—Euskarazko alea (*)—

Aurrera !

Informatika eta Telekomunikazioetako Teknologia Berriak Jendarteratzeko Aldizkaria

ITZko Bulego Teknologikoak argitaratua

2. zk.

2000ko abendua

Bidali zuen iradokizunak helbide honetara: aurrera@ej-gv.es

Aurkibidea

ESKERRIK ASKO!

AURRERA! Dibulgazioko Buletinaren bigarren zenbakia dugu hau eta eskerrak eman nahi dizkiegu irakurleei lehen zenbakiak izandako harrera eta onarpena dela eta. Era berean, **Industria Sailari** ere eskertu nahi diogu lehen aleko **"ALBOAN"** atalean lagundu izana.

Gogoratzen dizuet, **"ALBOAN"** atala eskura duzuela, Eusko Jaurlaritzako gainerako sailei zuen proiektuen, ideien, etab.en berri eman ahal izan diezaiezuen. Horrela, bada, animatu egiten ditugu gainerako sailak ekarpenak egitera, eta eskerrak ematen dizkiegu bigarren ale honetan lagundu diguten guztiei.

Bestalde, aditzera eman nahi dizuegu bigarren ale honetan **"GALDERAK"** izeneko atal berria ireki dugula, teknologia berriekin zerikusia duten gaiei buruz egiten dizkiguten galderei erantzuteko asmotan.

Buletinean interesa duzuenok, ez baduzue zuzenean postontzian edo paperean jasotzen, jakin ezazue Eusko Jaurlaritzako **Intranet-ean** kontsulta dezakezuela. Horretarako, '**Jakina-ra**' jo behar duzue eta '**Informatika eta Telekomunikazioak**' atalean sartu.

Azkenik, eta data kontuan hartuta, aukera hau baliatzen dugu milurteko berri ona opatzeko:

ZORIONAK eta URTE BERRI ON !!

(*) Erderazko eta Euskarazko aleak eskuragarri dituzu "Jakina" web orrian.

BLUETOOTH TEKNOLOGIA

Bluetooth teknologia konexioen merkatuan iraultzaile izan dadila espero da, izan ere, hari gabeko konexioak ahalbidetzen ditu, eta horrek abantaila ugari dakartza.

Zehaztapen honi esker, kostu txikiko irrati-motako loturak egin ahal izango dira gailuen artean, besteak beste, ordenagailu eramangarrien, telefono mugikorren eta bestelako zenbait eramangarriren artean. Gainera, gailu horiek guztiak irrati bidez Internetera konektatuta egon ahal izango dira.

HISTORIA

Bluetooth Harald deituriko errege bikingoaren izenetik dator, errege horrek geroago hartu zuen Blatand izenetik. Gaitzizena Danimarkako bi hitz zaharrek osatua da, "bla" (azal ilunekoa), alde batetik, eta "tan" (gizon handia), bestetik, eta ingelesek, fonetikoki beren hizkuntzara egokitzean, "Bluetooth" ahoskatu zuten.

Haraldek, txikitatik, gizarte bikingoa osatzen zuten familia-loturak errespetatzen eta ezezagunengandik ezkutatzen ikasi zuen. Filosofia horrengatik, hain zuzen ere, jarri zitzaion haren izena teknologia berri honi.

Eusko Jaurlaritzako Wap-a ikusi nahi baduzu, honako hau tekleatu besterik ez duzu:

euskadi.net (mugikorrarekin)

wap.euskadi.net (mugikorraren emuladorea PCan)

BLUETOOTH

Ikuspegi orokorra

Bluetooth teknologiari esker, 100 metrora arteko konexioak egin daitezke (10 metrokoak anplifikatzailerik gabe), bat-batean, hainbat gailuren artean, telefono mugikorren, agenden eta mahai gaineko PCen artean, esaterako. Eta hori guztia kablerik erabili gabe.

Komunikazioak irrati-transmisio bidez egiten dira, eta, ondorioz, datuen eta ahotsen transferentzia denbora errealean izaten da.

Bluetooth teknologiaren bidez garatutako transmisio-modu sofistikatuak interferentziekiko babesa eta transmititutako datuen segurtasuna bermatzen ditu.

Bluetooth-eko irrati-sistema mikrotxip txiki batean dago eta mundu guztian har daitekeen 2,4 GHz frekuentzia-bandan egiten du lan.

Zehaztapenean bi maila bereiz daitezke:

- Maila txikia: Distantzia txikiak hartzen ditu, gela batekoa, adibidez.
- Maila handia: Distantzia ertainak hartzen ditu, etxe batekoa, esaterako.

Software-ak mikrotxip bakoitzean sortutako kodea kontrolatzen eta identifikatzen du, eta komunikazioa soilik aurretiaz programatutako unitateen artean izan dadila bermatzen du.

Bluetooth hari gabeko teknologiari esker, komunikazioak puntutik puntura eta puntutik puntu anitzera izan daitezke. Gaur egungo zehaztapena baliatuz, irrati-gailu maisu batekin 7 gailu morroi konektatzea lortu da. Multzo horri "**piconet**" deritzo. Piconet horietako asko ad hoc (behin-behinean) lot daitezke, konfigurazio ezberdinen arteko komunikazioa lortu ahal izateko.

ZUZENKETAK

XML/HTTP eta JAVA RMI/IIOP alderatzeko taulan, 1 zk.ko Buletineko 1. argitaraldiko 10. orrialdean, Javari buruz "Objektuetara ez bideratua" zioen, eta, aldiz, "Objektuetara bideratua" behar zuen.

Egin daitezkeen aplikazioak

•**Internetera zubia:** Bluetooth teknologiarekin, zauden lekuan zaudela, "munduarekin" konektatu ahal izango zara. Horrela, bada, ordenagailu eramangarria izanez gero, edozein lekutan nabigatu ahal izango duzu Interneten, bai telefono mugikor batekin konektatuta bazaude (teknologia zelularra) eta bai hari bidez konektatuta bazaude (ad.: ISDN[1], PSTN[2], xDSL[3], LAN[4]).

•**Bulegoko ekipamendua:** Teknologia hau baliatuz, periferiko guztiak hari gabe konekta daitezke elkarren artean. Esaterako, mahai gaineko ordenagailua inprimagailuekin, eskanerrekin[5], faxekin, saguekin eta teklatuekin konekta daiteke, hainbeste traba egiten duten kablerik erabili gabe. Lan egiteko modu horri esker, askatasun-sentsazioa handiagoa izaten da lan egitean.

•**Konferentzia interaktiboa:** Bileretan eta hitzaldietan, bat-batean transferi dakizkieke dokumentuak aukeratutako parte-hartzaileei, bai eta negozio-txartel elektronikoak elkarri eman, hari bidezko inongo konexiorik erabili beharrik gabe.

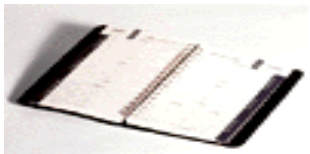
•**Aurikularrak**: Teknologia honekin, aurikularrak telefono mugikorrarekin, ordenagailu eramangarriarekin edo beste edozein gailurekin "konektatu" ahal izango dira, eskuak libre izan ahal izateko, bai bulegoko lan garrantzitsuak egiteko orduan, kotxean,... Aurikularrak erabiliz, unean bertan erantzun dakizkieke deiei, ahotsaren bidez konexioak aktiba daitezke, ...

Horrez gain, hari gabeko aurikularren bidez entzuten den soinua kalitate handikoa da, hormak oztopo izan gabe, eta ordenagailu eramangarrietan ere erreproduzi daiteke audio eran. Halaber, bai bolumena eta bai mikrofonoaren irabazia kontrola daitezke.

•**LAN:** Bluetooth lan-tresna bulegoan instalatuz gero, esan bezala, hainbeste traba egiten duten eta hain deserosoak diren kableak erabiltzea saihestuko da.

Modu honetan, ez da zertan eremu oso bat kable bidez josi lan-estazio berriak finkatu ahal izateko. Jakinda teknologia honi esker gauza daitezkeen konexioak puntutik punturakoak eta puntutik puntu anitzerakoak direla, birtualki konexio mugagabeak egin ahal izango dira.

•**Sinkronizazio automatikoa:** Gailu eramangarrietan bildutako informazio guztia, Bluetooth teknologia duen beste edozein gailutik baliatu ahal izango da, kablerik erabili beharrik gabe.



HIZTEGIA

[1] ISDN edo RDSI

(*Integrated Services Digital Network*).
Nazioarteko komunikazioko estandarra, ahotsa, bideoa eta datuak bidaltzekoa, telefono-linea digital bidez edo telefono normalen kable bidez. ISDNk 64 Kbps-ko abiaduran transferitzen ditu datuak.

Telefono-konpainia gehienek bi linea eskaintzen dituzte aldi berean. Linea bat ahotserako erabil daiteke eta bestea datuetarako, edo, bestela, bi lineak datuetarako erabili; abiadura 128 Kbps-koa da, gaur egungo modem azkarrenen abiaduraren hirukoitza.

[2] PSTN

(*Public Switched Telephone Network*). Nazioarteko telefono-sistema, kobrezko kable bidez ahots-datuak transmititzen dituena.

Hori guztia, teknologia digitalean oinarritutako laneko telefono berriekin alderatuta. **POTS** izenarekin ere ezagutzen da.

HIZTEGIA

[3] xDSL

(*Digital Subscriber Lines*). Kategoria nagusi bi ADSL eta SDSL dira.

DSL teknologiek modulazio-eskema sofistikatuak erabiltzen dituzte datuak kobrezko kableetan sartzeko. Telefono-estazio batetik etxe edo bulego batera konexioak egiteko erabiltzen dira, baina ez bi telefono-estazioen artean.

[4] LAN

(*Local Area Network*). Elkarren artean konektatutako ordenagailuak, baliabide berak erabiltzen dituztenak, besteak beste, biltegiratze-memoria, periferikoak edo aplikazioak.

[5] Eskanerra

Informazio analogikoa, esaterako, inprimatutako orrialdeak edo argazkiak, balore digital bihurtzen dituen periferikoa. Modu horretan, datuak ordenagailutik kudeatu edo biltegira daitezke. Beste eskaner-mota bat "escaner dedikatuak" dira, adibidez, hatz-arrastoei buruzko informazioa antzematen dutenak ekipo bateko erabiltzaile baliagarriak identifikatu ahal izateko.

• **Bideo-kamerak:** Bluetooth teknologia oso moldagarria da, eta horren adierazgarri dugu kameren eta ordenagailu eramangarrien artean irudi finkoak eta bideo-klipak transferitu ahal izatea. Kamera digitala Bluetooth denean, argazkiak eta bideoak bidal daitezke berehala, edozein lekutatik, kable bidezko konexiorik erabili beharrik gabe.

• **Kable bidezko konexioak**: Bluetooth teknologiaren bidez hainbat gailu digital lotu nahi dira elkarren artean, hari gabeko konexioak baliatuz. Munduarekin konektatzeko sarbidea behar duzu Bluetooth gailuan. "Mugimenduan" zaudenean, sarbidea askotan telefono mugikorra izaten da; "mugitu gabe" zaudenean, berriz, etxean, bulegoan edo hotelean, esaterako, kable bidezko konexioa ere izan daiteke sarbidea (PSTN[2], ISDN[1], LAN[4] edo xDSL[3]).

Sarbidea edozein dela ere, konexio guztiak berehalakoak dira eta ez dira eteten nahiz eta igorlearen eta hartzailearen artean objekturen bat egon.

3 1ean modeloa: Etxean telefono eramangarri (linea finkoko) bezala funtzionatzen du telefonoak. "Mugitzen" ari zarenean, telefonoak mugikor (linea zelular) bezala funtzionatzen du, eta zure telefonoa Bluetooth teknologia duen beste telefono mugikor baten eremuan sartzen denean, walkie-talkie baten antzera funtzionatzen du.

• **Bestelako gailu elektronikoak:** Bluetooth teknologiako aurreikuspenak mugagabeak dira, izan ere, egunero azaltzen dira produktu eta aplikazio berriak, bai eta funtzionalitate berriak ere, existitzen diren gailuetarako. Besteak beste, eskaner[5] eta disko gogor eramangarriak, informazioa eskumuturreko erlojuetan, hozte-guneak, kafe-makinak, aurkezpen-proiektoreak, ..., adibide gutxi batzuk besterik ez dira, erakusten digutenak hari gabeko bizkortasunak eta segurtasunak gure eguneroko bizitza soilduko dutela.

Bizkortasuna eta segurtasuna

Bluetooth teknologia diseinatua dago erabat funtzionala izan dadin, bai giro zaratatsuetan ere, eta ahots-transmisioa baldintza latzetan ere entzun ahal izan dadin. Bluetooth teknologiak transmisio-bizkortasun handia eskaintzen du eta datuak babestuta daude, errore-konexio metodo aurreratuen bidez, bai eta **enkriptazioko** eta **autentifikazioko** metodoen bidez, erabiltzailearen **pribatutasuna** bermatuta gera dadin.

Frantziako armadak banda bera erabiltzen du (2.4 GHz) transmisioetarako, eta, hortaz, Frantzian Bluetooth gailuek frekuentzia bera erabiliko dute, baina 23 frekuentziara jauzi eginez, 79ra egin beharrean.

2002. urtean Bluetooth teknologia milaka gailu elektronikotan sartuta egongo dela espero da.

Helbide interesgarria:

www.ericsson.com.mx/products/w_data_w_internet/bluetooth/index.shtml

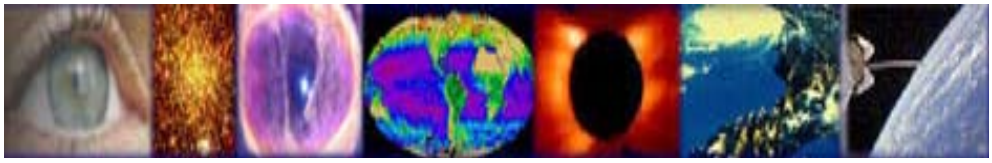
WINDOWS 2000ra MIGRAZIOA

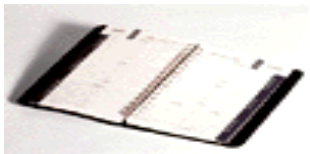
Win 2K Professional NT Workstation 4.0 ordezten duen sistema eragile bezeroa da.

Win 2K Server negozio-zerbitzarientzako estandarra da eta NT Server 4.0 ordezten du.

Win 2K Advanced Server-ek WNT 4.0 Enterprise ordeztuko du sare handietan.

Win 2K Datacenter Server datu-kopuru handietarako eta on line transakzioak prozesatzeko diseinatua dago.





ZERGATIK MIGRATU WINDOWS 2000ra?

Azken lau urteetan Windows NT izan da Microsoften sistema eragilerik ospetsuena enpresetako aplikazioetarako, zerbitzu errazak eskaintzen baititu fitxategiak erabiltzeko eta sail desberdinetatik inprimatzeko, e-commerce[6] eta Web[7] aplikazioak.

Windows 2000ra migratzeko arrazoirik garrantzitsuena da sistema eragile honen ezaugarriek enpresentzat dakarten abantaila:

- Active Directory (Directorio aktiboa)
- Intellimirror
- Windows Management
- Erabiltzaile mugigarrientzako euskarria

Ez da ahaztu behar migrazio-prozesu orotan hainbat aldaketa eta bateraezintasun gertatzen dela.

Microsoften arabera, kritikotzat jotako 500 aplikazioetatik, %90 W2000rekin bateratzeko modukoak dira. Hala ere, zer gertatzen da gainerako % 10arekin edo enpresek berek ordurako garatuta zeuzkaten aplikazioekin?.

- WNTn lan egiten duen 32 bit-eko aplikazioa bada, W2000n lan egiteko probabilitatea % 99koa da.
- WNTn lan egiten duen 16 bit-eko aplikazioa bada, W2000n lan egiteko probabilitatea % 80koa da.
- Win9x-n lan egiten duen aplikazioa bada, W2000n lan egiteko probabilitatea txikiagoa da aurrekoekin alderatuta, eta, hortaz, migrazioaren ondoren berridazketa egin beharko da.

W2000 diseinuan, Microsoftek aldaketa batzuk ezarri ditu, besteak beste, erregistro eta fitxategietarako egitura berriak, eta fitxategi-lokalizatzea, konfiantza eta erabilgarritasun aldetik aurreko sistema eragileak baino hobeak izateko.

HIZTEGIA

[6] e-commerce

Denda birtualak sortzeko tresnak.

[7] WEB

World Wide Web-en laburdura. Interneteko zerbitzarien multzoa, mota guztietako datuetan sartzeko aukera ematen duena, esaterako fitxategi grafikoetan, soinuzko zein idatzizkoetan, beste zerbitzarietako dokumentuen erreferentziak (lotura edo link izenekoak) emanez.

[8] Cluster

Biltegiratze-taldea, normalean biltegiratze-unitate bateko sektore-multzo bati lotua.

Noizean behin, sistema eragileak cluster edo luku erabili bat markatzen du, esleitutako fitxategirik izan ez arren (horri cluster galdua deritzo).

Diskoko lekua handitu daiteke, cluster edo luku galduak berresleituz, baina, lehendabizi, segurtatu egin behar da clusterrek datu baliagarririk ez dutela.

[9] Mikroprozesadorea

Ordenagailu bateko prozesu-unitatea duen zirkuitu elektronikoa. Mikroprozesadore batek instrukzioak hartu, deskodetu, eta bete egiten ditu, barne-erregistroak erabiliz, eta kanpo-memoria helbideratzen du.

HIZTEGIA

[10] Interfazea

Bi gailuen arteko lotura, datuen komunikazio egokia segurtatzen duena. Ezagunenak interfaze paraleloa eta seriekoa dira.

[11] VPN

(*Virtual Private Network edo Sare Pribatu Birtuala*). Kable publikoak baliatuta eraikitako sarea. Esaterako, sistema batzuen bidez, sareak sor daitezke informazioa garraiatzeko bide gisa Internet erabiliz.

Sistema hauek enkriptazioa eta bestelako segurtasun-bide batzuk erabiltzen dituzte, segurtatzeko baimendutako erabiltzaileak bakarrik sar daitezkeela sarera eta beste inork ezingo duela informazio hori atzitu.

[12] ISP

(*Internet Service Provider*), **IAP** (*Internet Access Providers)* ere deitua. Interneten sartzeko aukera ematen duen konpainia da. Zerbitzuak software-pakete bat, identifikazioa (erabiltzaile-izena) eta password-a ditu.

ISPek konpainia handiei ere zerbitzatzen die, Interneten zuzenean sartzeko aukera emanez.

ISP ezagunenak hauek dira: Airtel, Eresmas, Euskatel, Jazztel, Navegalia, ...

Hobekuntzak

• **Aplikazioen errendimendua hobetzea.** W2000ren *Windows Management Instrumentation* (**WMI**) zerbitzuak aplikazio konfiantzazkoagoak eta errazagoak eskaintzen ditu, eta, horrez gain, aplikazio horiek monitorizatzeko eta erabiltzeko aukera.

• **Euskarri multierabiltzailea eta "errantea".** W2000k ziurtatutako aplikazioek erabiltzaileak eta makinak bananduko dituzte. Ondorioz, erabiltzaileek makina ezberdinetatik izango dute aukera beren datu eta aplikazioak baliatzeko eta, halaber, hainbat erabiltzailek makina bera erabili ahal izango dute.

• **Segurtasun integratua.** Ziurtatutako aplikazioek erabiltzeko errazak diren segurtasun-neurriak eskaintzen dituzte eta autentifikatze-prozesu (single-sign-on) soilduak izaten dituzte.

Adituen arabera:
- Unix-eko bertsio komertzial gehienek oso segurtasun optimoa dute Internetekin lan egiteko.
- 2005ean Linux izango da sistema eragilerik seguruena.

• **Erabilera errazagoa.** Aplikazioak Active Directory-n gordetako informazio orokorrean sartu ahal izango dira, segurtasunari, politikei, helbideei eta konfigurazioko gainerako gaiei buruzkoetan.

• **Instalazio eta desinstalazio garbiak.** Instalazio-prozesuan zehar, aplikazioek ez diete mahai gaineko konfigurazioei ezta gainerako aplikazioei kalte egiten.

• **Cluster[8] zerbitzuak ustiatzeko gaitasuna, downtime murrizteko**. Downtime da makina produktiboa ez deneko laneko aldia.

Zein segurtasun-mota eskainiko digu Windows 2000k?

Microsoftek Microsoft 2000 Server (zerbitzaria) eta Professional (mahai gainekoa) edizioak diseinatu ditu, plataforma egonkorragoa eta seguruagoa izan dadin. Hona hemen ezaugarriak:

• **Active Directory:** WNT 4.0. domeinuan oinarritutako erabiltzaile-direktorioak ordezteko diseinatua dago. Direktorio honetan sareko objektu eta baliabide guztiak gordeta daude, sareko beste edozein puntutan bikoiztu daitekeen datu-base hierarkikoan.

• **Kerberos, 5 bertsioa:** Autentifikatze-protokolo estandarizatua, segurtasunean oso erabilia. Protokolo hau WNTko beste protokolo bat ordezteko diseinatu zen. Kerberos oso hedatua dago Internet erabiltzen duten enpresetan, eta zerbitzu hauek eskaintzen ditu:

1. Autentifikatze bizkorragoa
2. Elkarrekiko autentifikatzea
3. Win-Unix elkarreragingarritasuna
4. Gako publikoko hedapenak

- **Smart Cards-en euskarri:** Kreditu-txartelen tamainako txartelak dira, eta mikroprozesadorea[9], memoria eta interfazea[10] dituzte, lan-estazioekin edo sareekin lan egin ahal izateko.

- **Gako publikoa:** W2000 gako publikoko kriptografiako zerbitzu berritzaileetarako prestatuta dago (**PK**, *Public Key*).

- **IPsec: TCP/IP** trafikoa enkriptatzeko sare-protokoloa da. Hiru segurtasun-eremu hartzen ditu: autentifikazioa, datuen osotasuna eta datuen pribatutasuna.

- **NT fitxategi-sistema hobetua: NTFS** (*NT File System*) hobetua izan da, enkriptatze-funtzioak ere izateko.

- **Sare pribatu birtualentzako (VPN[11], *Virtual Private Network*) euskarria hobetzea:** VPNak erraz administratzeko tresna berriak eskaintzen ditu, esaterako, erabiltzailearen eta zerbitzuaren artean konexioa ezartzeko prozesua. Era berean, Interneten bizkor sartzeko aukera ematen die Interneteko Zerbitzu Hornitzaileei (**ISP[12]**, *Internet Service Providers*) eta sistema-administratzaileei.

> Eusko Jaurlaritzak aurki zerbitzari guztiak W2000ra migratzeko asmoa dauka

Helbide interesgarriak:

http://enete.us.es

http://www.microsoft.com/spanish/windows2000

	WNT 4.0	WINDOWS 2000
GAITASUNA	40.000 erabiltzaile onartzen ditu domeinu bakoitzeko	Sareko baliabide diren 10 milioi objektu onartzen ditu, besteak beste, erabiltzaileak, ekipoak eta inprimagailuak.
KOPIA	Domeinu nagusiko (Maisua) kontrolatzaileak soilik irakur eta idatz dezake domeinuko datu-basean. Aldaketak bikoiztu egiten dira Backup domeinuko kontrolatzaileen kasuan	Multimaster – Domeinuko kontrolatzaile guztiek dute domeinuko datu-basearen kopia.
IP IZENEN EBAZPENA	Internet Izenen Windows Zerbitzua (WINS, Windows Internet Naming Service)	DNS zerbitzaria (Domain Name Server)
DOMEINU-IZENAK	NetBIOSeko izenak	DNS domeinuko izenak

GALDERAK

Zer da Java RMI/IIOP?

- **RMI** (*Remote Method Invocation)* Banatutako programazioko berezko teknologia, objektuei zuzendua eta erabat Javan oinarritua. Teknologia honen helburua da, VMn (*Virtual Machine*) exekutatzen ari diren objektuak gai izan daitezela VM ezberdinetan exekutatzen ari diren objektuen metodoak deitzeko. Azpimarratzekoa da, VMak makina berean edo sare bidez konektatutako makina ezberdinetan egon daitezkeela.

- **IIOP** (*Internet Inter-ORB Protocol*) Interneten elkarreragina izateko protokolo estandarizatua espezifikatzen du, eta, ondorioz, produktu ospetsuenetan oinarritutako beste ORB batera-garriekin elkarreragina izatea ahalbidetzen du.

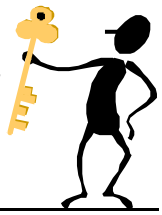
- **MIDDLEWARE** Bi aplikazio ezberdin konektatzen dituen software-a.

- **ORB** (*Object Request Broker)* Bezeroen eta zerbitzarien artean middleware gisa diharduen osagaia.

SEGURTASUNA POSTA ELEKTRONIKOAN

Guztiok dakigunez, gaur egun ez dago sistema informatikorik informazio-segurtasuna % 100ean bermatzen duenik, izan ere, hainbat modutan hauts daiteke sistema baten segurtasuna.

Hala ere, informazioa segurtatzeko estrategia egokia bideratzea enpresa salbatzeko bidea izan daiteke.



KRIPTOGRAFIA

Kriptografia hitza grekoko *kryptos* ('ezkutatu') eta *gráphein* ('idatzi') hitzetatik dator, eta, hortaz, 'idatzi ezkutua' esan nahi du.

Ezkutuko informazioa bidali nahi duenak teknika kriptografikoak erabiliko ditu mezua "ezkutatu" ahal izateko (zifratu[15] edo enkriptatu esango dugu). Jarraian, mezua bidaliko da ustez "segurtasunik gabekoa" den komunikazio-lineatik, eta, gero, baimena duen hartzaileak bakarrik irakurri ahal izango du mezu "ezkutua" (deszifratu edo desenkriptatu deituko diogu).

Kriptografia bi adar nagusitan banatzen da: gako pribatuko kriptografia edo kriptografia simetrikoa, batetik, eta gako publikoko kriptografia edo kriptofrafia asimetrikoa, bestetik.

Erasoen jatorria:
"Hacker" independientea, %34,74
Lehiakidea, %24,88
Enplegatu nahigabetua, %40,33

KRIPTOGRAFIA SIMETRIKOA

Simetriak esan nahi du alderdiek gako bera dutela bai enkriptatzeko eta bai deskriptatzeko.

Oro har, zifratu nahi den mezuari hainbat funtzio aplikatzen zaizkio, soilik gako bakarra ezagututa alderantziz aplikatu eta mezua deszifratu ahal izateko.

Eragozpen bat dauka, izan ere, komunikazioetan erabiltzeko, gakoak egon behar du bai igorlearenean eta bai hartzailearenean, eta, ondorioz, arazoa da nola transmititu gakoa modu seguruan. Sistema kriptografiko ezagunena **DES**[13] deiturikoa da.

KRIPTOGRAFIA ASIMETRIKOA

Kriptografia asimetrikoak bi gako ezberdin erabiltzen ditu erabiltzaile bakoitzeko: bata publikoa, gainerako erabiltzaileek ezagutzen dutena, eta jabeari zuzendutako mezuak zifratzeko, edo deszifratzeko/sinadura egiaztatzeko erabiliko dutena; bestea pribatua, jasotako mezuak deszifratzeko (gako publikoarekin enkriptatuak) eta norberaren mezuak sinatzeko. **RSA**[14] da sistema asimetrikorik erabiliena.

Praktikan, kriptosistema-mota bien arteko konbinazioa erabiltzen da, izan ere, bigarrenak ere eragozpena dauka, teknologikoki lehenengoa baino askoz ere garestiagoa dela, alegia.

HIZTEGIA

[13] DES

(*Data Encryption Standard*, datu-enkriptazioko estandarra). Algoritmoa, jatorrian IBMk Lucifer izenarekin garatutakoa, informazio garrantzitsua sailkatu gabe guztiak zifratzeko estandar gisa.

DESek 64 bit-eko blokeak zifratzen ditu, permutazio eta ordezte bidez, eta, horretarako 64bit-eko gakoa erabiltzen du, horietako 8 paritatezkoak izaki.

[14] RSA

(*Rivest, Shamir and Adelman,* teknikaren asmatzaileak). RSA algoritmoaren funtsa da ez dagoela bide eraginkorrik zenbaki oso luzeak faktorizatzeko. Horregatik, RSA gakoa lortzeko ordenagailu asko eta denbora behar dira.

RSA algoritmoa enkriptazioko estandar bilakatu da industria sendoetan, bereziki Internetera datuak bidaltzeko. Oinarrian hainbat software produktu daude, besteak beste, Netscape Navigator eta Microsoft Internet Explorer.

Teknologia aldetik hain da indartsua, Ameriketako Gobernuak murriztu egin du atzerriko herrialdeetara zabaltzea.

DES RSA baino bizkorragoa da, eta, ondorioz, gehiago erabiltzen da Interneten eta merkataritza elektronikoan.

Duela 25 urte arte, mezu zifratuen trukea militarren, diplomatikoen eta zerbitzu sekretuen pribilegioa zen.

1991n, **PGP (Pretty Good Privacy)** programa ospetsua atera zenean, lortu zen jende guztiak ziurtasun osoko posta elektronikoaren abantailak izatea.

Errealitatean, mezuak (luzeak) kodetu egiten dira, oso eraginkorrak diren algoritmo simetrikoen bidez, eta, ondoren, kriptografia asimetrikoa baliatzen da gako simetrikoak (laburrak) kodetzeko.

ZER DA PGP?

PGP (Pretty Good Privacy, "pribatutasun nahiko ona") Phil Zimmermann-ek garatutako segurtasun-paketea da, posta elektronikoa zifratzeko hedatuena eta egiaztatuena, bai Interneterako eta bai X.400erako. 128 bit erabiltzen ditu.

PGP erabilita, posta elektronikoak abantaila hauek izango ditu:

- Konfidentzialtasuna[16]
- Autentifikazioa[17]
- Osotasuna[18]

PGPren zein bertsio erabili behar da?

Nazioarteko bertsiorik garrantzitsuenak bi hauek dira: 2.6.3i eta 5.0i. Garai desberdinetan sortutakoak dira eta kalitate aldetik ere alde handia dute; 5.0i da modernoena eta erabiltzeko errazena.

2.6.3i bertsioa, sendoa eta fidagarria izan arren, ez zen erabiltzeko erraza, ez baitzuen interfaze grafiko egokirik.

Erabiltzaileek ziurtagiriak trukatzen dituzte elkarren artean, ziurtatze-entitaterik erabili beharrik gabe.

5.0i bertsioak zifratu simetrikoko edo asimetrikoko algoritmo ezberdinen artean hautatzeko aukera ematen dio erabiltzaileari.

SINADURA DIGITALAK

Zer dira?

Dokumentu batean agertzen den karaktere-multzoa, egilea zein den (**autentifikazioa**) eta datuak gerora aldatu ez direla (**osotasuna**) frogatzen duena.

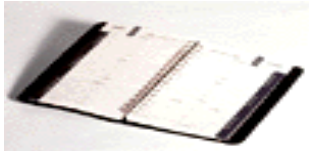
Nola egiten dira?

Sinatzailearen software-ak, sinatzean, *hash*[19] ("nahaste") algoritmoa aplikatzen du testuan, eta luzera finkoko aterakina, mezu horretarako zehatza, lortzen da (mezua apur bat aldatuz gero, aterakina erabat bestelakoa izaten da).

Nola egiaztatzen da sinadura digitalaren baliagarritasuna?

Hartzailearen software-ak aterakin zifratua, sinadura digitala, deszifratzen du, igorlearen gako publikoa erabiliz. Emaitza karaktere-bloke bat izaten da.

Ondoren, mezuaren testuari dagokion *hash* aterakina kalkulatzen du. Bi testuak bat badatoz, sinadura baliagarritzat jotzen da, baina, alderen bat badago, txikia bada ere, orduan ez da baliagarritzat jotzen.



HIZTEGIA

[15] Zifratu

Irakurgarria (testu argia) den mezu normala hartu eta lehen begiratuan ulertezina den karaktere-nahaste bihurtu (testu zifratua).

[16] Konfidentzialtasun

Honen bidez, segurtatzen da ezezagunek ezin dezatela posta irakurri.

[17] Autentifikazio

Pertsona bat identifikatzeko prozesua, erabiltzailearen izenean eta password-ean oinarritua. Autentifikazioak segurtatzen du pertsona bat berak dioena dela, baina ez du informaziorik ematen pertsona horren sartze-eskubideei buruz.

[18] Osotasuna

Honen bidez, segurtatzen da inongo hirugarrengok ez duela bidalitako edo jasotako mezurik ezingo dela aldatu.

[19] Hash

Norabide bakarreko funtzioa, luzera arbitrarioko fitxategi edo dokumentua luzera iraunkorreko katearekin lotzen duena (gaur egun, irteteko 160b erabiltzen dira); hash funtzio ezagunenak hauek dira: MD5, SHA1, RIPMED 160.

¡¡Albiste laburrak!!

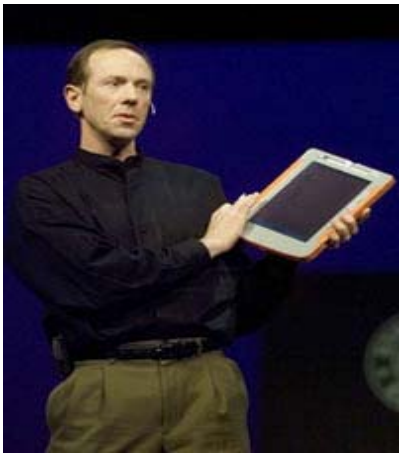
Microsoften Tablet PC

Microsoften gailu berria PDA (Personal Digital Assistant) baino apur bat handiagoa da eta eskuz idatzitako oharrak gordetzen ditu, gero elektronikoki erabiliak izan daitezkeenak.

Tablet PC 2002. urtean helduko da segur aski dendetara. Lehen begiratuan, oharrak erreproduzitzeko gailu soila da, baina, erregistratutakoan, editatu eta aldatu egin daitezke, bai eta hitz bidezko bilaketak egin ere.

Tablet PCk folio baten tamaina izango du eta ordenagailu eramangarria baino arinagoa izango da. Oso erabilgarria izango da bulegotik kanpo gaudenean, bileraren batean gaudenean, ...

> "Tablet PCri esker, bi bider ordu gehiago egon ahal izango naiz ordenagailutik deskonektatuta" esan zuen Bill Gates-ek.



Terminal berriak Microsoften Whistler sistema eragilearekin (gaur egun froga-urratsean dago) funtzionatuko du, eta teklatua, sagua, eta RAM memoria gehigarria izango ditu. Baina abantaila nagusia izango da, eskuz idatzitako oharrak, lehen esan bezala, hitzeko, esaldiko edo paragrafoko formateatu ahal izango direla, testu-prozesatzaileetan egiten den moduan.

Eta, jakina, Tablet PCk idazkera ezagutzeko sistemarik aurreratuena izango du, nahiz eta azaroaren 12an Las Vegas-en izandako Comdex Informatika Azokan egindako aurkezpenean ez zen sistemaren demostraziorik egin. Microsofteko bozeramaile batek esan zuenez, aparatua kalera heltzen denean, teknologia hau txertatuta etorriko da.

Aurreko urtean ikertzen ibili ziren nola lortu informatika-terminalek beraien artean elkarreragina izatea (kontsumitzaileari dokumentu bera aparatu ezberdinetatik erabiltzeko aukera eskaintzeko).

AHOTSAREN BIDEZ LAN EGITEA

Ahots-interfazeek aldatu egingo dute informatika-sistemak erabiltzeko modua. Ahotsaz baliatuz, testuak zuzendu eta ordenagailua kontrolatu ahal izango da, zehatzago eta erosoago.

Era berean, ahotsaren bidez Web-a kontrolatu ahal izango da, eta, ondorioz, Interneten nabigatu eta posta elektronikoan mezuak sortu eta bidali ahal izango ditugu.

Ahots-interfazeak

Internet iraultzailea izan da bezeroei zerbitzuak kudeatzeko orduan. E-business munduan lehiakorra izateko, konpainiek soildu eta hobetu egin behar dute erabiltzaileekiko harremana, dauden lekuan daudela informazioa erraz eskura ahal izan dezaten.

Erabiltzaileek gero eta gehiago eskatzen dute informazioa modu pertsonalean eskuratu ahal izatea eta transakzioak nahi bezala egin ahal izatea. Horretarako, konpainiek lan egiteko modu erraza eskaini behar dute, eta, hortaz, informazioa eskuratzeko interfazeak gero eta **naturalagoak** dira.

Informazioa edozein ordutan eta edozein lekutatik eskuratzeko eskariaren ondorioz, gero eta sarriago sartzen da jendea Interneten gailu mugigarriak erabiliz. Horregatik dago gero eta telefono eta bestelako gailu gehiago, eta horregatik dira aipatu gailuen teklatuak gero eta txikiagoak.

Horrela, bada, ahotsaren teknologia gero eta garrantzitsuagoa izango da informazioa eskuratzeko erabiltzaile-interfazeak diseinatzeko orduan.

Giza lengoaiaren teknologiek hainbat funtzio berri dituzte ordenagailuetan, esaterako:

- **Ahotsa ezagutzea**
- **Ahots-sintetizatzaileak,** testua ahots bihurtzeko sistemetan sartzen direnak.

APLIKAZIOAK

1. Lengoaia naturaleko komandoak erabiltzea sistemari zer egin nahi den esateko: adibidez, mezuak, formularioak eta bestelako dokumentuak erraz sortzea, editatzea eta zuzentzea.

2. Ahotsaren bidez aktibatutako txantiloiak erabiltzea formatu estandarra duten dokumentuetan, esaterako aurrekontuetan.

3. Ahots bidezko metodo laburtuak (makroak) erabiltzea sarri erabiltzen den testua txertatzeko, esaterako helbideak eta paragrafo estandarrak. Horrela, denbora irabazten da.

4. Hitz egitea, aplikazioak irekitzeko eta ixteko, pantailako leihoen tamaina aldatzeko.

5. Web-ean nabigatzea eta posta elektronikoa kudeatzea.

6. Internet Explorer, Netscape eta Chat programei zuzenean diktatzea, posta eta mezu berehalakoak sortzeko.

7. Ahots-bidezko-testua funtzioak aukera ematen du posta elektronikoa, Web-orrialdeak eta bestelako dokumentuak hitz eginez irakurtzeko.

Helbide interesgarriak:

www.hj.com/JAWS/JAWS37.htm

www.hj.com/NewsCommentary/Adaptive.html

ALBOAN: EJIE
PKI
SEGURTASUN-TXARTELA

HELBURUAK

PKI Eusko Jaurlaritzako aplikazioetan inplementatzea

Helburua da beharrezko politikak, estandarrak eta zerbitzuak ezartzea, erabiltzaileen komunikazio-esparrua konfidentziala, egiletasuna, **osoa** eta mezu edo transakzioak **zapuzten ez dituena** izan dadin. Modu horretan, PKIri esker (Public Key Infraestructure), enpresako izapide guztiak Internet bidez egin ahal izango dira, modu seguruan.

EZAUGARRIAK

Gakoa 1024 bit-ekoa da eta 5.01 Internet Explorer-en instalatzekoa da. Txartel-irakurgailua saguarekin batera konektatuta dago seriean.

Eusko Jaurlaritzako posta

Erakundeak Exchange posta-zerbitzaria erabiltzen du.

Exchange zerbitzariek hartu-agiriak bidaliko dizkiote elkarri.

Outlook-etik CRLak (*Client Revocation List*, Erabiltzaileak Ezeztatzeko Zerrenda) balioztatuko dira.

Zifratzeko gako publikoak Exchange direktorioan argitaratuko dira.

ADIBIDEA

INTEK proiektu pilotua:

Helburua da Enpresen Ikerketa eta Garapen Teknologikoa Sustatzeko Atalean Laguntza Eskaeren Tramitazio Telematikoa ahalbidetzea. Industria Saileko e-delfos proiektuaren barruan dago.
Web aplikazioa, Java-n garatua, Weblogic aplikazio-zerbitzariarekin.

Joan den asteartean, azaroaren 12an, Gobernu Kontseiluak onartu egin zuen Eusko Jaurlaritzako PKI proiektua.

Informazio gehiago: http://www.ej-gv.es/intek