretat que eviten vulnerabilitats conegudes. Així i tot, sempre hem d'assumir que hi ha vulnerabilitats no conegudes i que poden donar lloc a incidents de seguretat. Aquestes vulnerabilitats no conegudes, de les quals és molt difícil protegir-se, es denominen *vulnerabilitats de dia zero*, o en anglès, *zero-day vulnerabilities*.

Vegeu també

En l'apartat 2 d'aquest mòdul presentarem una classificació de les vulnerabilitats.

Així mateix, també veiem que molts atacs informàtics exploten més d'una vulnerabilitat. Això és especialment latent en atacs que fan diverses accions diferents. Un exemple clar en què s'exploten diverses vulnerabilitats són les xarxes de zombis.

Vegeu també

Les xarxes de zombis s'estudien en el mòdul "Botnets".

2. Gestió de vulnerabilitats

Un procés molt important dins de la seguretat informàtica avui dia és la gestió de vulnerabilitats. Dins de la seguretat preventiva, un dels punts clau és trobar vulnerabilitats en sistemes existents que puguin representar una amenaça davant atacs potencials. A aquest efecte es destinen molts recursos a diferents nivells, des dels fabricants mateixos de maquinari i programari, fins a entitats governamentals o associacions altruistes.

Els equips encarregats de la gestió de vulnerabilitats i incidents de seguretat solen rebre el nom de CERT (*computer emergency response team*) o CSIRT (*computer security incident response team*). La principal tasca d'aquests equips és la gestió d'incidències de seguretat. En la pràctica, serveixen com a mitjà per a la difusió de vulnerabilitats de seguretat a usuaris (particulars o organitzacions), que solen ser reportades pels usuaris mateixos.

El primer centre de coordinació CERT va ser creat el 1988, per DARPA (*Defense Advanced Research Projects Agency*), en l'Institut d'Enginyeria del Programari (*Software Engineering Institute*, SEI) de la Carnegie Mellon University als Estats Units, i actualment continua essent una referència internacional. La necessitat de crear aquest centre va ser impulsada pel gran impacte que va tenir el cuc Morris. L'aparició d'Internet feia possible la ràpida distribució de codi maliciós, i donar lloc a l'aparició de virus, cucs*, etc. Com a resposta a aquesta problemàtica es van crear aquests equips CERT, que ràpidament s'han estès per tot el món. Actualment, el CERT original de la Carnegie Mellon University es coneix com a CERT/CC (CERT Coordination Center), ja que actua com a coordinador i dóna suport a equips CERT (o CSIRT) de nivell nacional (generalment governamentals) a tot el món. En la taula 1 es mostren alguns dels principals CERT en territori espanyol, incloent-hi la seva URL, l'any de creació i l'àmbit d'aplicació.

*En anglès, *worm*

Morris Worm

El cuc Morris va ser un dels primers virus que es van distribuir per Internet. Va ser creat per Robert Morris, un estudiant de la Cornell University, i distribuït des del MIT (*Massachusetts Institute of Technology*) el 1988. Es propagava explotant diferents vulnerabilitats del sistema operatiu UNIX. Encara que no hi ha dades fiables, es va estimar que va arribar a infectar aproximadament un 10% de les màquines que en aquella època estaven connectades a Internet.

La proliferació d'equips CERT pel món ha fet necessari establir una certa coordinació entre aquests. A part de CERT/CC, hi ha centres de coordinació d'equips CERT a escala internacional, com FIRST (*forum of incident response and security teams*), TF-CSIRT (*computer security incident response teams task force*) en l'àmbit europeu, o CSIRT.es (equips de seguretat i atenció a incidents) en l'espanyol.

Els equips CERT disposen de bases de dades i canals de distribució (com llistes de correu) per a distribuir informació relativa a vulnerabilitats. La seva tasca principal és recollir informació sobre vulnerabilitats, classificar-les i publicar-ne l'existència, i també possibles mesures per a mitigar-les. La informació la so-

Taula 1. Principals equips CERT en territori espanyol

esCERT UPC	Universitat Politècnica de Catalunya	
	http://escert.upc.edu/	1994
	Universitats i PIME catalanes	
IRIS-CERT	RedIris (Red.es, Ministeri d'Indústria, Turisme i Comerç)	
	http://www.rediris.es/cert/	1997
	Universitats	
S21sec CERT	Grup S21sec Gestió SA.	
	http://www.csirtcv.gva.es/	2000
	Clients i ciutadans	
CCN-CERT	Centre Criptogràfic Nacional (Centre Nacional d'Intel·ligència, Ministeri de Defensa)	
	https://www.ccn-cert.cni.es/	2006
	Administració pública (general, autonòmica i local)	
INTECO CERT	Institut Nacional de Tecnologies de la Comunicació (Ministeri d'Indústria, Turisme i Comerç)	
	http://cert.inteco.es/	2007
	PIME i ciutadans	
CSIRT-CV	Centre Seguretat TIC del País Valencià	
	http://www.csirtcv.gva.es/	2007
	Ciutadans, PIME i Administració pública del País Valencià	
CESICAT	Centre de Seguretat de la Informació de Catalunya (Generalitat de Catalunya)	
	http://www.cesicat.cat/	2010
	Ciutadans, PIME, universitats/centres d'investigació i Administració pública a Catalunya	

len subministrar fabricants, organitzacions o usuaris directament a un CERT, que després sol distribuir informació a altres equips CERT amb els quals estigui coordinat. Així mateix, la distribució pot ser directa i oberta al públic, restringida a organitzacions concretes, o a subscriptors. Com recullen i distribueixen informació els CERT depèn molt del tipus de CERT i el seu àmbit d'aplicació. En general, es considera una bona pràctica difondre informació de vulnerabilitats de manera oberta i gratuïta a tota la comunitat d'usuaris d'Internet amb l'objectiu de millorar la seguretat general de la Xarxa. Per això, la major part dels CERT importants distribueixen aquesta informació lliurement.

Exemple de publicació de vulnerabilitat

En la taula 2 podem veure una vulnerabilitat real reportada per CCN-CERT sobre l'aplicació Powerpoint de Microsoft. La publicació d'aquesta vulnerabilitat inclou informació que pot ser d'utilitat a usuaris o organitzacions. Aquest és un format típic usat per la majoria dels CERT. Perquè una vulnerabilitat sigui admesa en una BD d'un CERT, generalment passa per un procés de verificació. Aquest procés és complex i important, ja que entre altres coses s'encarrega de classificar i etiquetar de manera única la vulnerabilitat. Aquesta identificació única (en el cas de la taula 2 és CVE-2011-1269, i CVE-2011-1270) permet evitar duplicats i coordinar accions entre diferents CERT. En el subapartat 2.2. veurem com s'etiqueten aquestes vulnerabilitats.

2.1. Sobre la lliure publicació de vulnerabilitats

A l'hora de decidir si es fa o no pública una vulnerabilitat, es planteja un dilema que sol implicar una polèmica important. D'una banda, hi ha els partidaris

Taula 2

Múltiples vulnerabilitats en el Microsoft PowerPoint	
Classificació de la vulnerabilitat	
Risc	mitjà
Nivell de confiança	Oficial
Impacte	Obtenir accés
Dificultat	Expert
Requisits de l'atacant	Accés remot sense compte a un servei estàndard
Informació sobre el sistema	
Plataforma afectada	Microsoft
Programari afectat	Microsoft Office 2003 SP3
	Microsoft Office XP SP3
	Microsoft Office 2007 SP2
	Microsoft Office 2004 per a MacOS
	Microsoft Office 2008 per a MacOS
	Open XML File Format Converter per a MacOS
Descripció	
S'han descobert múltiples vulnerabilitats en el Microsoft PowerPoint de Windows i MacOS. Les vulnerabilitats són descrites a continuació:	
- CVE-2011-1269: s'ha descobert una vulnerabilitat en el PowerPoint. La vulnerabilitat consisteix en un error en la manera com tracta els arxius. Un atacant remot podria obtenir accés o executar codi arbitrari mitjançant un arxiu de PowerPoint especialment manipulat.	
- CVE-2011-1270: S'ha descobert una vulnerabilitat en el PowerPoint. La vulnerabilitat consisteix en un error en la manera com tracta els arxius. Un atacant remot podria obtenir accés o executar codi arbitrari mitjançant un arxiu de PowerPoint especialment manipulat.	
El butlletí MS11-036 substitueix el MS11-022	
Solució	
Actualització de programari	
Microsoft (MS11-036)	
Vegeu la taula d'actualitzacions a: http://www.microsoft.com/technet/security/bulletin/MS11-036.mspx	
Identificadors estàndard	
CVE	CVE-2011-1269
	CVE-2011-1270
BID	NULL
Recursos addicionals	
Microsoft Security Bulletin (MS11-036): http://www.microsoft.com/technet/security/bulletin/MS11-036.mspx	
Historial de versions	
Versió	Data
1.0	2011-05-11

Font: CCN-CERT

de publicar lliurement una vulnerabilitat una vegada és coneguda; d'aquesta manera, tothom pot en conèixer l'existència i aplicar les mesures preventives adequades. D'altra banda, hi ha gent que pensa que fer pública informació relativa a vulnerabilitats equival a donar armes a l'enemic, ja que moltes vegades són vulnerabilitats conegudes (no corregides) les que s'utilitzen en atacs informàtics.

En el camp de la seguretat informàtica, en general, es considera com a bona pràctica oferir la major claredat possible sobre problemes i mecanismes de seguretat, i no basar la seguretat d'un sistema en l'ocultació d'informació. És a dir, un atacant el primer que fa en voler atacar un sistema concret és recollir informació sobre aquest sistema: sistema operatiu, programari que utilitza,

etc., i després busca vulnerabilitats que puguin ser explotades en aquest sistema. Intentar ocultar informació sobre el sistema per impedir que l'atacant hi pugui buscar vulnerabilitats és una cosa comuna. No obstant això, aquesta és una pràctica de dubtosa eficàcia i pot arribar a donar una falsa sensació de seguretat. Per això, molts experts advoquen per assumir que el possible atacant disposa d'aquesta informació i, per tant, no és necessari ocultar-la. Aquesta idea pren el seu inici en el principi de Kerckhoff (1835-1903) sobre els criptosistemes.

Principi de Kerckhoff

Els criptosistemes "no han de ser necessàriament secrets, i han de poder caure en mans de l'enemic sense que això comporti cap inconvenient".

A. Kerckhoffs (1883). "La cryptographie militaire". *Journal des sciences militaires* (vol. IX, pàg. 5-83, gener, pàg. 161-191, febrer).

Aquesta idea que el mètode o sistema no ha de ser secret s'estén avui dia per a la majoria dels sistemes d'informació, i molts experts advoquen per la lliure publicació de vulnerabilitats.

Seguint aquests principis, la majoria dels CERT adopten un compromís en la publicació de vulnerabilitats. En general, advoquen per la lliure publicació. No obstant això, solen informar als fabricadors dies abans de l'aparició de la vulnerabilitat en la seva web perquè aquests puguin desenvolupar mesures preventives o pegats de seguretat.

Vulnerabilitats publicades pel CERT/CC

El CERT/CC actualment fa pública qualsevol vulnerabilitat que li sigui reportada en 45 dies, independentment de l'existència de pegats o solucions per part dels fabricants. Durant aquests 45 dies, el CERT/CC notifica al fabricant del producte en què s'ha trobat la vulnerabilitat. La independència d'aquests equips CERT possibilita que puguin evitar pressions per part de fabricants en la publicació de vulnerabilitats dels seus productes.

2.2. Etiquetatge i identificació de vulnerabilitats

Per a poder identificar vulnerabilitats, hi ha identificadors únics que impedeixen que es publiquin duplicats i faciliten la possibilitat de fer referència a vulnerabilitats concretes. El sistema d'identificació més important a escala internacional és el CVE (*common vulnerabilities and exposures*). El CVE es presenta com un estàndard de noms de vulnerabilitats de seguretat informàtica d'ús gratuït i públic. S'autodefineix com un diccionari de vulnerabilitats (no com una base de dades), on qualsevol pot buscar el nom (identificador) que rep una vulnerabilitat concreta.

Per a etiquetar una vulnerabilitat en el CVE, se segueix el procediment següent:

1) Es descobreix una vulnerabilitat.

2) Se li assigna un identificador CVE amb l'estat *candidat*. Aquesta assignació la fa un *CVE candidate numbering authority* (CNA), que són els principals fabricants de programari i maquinari, i també organitzacions i empreses del sector, autoritzats pel CVE.

3) La vulnerabilitat es publica a la pàgina web del CVE i se'n proposa al consell editor del CVE l'aprovació.

4) El consell editor decideix mitjançant votació si accepta la vulnerabilitat, amb la qual cosa passa a estat *entry* i s'afegeix a la llista de CVE, o si per contra es desestima.

La importància del CVE està determinada per la gran adopció a escala internacional. La majoria dels equips CERT, fabricadors de programari i maquinari, desenvolupadors de sistemes operatius i organitzacions, i també productes destinats a la seguretat informàtica, utilitzen els identificadors CVE.

Gestió del CVE

Actualment, el CVE està gestionat per *The Mitre Corporation*, empresa nord-americana que actua com a líder del consell editor. Cal destacar també que el CVE està actualment patrocinat pel *US Department of Homeland Security*.

El consell editor de CVE ha de decidir entre altres coses què es considera com a vulnerabilitat. Per a això, utilitza una definició pròpia.

Segons el CVE, una vulnerabilitat és un estat d'un sistema informàtic (o conjunt de sistemes) que compleix algun dels casos següents:

- Permet a un atacant executar ordres com un altre usuari.
- Permet a un atacant accedir a dades violant les restriccions de control d'accés específiques per a aquestes dades.
- Permet a un atacant suplantar una altra entitat.
- Permet a un atacant dur a terme una denegació de servei.

Com es pot veure, la definició de vulnerabilitat de CVE és bastant més restrictiva i específica que la definició genèrica que hem adoptat en l'apartat 1. Això és així per poder restringir una mica l'aplicabilitat del CVE, ja que d'una altra manera resultaria molt difícil poder incorporar totes les vulnerabilitats. Cal tenir en compte també que el CVE neix i es gestiona sota el patrocini d'agències d'espionatge i defensa la principal preocupació de les quals és la defensa davant atacants (per això la insistència en l'atacant en la definició).

BugTraq

A part del CVE, hi ha altres esquemes d'identificació de vulnerabilitats. Cal destacar BID (BugTraq ID), que és un identificador assignat per la llista BugTraq. BugTraq és una llista de correu electrònic sobre seguretat informàtica creada el 1993. El seu objectiu (entre altres) era facilitar la difusió de vulnerabilitats lliurement (sense necessitat de sol·licitar permís al fabricant). Encara que va ser molt popular, ha anat perdent importància especialment després que va ser adquirida per l'empresa SecurityFocus, que al seu torn va ser absorbida per Symantec.

2.3. Bases de dades de vulnerabilitats

Encara que, com s'ha comentat anteriorment, la majoria dels equips CERT ofereixen bases de dades de vulnerabilitats, hi ha algunes bases de dades a les quals els CERT solen fer referència. Entre aquestes, destaquem:

- **The Open Source Vulnerability Database (OSVD)**. Base de dades de codi obert creada de manera independent, que està gestionada per l'organització sense ànim de lucre *Open Security Foundation*.

OSVD: http://osvdb.org/

- **National Vulnerability Database (NVD)**. Base de dades pertanyent al govern dels EUA d'accés públic.

NVD: http://nvd.nist.gov/

- **SecurityFocus Vulnerability Database**. Base de dades mantinguda per l'empresa Symantec. Aquesta empresa també disposa de la llista de distribució *BugTraq*, que va arribar a ser el principal canal de difusió de vulnerabilitats en els anys noranta.

SecurityFocus Vulnerability Database: http://www.securityfocus.com/bid

- **Exploit DB**. Base de dades de vulnerabilitats que té la particularitat que, a més de publicar les vulnerabilitats, publica els *exploits* corresponents (per això el seu nom). Aquests són programes o *scripts* que permeten explotar aquesta vulnerabilitat, és a dir, programes que permeten fer un atac que s'aprofiti de la vulnerabilitat. Encara que serveixen com a prova de concepte i per a provar sistemes, el seu ús maliciós potencial és el motiu pel qual la resta de les bases de dades i CERT no publiquen *exploits*.

Exploit DB: http://www.exploit-db.com/

A part d'aquestes bases de dades genèriques, tots els fabricants d'aplicacions, sistemes operatius (incloent les organitzacions que distribueixen sistemes operatius de codi lliure), o maquinari, solen tenir bases de dades on troben classificades vulnerabilitats relacionades amb els seus productes, sistemes o serveis.

2.4. Avaluació de vulnerabilitats

En l'exemple de la taula 2 es pot observar que a la vulnerabilitat se li atribueix un nivell de risc, dificultat o impacte. El fet de poder donar aquest nivell de risc és important, ja que permet avaluar quines vulnerabilitats són potencialment més perilloses i, per tant, més urgents. Això també es té en compte a l'hora de fer una estimació del risc del sistema. De totes maneres, és difícil establir una mètrica comuna per a avaluar la criticitat de vulnerabilitats.

En aquesta línia, el sistema d'avaluació més estès es coneix com a CVSS (*Common Vulnerability Scoring System*). CVSS és un intent d'estandarditzar un mètrica comuna per a avaluar vulnerabilitats. La idea és obtenir un nombre (o conjunt de nombres) que ens donin una idea del perill potencial que representa una vulnerabilitat.

CVSS distingeix entre tres mètriques bàsiques:

- **Mètrica base**, aspectes de la vulnerabilitat constants en el temps i entorn descrits en la taula 3. Aquestes mètriques proporcionen un valor entre 0 i 10 que determina la gravetat de la vulnerabilitat. Aquesta s'etiqueta

com a *low* (valor en [0.0,3.9]), *medium* (valor en [4.0,6.9]) o *high* (valor en [7.0,10.0]). La mètrica base també s'expressa com a vector:

`AV:[L,A,N]/AC:[H,M,L]/Au:[M,S,N]/C:[N,P,C]/I:[N,P,C]/A:[N,P,C].`

Taula 3. Mètrica base de CVSS

Vector d'accés (AV)	Com s'explota la vulnerabilitat. Pot ser localment (L), des d'una xarxa adjacent (A) o des de qualsevol xarxa (N).
Complexitat d'accés (AC)	Complexitat que requereix l'atacant una vegada ha accedit al sistema. Aquesta pot ser alta (H), mitjana (M) o baixa (L).
Autenticació (Au)	Nombre de vegades que l'atacant s'ha d'autenticar contra un sistema. Poden ser múltiples (M), una (S) o cap (N).
Impacte de confidencialitat (C), integritat (I) i disponibilitat (A)	Tres indicadors sobre l'impacte que pot tenir la vulnerabilitat en la confidencialitat, integritat i disponibilitat del sistema. Per a cadascun els valors pot ser: cap (N), parcial (M) o complet (C).

Exemple

La vulnerabilitat CVE-2002-0392 de la taula 4 té un vector base:

`AV:N/AC:L/Au:N/C:N/I:N/A:C`

És a dir, vector d'accés: *network*, des de qualsevol xarxa (AV:N); complexitat d'accés: baixa (AC:L); autenticació: cap (Au:N); confidencialitat: cap (C:N); integritat: cap (I:N), i disponibilitat: complet (A:C). Aquest vector ja ens dóna molta informació de la vulnerabilitat. Aquesta és una vulnerabilitat que es pot explotar des de qualsevol xarxa, que té impacte sobre la disponibilitat (possiblement mitjançant un atac de denegació de servei), és fàcil d'explotar i sense necessitat d'autenticar-se.

Taula 4. Mètrica base de CVSS

Vulnerabilitat		Puntuacions CVSS		
		Base	Temporal	Entorn
CVE-2002-0392	Apache Chunked-Encoding Memory Corruption Vulnerability	**7,8**	6,4	0,0-9,2
CVE-2003-0818	Microsoft Windows ASN.1 Library Integer Handling Vulnerability	**10,0**	8,3	0,0-9,0
CVE-2003-0062	Buffer Overflow in NOD32 Antivirus	**6,2**	4,9	0,0-7,5

Càlcul de CVSS

Hi ha aplicacions que faciliten el càlcul de la puntuació CVSS, com les següents:

- NIST CVSSv2 Calculator (http://nvd.nist.gov cvss.cfm)
- IPA, Japan (http://jvnrss .ise.chuo-o.ac.jp/jtg/cvss /en/CVSSv2.html)

- **Mètrica temporal**, mètriques que poden canviar en el temps. Són opcionals i no s'utilitzen per a obtenir la mètrica final. Comprenen l'explotabilitat (existència d'*exploits* i el grau de disponibilitat), nivell de curació o *remediation level* (existència de solucions i si són definitives o temporals) i la confiança de l'anunci (fins a quin nivell s'ha confirmat l'existència de la vulnerabilitat). La mètrica temporal es combina amb la base per a donar un valor entre 0 i 10.

- **Mètriques de l'entorn**, mètriques relatives a l'entorn del sistema informàtic pròpiament dit, que inclou el risc que pot representar a una organització o a persones individuals. Aquí es preveu el *dany col·lateral potencial*, que mesura el dany que pot ocasionar a tercers l'explotació d'aquesta vulnerabilitat (dany a persones, a béns físics, a la productivitat o als beneficis). També s'inclou la distribució d'objectius o *target distribution*, que mesura la proporció de sistemes vulnerables en l'entorn. Aquestes mètriques donen un valor entre 0 i 10, que generalment s'expressa com a interval mínim-màxim.

A partir de totes aquestes mètriques, CVSS proporciona un valor numèric o puntuació general sobre la vulnerabilitat. En la taula 4 veiem algun exemple de puntuacions CVSS per a 3 vulnerabilitats concretes. La puntuació que se sol utilitzar més és la de mètriques base; en aquest cas ens dóna uns valors que classificarien les dues primeres vulnerabilitats amb un nivell de criticitat alt (*high*) i l'última amb un nivell mitjà (*medium*).

3. Classificació de vulnerabilitats

Hi ha diverses classificacions de vulnerabilitats i cap no preval sobre la resta. El fet d'adoptar una classificació o una altra està moltes vegades condicionat pel propòsit d'aquesta classificació. En el nostre cas, i amb l'objectiu de proporcionar una visió global de la seguretat informàtica, hem adoptat una classificació que es basa en el tipus de sistema el qual afecta la vulnerabilitat. D'aquesta manera, distingim entre els següents:

- **Vulnerabilitats de baix nivell i programari maliciós**. Aquí entren vulnerabilitats que afecten el sistema operatiu i aplicacions a baix nivell propiciades generalment per errors en la programació, com desbordaments de memòria intermèdia o *race conditions*. També s'inclou en aquest tipus de vulnerabilitats l'estudi de programari maliciós, com virus o cucs que exploten aquest tipus de vulnerabilitats.

- **Vulnerabilitats de xarxa**. Són vulnerabilitats que afecten programari i components de xarxa o interconnexió de xarxes. Aquestes vulnerabilitats poden ser des de xarxes locals a Internet. Principalment, s'observen vulnerabilitats en els diferents protocols de xarxa, i també vulnerabilitats derivades de l'anàlisi de trànsit.

- **Vulnerabilitats en aplicacions web**. La importància d'Internet i les aplicacions web, des del comerç electrònic, les xarxes socials, o el que actualment es denomina informàtica en el núvol, provoca que aquestes aplicacions mereixin un apartat propi. Aquestes són vulnerabilitats pròpies d'aplicacions pensades per a ser ofertes mitjançant una interfície web i a les quals generalment tenen accés un gran nombre d'usuaris. En general, es consideren vulnerabilitats de més alt nivell que les del primer apartat, i inclouen *cross-site scripting*, injecció de codi, etc.

- **Vulnerabilitats d'enginyeria social**. Aquest apartat concentra les vulnerabilitats associades als usuaris dels sistemes informàtics. Tenen més relació amb l'aspecte psicològic d'aquests usuaris que amb problemes purament tècnics. Exemples típics són el correu brossa, la pesca (o *phising*), etc.

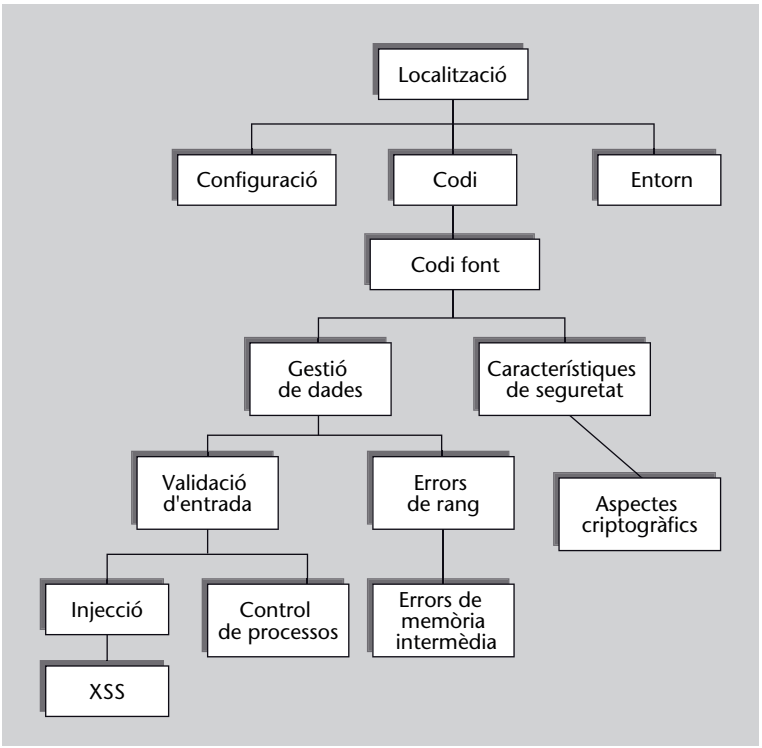
Una altra classificació possible de les vulnerabilitats es basa en la identificació del servei que afecten. D'aquesta manera, si prenem la classificació que tradicionalment s'aplica als serveis de seguretat (confidencialitat, integritat i disponibilitat), tenim vulnerabilitats que comporten:

- Pèrdua d'integritat.
- Pèrdua de confidencialitat.
- Pèrdua de disponibilitat.

En aquest cas, la classificació està orientada a identificar què poden permetre fer aquestes vulnerabilitats a un possible atacant. Per exemple, una vulnerabilitat que permeti una denegació de servei és manifestament una vulnerabilitat de disponibilitat, i també vulnerabilitats que permetin espiar comunicacions ho són de confidencialitat. Aquest és un dels criteris que expressa directament la mètrica base de CVSS vista en el subapartat 2.4..

Seguint la classificació anterior basada en serveis, trobem una possible extensió. El CWE (*common weakness enumeration specification*) proporciona una enumeració jeràrquica de tipus de vulnerabilitats orientades a programari. La classificació del CWE és molt detallada i permet fixar nombrosos nivells d'abstracció (segons es va baixant per la jerarquia); com a exemple mostrem una petita part d'aquesta classificació relativa a la localització de la vulnerabilitat en la figura 5.

Figura 5. Estructura parcial de CWE



En general, hi ha moltes maneres de classificar vulnerabilitats; per exemple, qualsevol dels criteris i mètriques que hem comentat en el subapartat 2.4. poden servir per a classificar vulnerabilitats.

Resum

En aquest mòdul hem introduït el concepte de vulnerabilitat pel que fa a sistema d'informació. Com hem pogut veure, les vulnerabilitats són de vital importància en qualsevol procés de seguretat, ja que una vulnerabilitat es pot veure com el primer graó del procés de seguretat. Aquesta importància ha quedat manifesta amb l'enumeració d'alguns exemples cèlebres d'atacs que explotaven vulnerabilitats concretes.

La definició mateixa de vulnerabilitat ens ha portat a definir conceptes molt relacionats, com els atacs i les amenaces. Encara que poden semblar el mateix, la distinció es fa necessària per a una comprensió correcta de cada concepte i la relació amb el risc que implica cadascun.

Posteriorment, hem analitzat com es fa la gestió de les vulnerabilitats, que, per a més efectivitat, necessita la coordinació de diferents centres a escala mundial. Hem identificat els centres més rellevants internacionals i nacionals posant l'accent en els mecanismes d'identificació, classificació i avaluació de vulnerabilitats en funció de la seva criticitat.

Finalment, hem donat algunes possibles classificacions que permeten agrupar les vulnerabilitats a partir de les seves característiques. A partir de les classificacions descrites es fonamentaran cadascun dels mòduls de l'assignatura.

Activitats

1. Busqueu per Internet algun atac informàtic recent del qual hàgiu tingut notícia. En aquest atac identifiqueu la vulnerabilitat o vulnerabilitats explotades i classifiqueu-les segons el que s'ha vist en l'apartat 3.

2. Busqueu la vulnerabilitat CVE-1999-0508 en diverses bases de dades de vulnerabilitats. Expliqueu breument en què consisteix aquesta vulnerabilitat i comenteu l'avaluació de la vulnerabilitat utilitzant els CVSS que donen les bases de dades i els seus possibles impacte, classificació i solució.

3. Busqueu una vulnerabilitat recent en alguna base de dades de vulnerabilitats i descriviu aproximadament com obtindríeu els valors CVSS a partir de les característiques de la vulnerabilitat. Finalment, utilitzeu alguna de les calculadores CVSS; per exemple, la que teniu disponible a http://nvd.nist.gov/cvss.cfm?calculator&version=2, per a obtenir els valors CVSS.

Glossari

amenaça *f* Violació de la seguretat en potència, que existeix en funció d'unes circumstàncies, capacitat, acció o esdeveniment que pugui arribar a causar una infracció de la seguretat o algun dany en el sistema.

atac *m* Agressió a la seguretat d'un sistema fruit d'un acte intencionat i deliberat que viola la política de seguretat d'un sistema.

common vulnerabilities and exposures *m* Estàndard públic per a la identificació de vulnerabilitats. Associa un identificador únic a cada vulnerabilitat diferent.
Sigla **CVE**

common vulnerability scoring system *m* Marc comú per a l'avaluació de la criticitat de vulnerabilitats.
Sigla **CVSS**

computer emergency response team *m* Equip de respostes a emergències informàtiques. Una de les seves tasques principals consisteix en la gestió de vulnerabilitats.
Sigla **CERT**

computer security incident response team *m* Equip de resposta a incidents de seguretat informàtica. Una de les seves tasques principals consisteix en la gestió de vulnerabilitats.
Sigla **CSIRT**

eina d'intrusió *f* Programa que permet accés privilegiat a un ordinador i n'aconsegueix ocultar la presència a l'administrador. Sol fer ús de diverses vulnerabilitats per a instal·lar-se i aconseguir el seu propòsit.

exploit *m* Programa o *script* que permet explotar una o diverses vulnerabilitats, és a dir, un programa que permet fer un atac aprofitant la vulnerabilitat.

política de seguretat *f* Conjunt de regles i pràctiques que defineixen i regulen els serveis de seguretat d'una organització o sistema amb el propòsit de protegir els seus recursos crítics i sensibles. En altres paraules, és la declaració del que està permès i el que no està permès fer.

risc *m* Expectativa de pèrdua expressada com la probabilitat que una amenaça particular exploti una vulnerabilitat concreta amb resultats especialment perjudicials.

vulnerabilitat de dia zero *f* Vulnerabilitat de l'existència de la qual, en el moment de ser explotada, no es té coneixement previ.
en zero-day vulnerability

vulnerabilitat de seguretat *f* Errada o debilitat en el disseny, la implementació, l'operació o la gestió d'un sistema, que pot ser explotada amb la finalitat de violar la política de seguretat del sistema.

Bibliografia

Bishop, M. (2002). *Computer Security: Art and Science*. Boston: Addison Wesley.

Mell, P.; Scarfone, K.; Romanosky, S. (2007). *A Complete Guide to the Common Vulnerability Scoring System Version 2.0* [article en línia] <http://www.first.org/cvss/cvss-guide.html>.

Shirey, R. (2000). *Internet Security Glossary*. RFC 2828, IETF.