Informazio Sistemen Arkitektura

Ingeniaritza Telematika Arloa

TELEK:O
UPV/EHU Bilbao

2. Atala: Segurtasuna Informazio Sistemetan

Informazio Sistemen Arkitektura

Telekomunikazioaren Ingeniaritza Teknikoko Gradua (3. Maila)

TELEK:O
UPV/EHU Bilbao

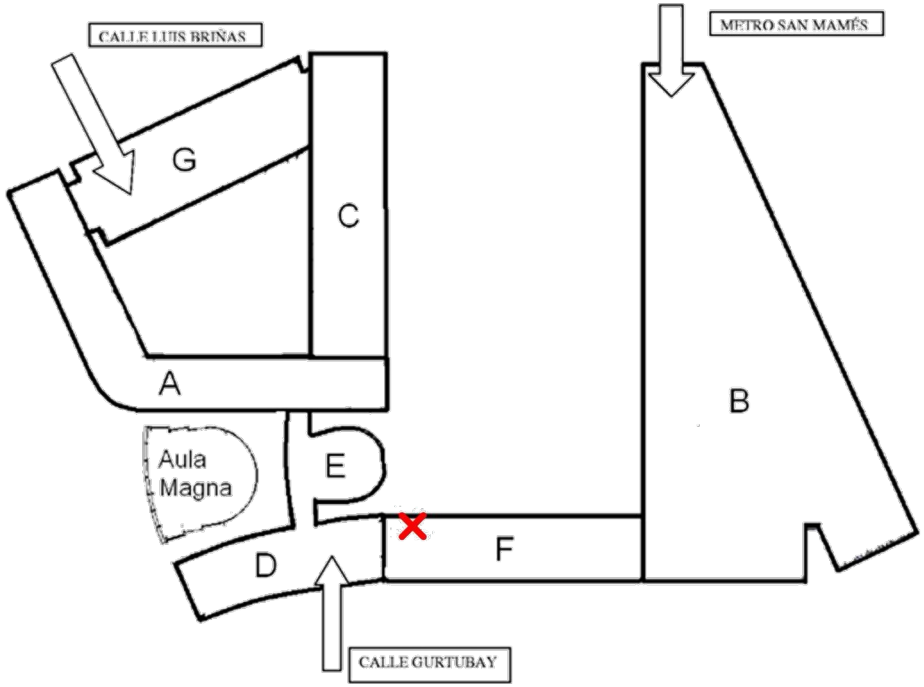
2. Atala

- **Helburuak edo gaitasunak**
  - Informazio sistemen segurtasunaren ikerketara hurreratzea, ekipo eta sistemen baliabideen (hardwarea, softwarea, firmwarea, informazioa, datuak eta komunikazioak barnean sartuz) osotasuna, erabilgarritasuna eta konfidentzialtasuna babesteko helburuarekin.
- **Bibliografia**
  - “Network and Internet Security”. William Stallings. Ed.: Prentice Hall. 1995.
  - “Network Security Essentials” (4th Edition). William Stallings. Ed.: Prentice Hall. 2011
    - **Irudi asko liburu honetatik hartu dira.**
  - “Cryptography and Network Security. Principles and practice” (5th Edition). William Stallings. Prentice Hall. 2010.
  - “Computer Networking: a top-down approach” (6th Edition). James F. Kurose and Keith W. Ross. Addison-Wesley. 2012.
  - “Applied Cryptography” (2nd Edition). Bruce Schneier. John Wiley & Sons. 1996.

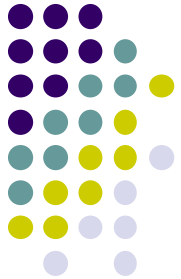
2. Atala. Segurtasuna Informazio Sistemetan

- **Irakasleak:**
  - Jasone Astorga jasone.astorga@ehu.eus
  - Eduardo Jacob eduardo.jacob@ehu.eus

Zubi eraikineko (F) 3. solairuan.



Aurkibidea



- Sarrera
- Segurtasunaren oinarriak informazio sistemetan
- Teknika kriptografikoak
- Segurtasuna Informazio Sistemetan
- Segurtasunaren egungo egoera
- Segurtasunaren kudeaketa

Aurkibidea

- **Sarrera**
- Segurtasunaren oinarriak informazio sistemetan
- Teknika kriptografikoak
- Segurtasuna Informazio Sistemetan
- Segurtasunaren egungo egoera
- Segurtasunaren kudeaketa

Sarrera

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

—*The Art of War,* Sun Tzu

- Segurtasunaren beharra dago
  - Ez da kontzeptu berri bat
    - Antzekotasunak ohiko munduarekin
- Informazioaren Segurtasunean (Information Security) eragina izan duten gertaerek
  - Digitalizazioa
  - Komunikazioak (sistema banatuak)
- Bere ikerketari hurreratzeko era ugari

Sarrera

- Segurtasunaren definizioa Informazio Sistemetan:

"The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)"

Iturria: NIST Computer Security Handbook

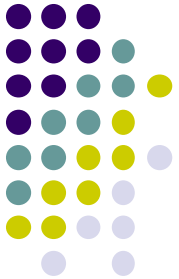
Honako definizioak agertzen diren bakoitzean, bat ikasi, kontzeptu nagusiak harrapatu, eta listo.
Orokorrean bat baino gehiago egongo da diapositiban.

CIA triad: Confidentiality, Integrity, Availability (Konfindentzialtasuna, Osotasuna, Eskuragarritasuna)

Sarrera

- Helburuak:
  - Segurtasun informatikoak informazio edo azpiegitura informatikoei eragiten dieten arriskuak minimizatzen dituzten arauak ezarri behar ditu.
    - Honen barnean sartzen dira: funtzionamendu ordutegiak, toki zehatzetara sartzeko mugak, autorizazioak, ukatzeak, erabiltzaile profilak, emergentzia planak, protokoloak, etab.
  - Segurtasun informatikoa aktibo informatikoak babesteko pentsatuta dago:
    - Azpiegitura konputazionala.
    - Erabiltzaileak.
    - Informazioa.

Sarrera



- Segurtasuna Informazio Sistemetan
  - Segurtasuna amaierako sistemetan (Computer security).
  - Segurtasuna komunikazio eta sareetan (Network security).
- Non aurki dezakegu “sare eta sistemen segurtasuna” gure inguruan?
  - Interneteko zerbitzaria/nabigatzailea transakzio elektronikoetarako (adibidez: Internet bidezko erosketak).
  - Banku elektronikoko bezeroa/zerbitzaria.
  - DNS zerbitzariak.
  - Bideratze-taulen eguneratze informazioa elkar trukatzen duten routerrek.
  - Beste adibiderik?

Sarrera

- Zeren aurka babesten gara?
  - Erasoen aurka.
    - Definizioa:
      - Informazio sistemaren inguruko baldintza (pertsona, makina, gertaera edo ideia), zeinak, aukera bat emanda, segurtasun arazo bat egotea ekar dezakeelarik.
    - Beraien kausak hauek izan daitezke:
      - Erabiltzaileak.
      - Programa maltzurrak.
      - Programazio erroreak.
      - Baimenik gabeko atzipenak.
      - Ezbeharrak (lapurretak, suteak, uholdeak)
      - Barneko langile teknikoak.
      - Informazio sistemen hutsegite elektroniko edo logikoak.
      - Etab.

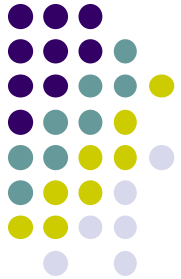
Sarrera

- Informazio sistema batean segurtasun maila egoki bat ezartzea konplexua da.
  - Eskainitako zerbitzuak definitu, tresna egokiak aukeratu, tresnen segurtasuna bermatu, etengabeko gainbegiratze beharra, eraginkortasunaren murrizketa, etab.
- Modu sistematiko bat behar da…
  - Segurtasun beharrak definitzeko eta
  - Betetzen dituzten neurri egokiak aukeratzeko.
- ITU-T-ren X.800 “Security Architecture for OSI” gomendioa.

Sarrera

- Estandarrak:
  - ISO 7498-2: Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture
  - ITU-T X.800 : Security architecture for OSI
  - RFC2828: Internet Security Glossary
  - IEC 62443: Zibersegurtasun industriala
  - Erlazionatuta; IEC 61508 Safety (beste segurtasuna)
- ISO 7498-2, ITU-T X.800:
  - Definitzen ditu:
    - Erasoak
    - Segurtasun zerbitzuak
    - Segurtasun mekanismoak

Sarrera

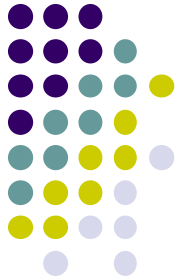


- ITU-T X.800 kontzeptuak:
  - Erasoak
    - Erakunde baten Informazio Sistemaren edozein osagairen segurtasuna arriskuan jartzen duen edozein ekintza.
  - Segurtasun zerbitzuak
    - Erakunde baten informazioaren prozesatze edo transmisio sistemen segurtasuna areagotzen duen prozesatze edo komunikazio zerbitzua.
    - Segurtasunaren aurkako erasoetatik babesteko sortzen dira eta zerbitzu bakoitza emateko mekanismo bat edo bat baino gehiago erabiltzen dira.
  - Segurtasun mekanismoak
    - Eraso bat detektatzeko, ekiditeko edo erasoak eragindako hutsegiteak zuzentzeko diseinatutako prozesua edo prozesu hori eusten duen ekipoa.

Sarrera

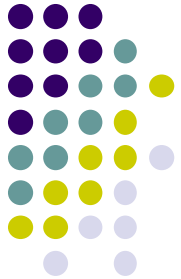
- OSI Segurtasun zerbitzuen definizioa
  - Definizioa:
    - *"**Security service** is a service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers as defined by ITU-T X.800 Recommendation"*
  - Barnean hartzen ditu:
    - Autentifikazioa
    - Sarbide kontrola
    - Konfidentzialtasuna
    - Datuen osotasuna
    - Ez ukatzea

Sarrera



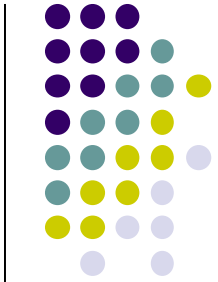
- OSI segurtasun mekanismoak:
  - Segurtasun zerbitzu bat inplementatzeko erabiltzen den teknika edo tresna.
  - Honetarako diseinuatuta daude:
    - Sistema baten segurtasun politikaren aurka doazen erasoak ekidin.
    - Sistema baten segurtasun politikaren aurka doazen erasoak detektatu.
    - Sistema baten segurtasunaren aurkako eraso batetik berreskuratu.
  - Ez dago zerbitzu guztiak eman ditzakeen mekanismo bakarra:
    - Mekanismo gehienek teknika kriptografikoak erabiltzen dituzte.
  - Sailkapena: prebentiboak, detektiboak eta errekuperagarriak.

Segurtasunaren oinarriak Informazio Sistemetan



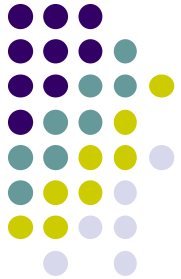
- Sarrera
- **Segurtasunaren oinarriak Informazio Sistemetan**
  - Erasoak
  - Zerbitzuak
  - Mekanismoak
- Teknika kriptografikoak
- Segurtasuna Informazio Sistemetan
- Segurtasunaren egungo egoera
- Segurtasunaren kudeaketa

Segurtasunaren oinarriak Informazio Sistemetan



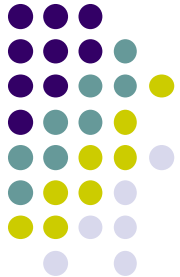
- Zer da Informazio Sistema bat? (I)
  - Informazioa:
    - Datu baseak.
    - Datu fitxategiak (Word, Excel…)
    - Agendak.
    - Posta elektronikoko mezuak.
    - WWW-eko liburu-markak (bookmark)
    - …

Segurtasunaren oinarriak Informazio Sistemetan



- Zer da Informazio Sistema bat? (II)
  - Informazioa edukitzeko, garraiatzeko edo bera maneiatzeko erabil daitekeen edozein elementu.
    - Zerbitzariak (datu baseak, posta elektronikoa, fitxategiak, WWW, izen-zerbitzariak,…)
    - Erabiltzaile plataformak (ordenagailu pertsonalak, PDAk,…)
    - Aplikazioak (bulegotika, aplikazio espezifikoak,…)
    - Sarea (hardware eta software sarbide elementuak, beraien konfigurazioa,…)

Segurtasunaren oinarriak Informazio Sistemetan



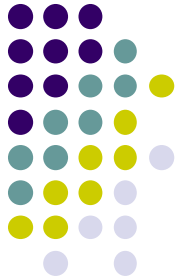
- Erasoak
  - Sistema baten segurtasunaren aurkako ekintza, mehatxu adimendun baten ondorioz:
    - Sistema baten “segurtasun-politikak” eta “segurtasun-zerbitzuak” ekiditeko, nahita egindako saiakera.

IETF (RFC 2828)

  - Edozein ekintza maltzur, Informazio Sistema baten baliabideak edo informazioa bera jaso, eten, ezeztatu, degradatu, edo suntsitzea helburutzat duena.

Committee on National Security Systems of USA

Segurtasunaren oinarriak Informazio Sistemetan



- Eraso motak (I):
  - Eraso pasiboak
    - Sistemaren gainbegiratzean oinarritzen dira eta konfidentzialtasunaren aurka doaz.
      - Informazioa zabaltzea: lortutako informazioa zabaldu egiten da.
      - Trafikoaren analisia: Informazioa zifratuta badoa, bere maiztasunari eta bere tamaina banaketari buruzko informazioa lor daiteke.
    - Detektatzeko zailak dira, ez dutelako aldaketarik eragiten sisteman. Hobea da erasoa ekiditen saiatzea, detektatzen saiatzea baino.

Informazioaren konfidentzialtasuna bermatu ekiditeko: Informazioa zifratu!

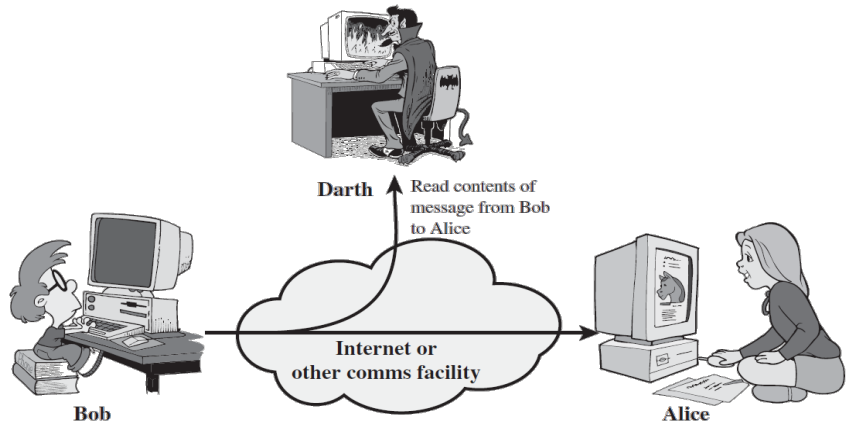
Eraso mota: "Informazioa inferitu"

Informazio inferitze-tik babesteko: "TRAFFIC PADDING" aplikatu: Trafiko gehigarria sartzea

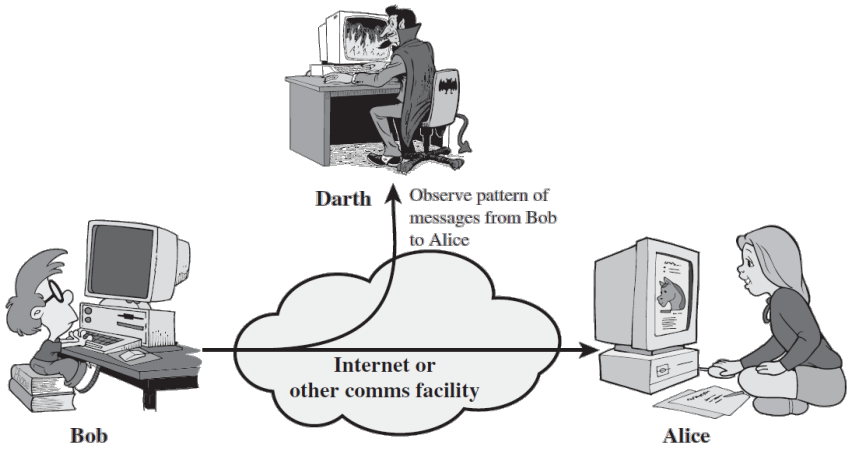
Segurtasunaren oinarriak Informazio Sistemetan

- Eraso pasiboak:

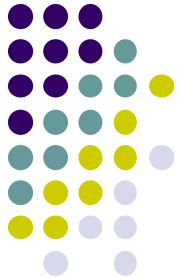
Informazioa zabaltzea



Trafikoaren analisia



Segurtasunaren oinarriak Informazio Sistemetan



- Eraso motak (II):
  - Eraso aktiboak: Mekanismoak detektiboak izan ohi dira, aldaketa hauen bila egoten direnak:
    - Sistemako elementuen aldaketan edo elementu berrien txertaketan datza:
      - Nortasunaren usurpazioa: entitate bat baimen ezberdinak dituen beste entitate ezberdin bat balitz bezala aurkeztu egiten da.
      - Birbidaltzea: aurretik atzitutako informazio sekuentziak berriro bidaltzen dira baimenik gabeko ondorio bat eragiteko helburuarekin.
      - Mezuen aldaketa: egiazko mezu baten parte bat aldatu egiten da.
      - Zerbitzu ukatzea: sistemaren funtzionamendu normala eragozten edo hondatzen saiatzea.

MAN IN THE MIDDLE!

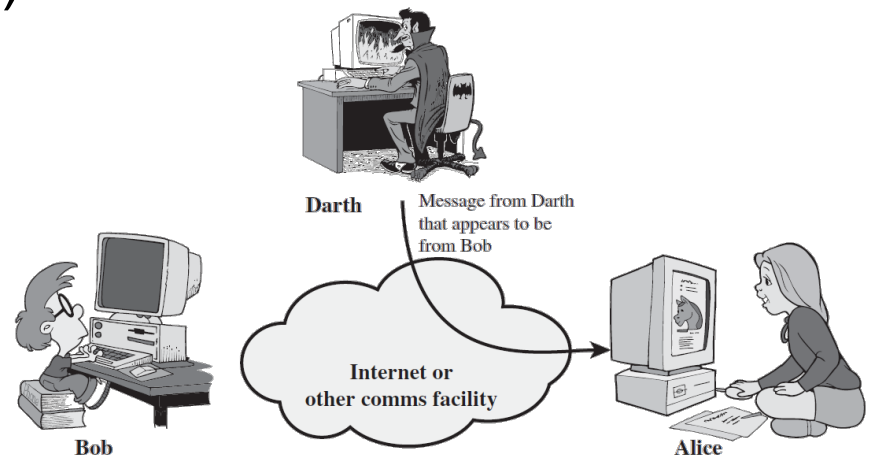
DoS : Denial of Service! (Distributed DoS)
TCP-SYN erasoa

  - Eraso pasiboen ezaugarrien alderantzizkoak

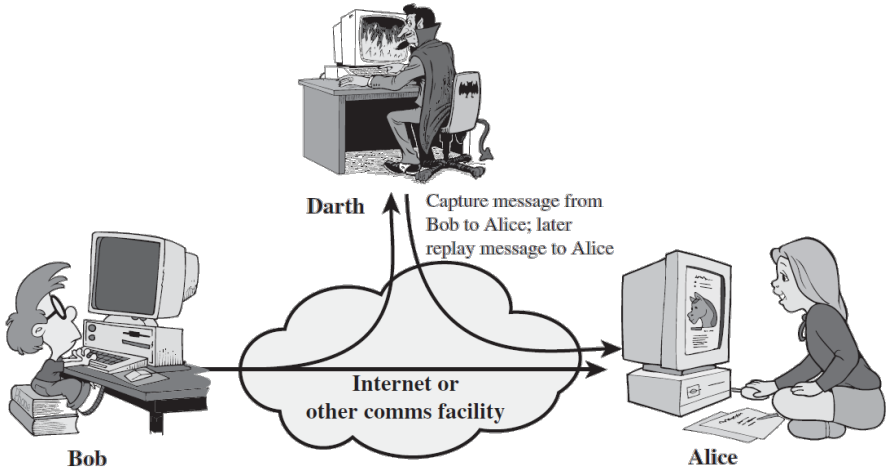
Segurtasunaren oinarriak Informazio Sistemetan

- Eraso aktiboak (I)

Nortasunaren usurpazioa



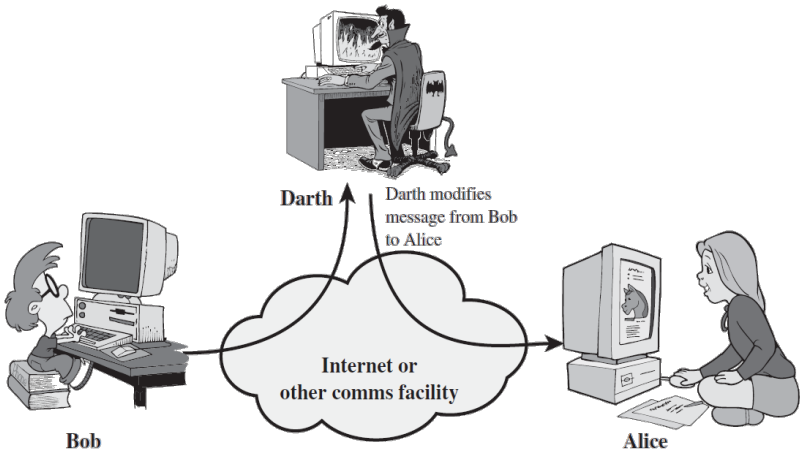
Birbidaltzea



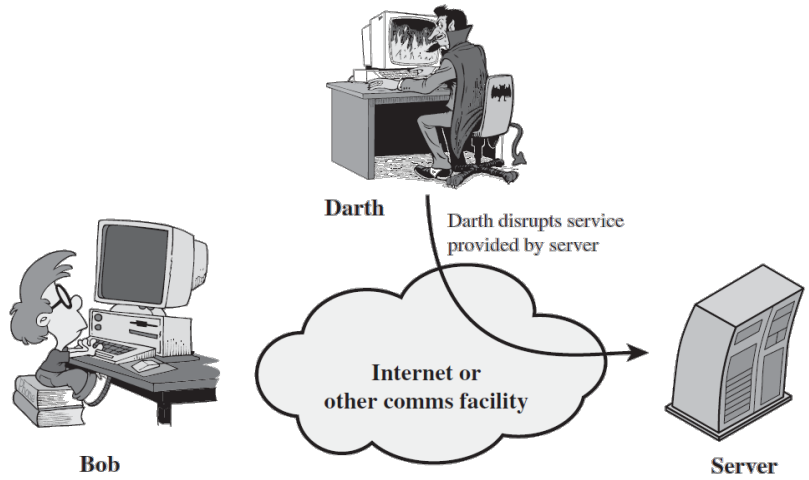
Segurtasunaren oinarriak Informazio Sistemetan

- Eraso aktiboak (II)

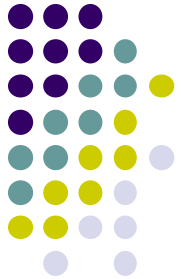
Mezuen aldatzea



Zerbitzu ukatzea

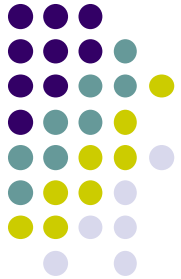


Segurtasunaren oinarriak Informazio Sistemetan



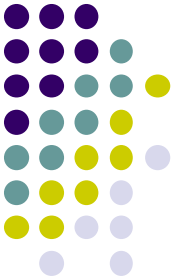
- Segurtasun zerbitzuak:
  - Autentifikazioa
  - Sarbide kontrola
  - Konfidentzialtasuna
  - Datuen osotasuna
  - Ez ukatzea
  - Eskuragarritasuna

Zerbitzuak. Autentifikazioa



- Mota berdineko entitateen artean:
  - Urrutiko entitatea benetan **berak dioena dela** egiaztatu.
  - Ezarpen eta datu-transferentzia faseetan.
- Datuen iturburuaren autentifikazioa:
  - Ez du bikoizketaren aurka babesten.
  - Datu-transferentzia fasean.
- Honako atazetan erabiltzen da:
  - Sarbide kontrola (edo autorizazioa).
  - Kontabilitatea (baliabideen kontrola).

Zerbitzuak. Sarbide kontrola



- Baimenik gabeko **erabileraren** aurkako sistemaren baliabideen babesa.
- Sarbide kontrola burutu ahal izateko entitateen identifikazioa beharrezkoa da ➔ autentifikazioa.
- Profilen eta xehetasunaren definizioa.

Zerbitzuak. Konfidentzialtasuna

- Baimenik gabeko **zabalkundearen** aurkako babesa.
- Lau mota:
  - Konexiora zuzendutakoa ➔ konexio batean transmititutako datuak.
  - Konexiora ez zuzendutakoa ➔ datu unitate sinpleak.
  - Eremu selektiboena ➔ konexio edo datu unitate baten eremu espezifikoak.
  - Trafiko fluxua ➔ trafikoaren analisiaren aurkakoa.

    Traffic Padding: Beharrezkoa ez den trafiko aleatorioa sortzen da, kanpoko analisia zailagotzeko.

Zerbitzuak. Datuen osotasuna

- Baimenik gabeko **aldaketen** aurkako babesa.
- Babestu beharreko helburuaren arabera:
  - Konexiora zuzendutako osotasun zerbitzua.
  - Konexiora ez zuzendutako osotasun zerbitzua.
- Erabilitako tresnaren berreskuratzeko ahalmenaren arabera:
  - Berreskuratze-gaitasuna daukan zerbitzua.
  - Berreskuratze-gaitasunik ez daukan zerbitzua.

Orokorrean berreskuratzeko metodoa birbidaltzea da.

Zerbitzuak. Ez ukatzea

DDOS-rekin ez du zerikusirik, nahiz eta hitz berdina izan euskaraz

- Burututako ekintzak ukatzeko aukeraren aurkako babesa.
- Bi mota:
  - Jatorriaren frogarekin ➔ hartzaileari jatorria bermatu
  - Helmugaren frogarekin ➔ jatorriari helmuga bermatu

Sinadura digitala eta zertifikatuak!

Zerbitzuak. Eskuragarritasuna

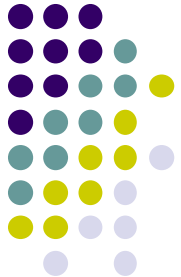
- Sistemak eskuragarri egon behar dira “beti”…
  - Sistema erredundanteak.
  - Hutsegiteen detekzioa.

Etenaldiak minimizatzeko eta haien efektu negatiboak ahalik eta gutxien mintzeko

- …edo hutsegiteak aurretik ezarritako denbora mugatu batean zuzendu behar dira
  - Kontingentzia plana.
  - Ordezko elementuen biltegia.
  - Konfigurazioen kudeaketa.

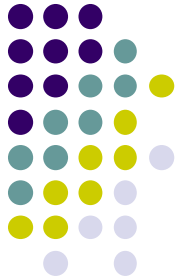
Eraso (birus, identitate lapurketa) gertatu baino lehen, arazo baten aurkako plana. (Edo beste gertakari bat: Suteak, lapurketak...)

Mekanismoak



- OSI segurtasun mekanismoak:
  - Zehatzak:
    - Zerbitzu bat ematera zuzendutako teknikak.
    - Adibideak:
      - Zifratzea, sinadura digitala, sarbide kontrola, osotasuna, autentifikazio trukea, trafiko betegarria, bideratze kontrola, ziurtapena.
  - Orokorrak:
    - Segurtasunaren kudeaketarako alderditzat har daitezke. Beharrezkoa den segurtasun mailarekin zuzenean erlazionatuta.
    - Adibideak:
      - Konfiantza, segurtasun etiketak, detekzioa, berreskurapena.

Mekanismoak



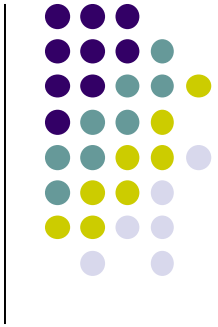
- Interesgarria da honako hau kontutan hartzea:
  - Sare mailako mekanismoak Gaur egun askotan aplikatzen dira sare (IP) mailan
    - Sareko trafiko guztia autentifikatu eta zifratu behar da.
    - Aplikazio guztiak babestu behar dira.
    - Nodo guztietan soluzio bera behar da.
    - IPv6 eta IPSec segurtasuna kontutan izanik diseinatu ziren.
    - Konponbide partzialak daude: erakundearen router-en artean: VPN-ak

IPSec IPv6 gainean joateko zegoen diseinatuta. IPv6 halanolako erabilera duelako, IPSec IPv4 gainean funtzionatzeko ahalmena garatu da, segurtasuna garrantzitsua delako.

Mekanismoak

- Interesgarria da honako hau kontuan hartzea:
  - Aplikazio mailako mekanismoak.
    - Mekanismo orokorrik ez dagoenez, interesatzen zaigun aplikazio bakoitzarentzat soluzio bat bilatu behar da.
    - Adibideak:
      - Posta elektronikoa: S/MIME, PGP, PEM...
      - Autentifikazioa eta gakoen elkar trukatzea: Kerberos, DCE, X.509, SKIP
      - Urruneko fitxategi sistemak: Secure NFS
      - Sarearen kudeaketa: SNMP v2
      - Telnet: SSH, SSL
      - WWW: SSL, SHTTP
      - FTP: SSL
      - Biltegiratze segurua: CFS
      - Ordainketa segurua: SET?

Mekanismo eta zerbitzuen arteko erlazioa

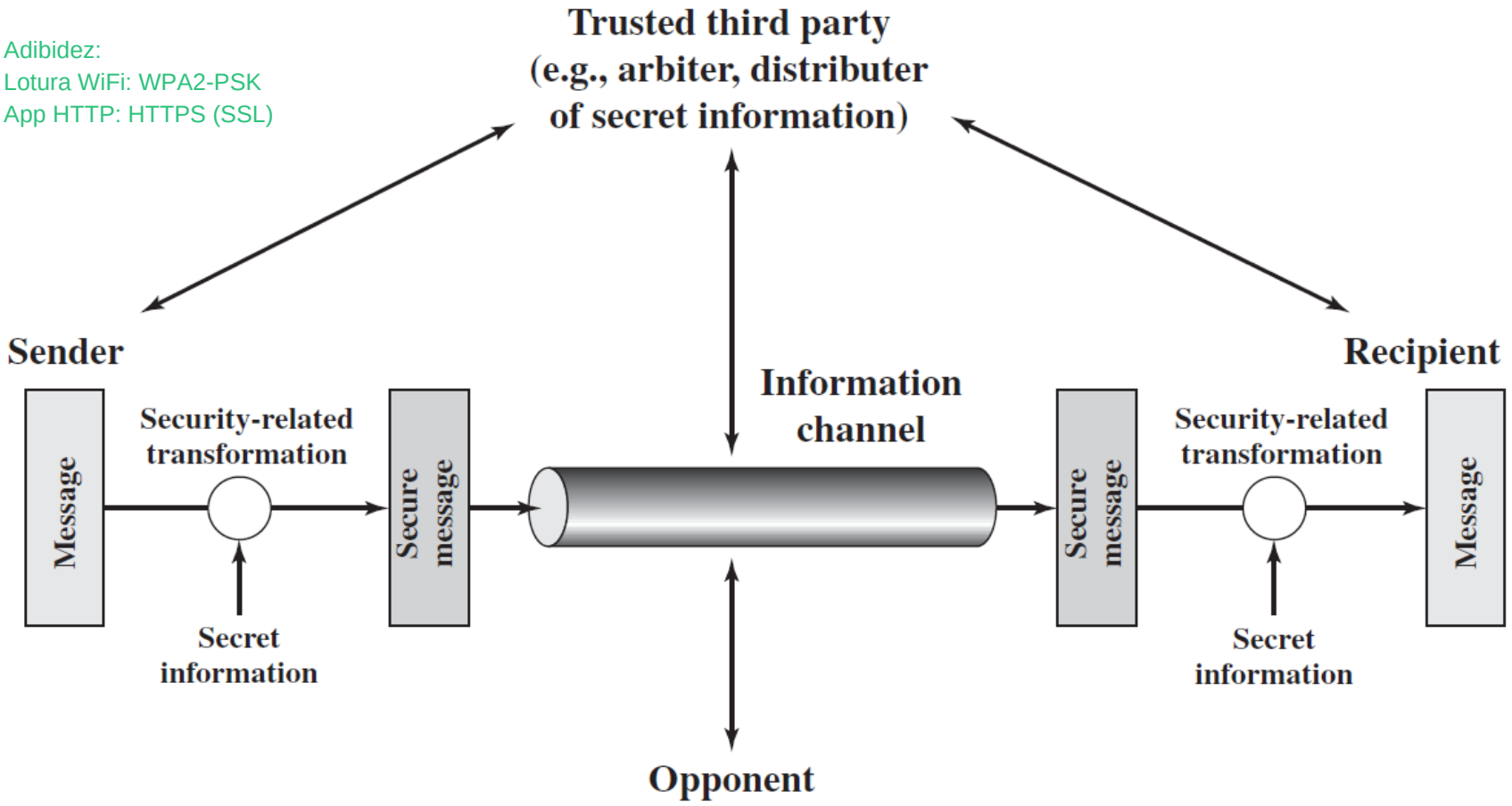


	Mechanism							
Service	**Encipherment**	**Digital Signature**	**Access Control**	**Data Integrity**	**Authentication Exchange**	**Traffic Padding**	**Routing Control**	**Notarization**
Peer Entity Authentication	Y	Y			Y			
Data-Origin Authentication	Y	Y						
Access Control			Y					
Confidentiality	Y						Y	
Traffic-Flow Confidentiality	Y					Y	Y	
Data Integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

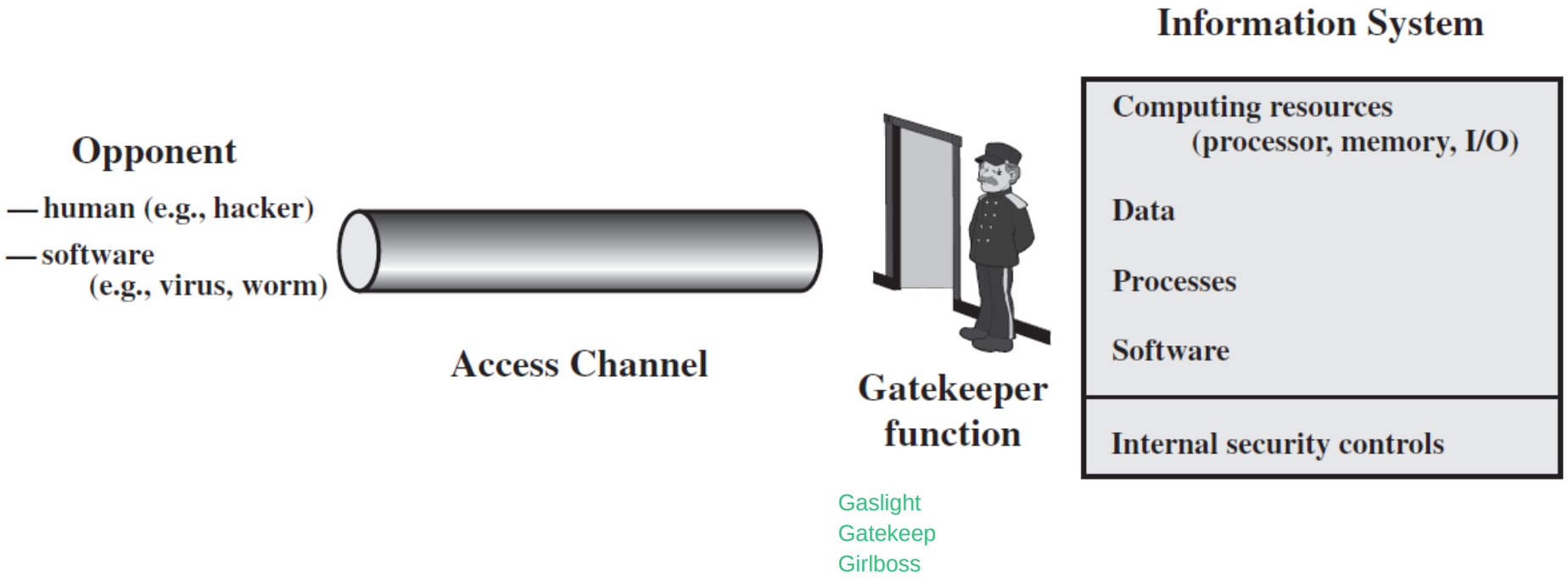
Sareko segurtasun eredua

Sare mailakoa bakarrik adierazita dago!
Honen gainean/azpian segurtasun maila gehiago!

Adibidez:
Lotura WiFi: WPA2-PSK
App HTTP: HTTPS (SSL)

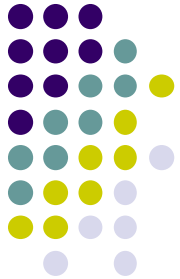


Sare sarbiderako segurtasun eredua



Gaslight
Gatekeep
Girlboss

Aktiboak, mehatxuak eta erasoak

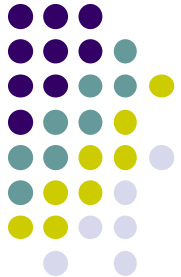


- Mehatxua:
  - “Informazio sistemaren inguruko baldintza (pertsona, makina, gertaera edo ideia) zeina, aukera bat emanda, segurtasun hauste bat egotea ekar dezakeelarik (konfidentzialtasuna, osotasuna, eskuragarritasuna edo legezko erabilera).”

- Erasoa:
  - “Eraso bat mehatxu baten gauzatzea baino ez da”

[Iturria: http://delitosinformaticos.com/seguridad/clasificacion.shtml]

Aktiboak, mehatxuak eta erasoak



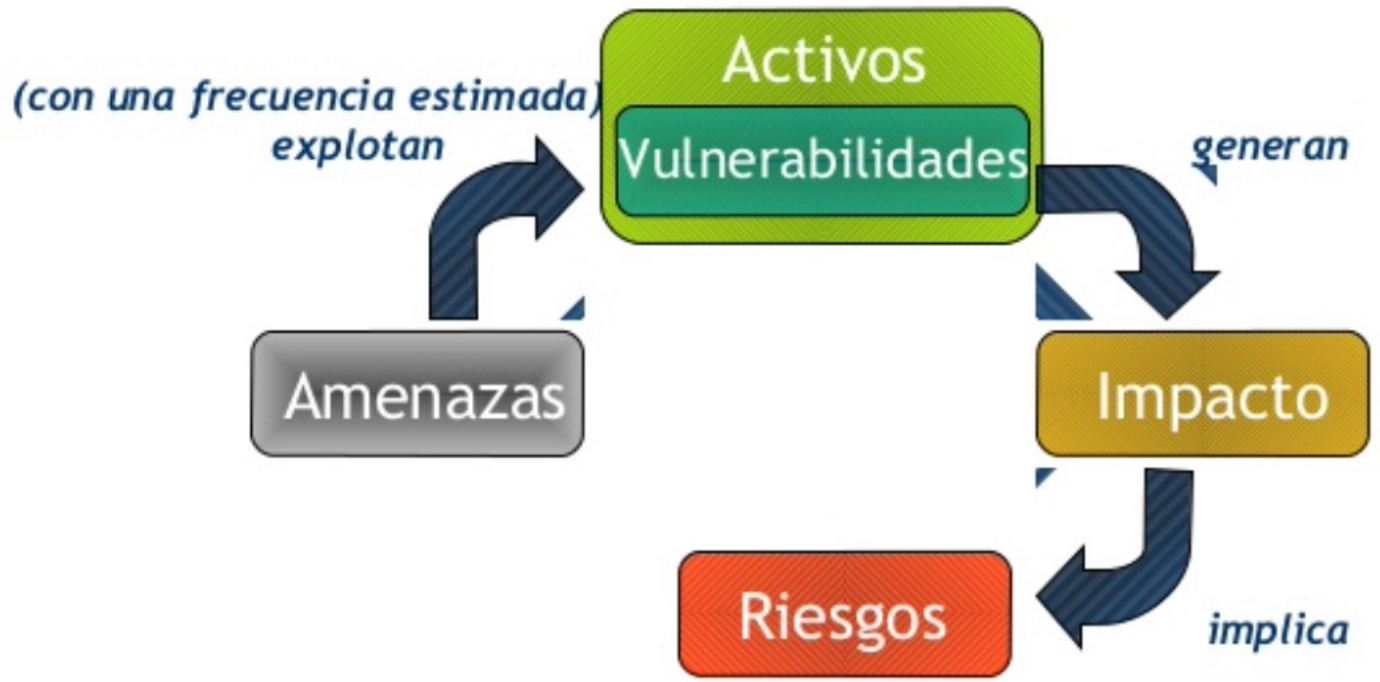
- Segurtasunaren aurkako mehatxuak (I):
  - Entitate, egoera, gaitasun, ekintza edo gertaera batek kalteak sor ditzakenean existitzen den segurtasun hauste posiblea.
  - **Ahultasun** baten ustiapen posibletik eratortzen den arriskua.
    - “Sistema baten diseinuan, inplementazioan edo operazioan existitzen den akats edo ahultasuna, eta sistema horren segurtasun politika hausteko ustia daitekeena”

      [Iturria: Stallings]
  - Mehatxu motak aztertzeko IS baten funtzioa informazioa ematea dela aintzat hartzen da.
    - Iturri batetik (fitxategia, memoria,...) helmuga batera informazio fluxu bat dagoela kontuan hartzen da.

Aktiboak, mehatxuak eta erasoak

- Honakoen arteko harremana: Mehatxuak - Aktiboak - Ahultasunak - Eragina, Arriskuak:

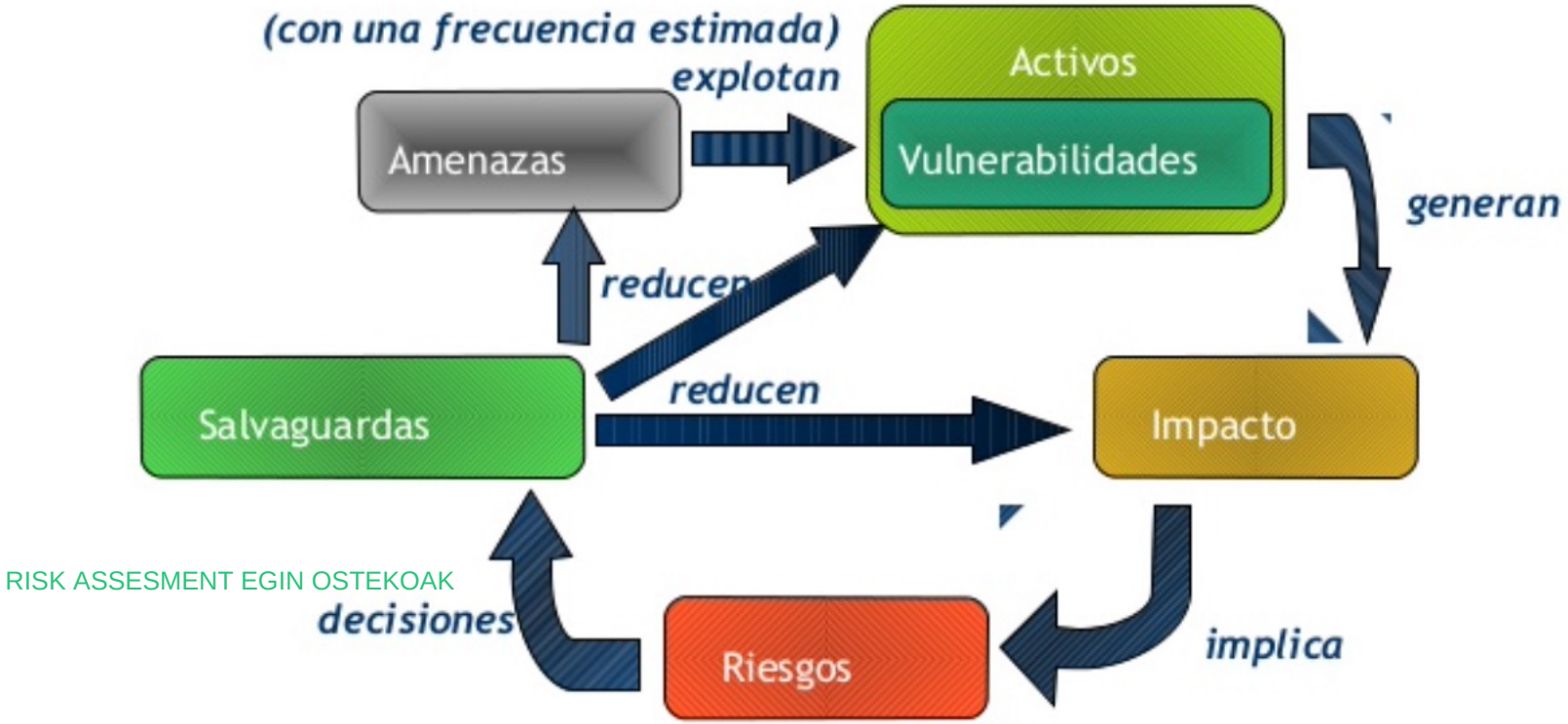
  - Relación Amenazas-Activos-Vulnerabilidades-Impacto-Riesgo:



[Iturria: Análisis y Gestión de Riesgos Fernando Aparicio, 8/4/20051 Security Xperts]

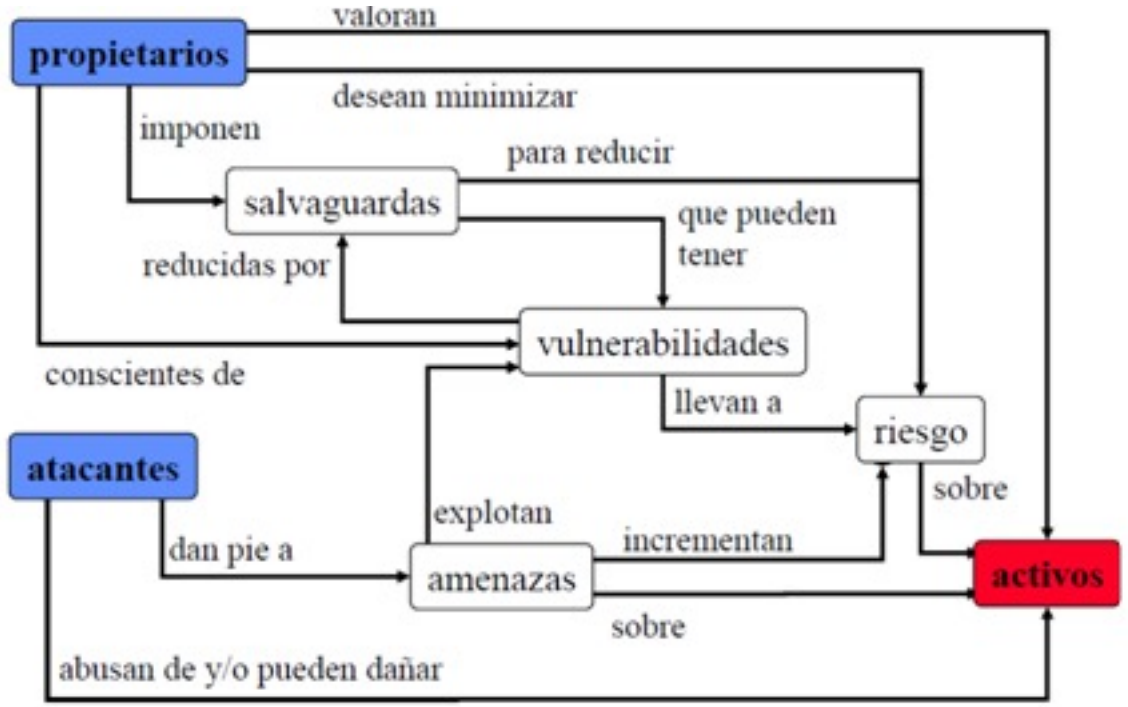
Aktiboak, mehatxuak eta erasoak

- Honakoen arteko harremana: Mehatxuak - Aktiboak - Ahultasunak - Eragina, Arriskuak:



[Iturria: Análisis y Gestión de Riesgos Fernando Aparicio, 8/4/20051 Security Xperts]

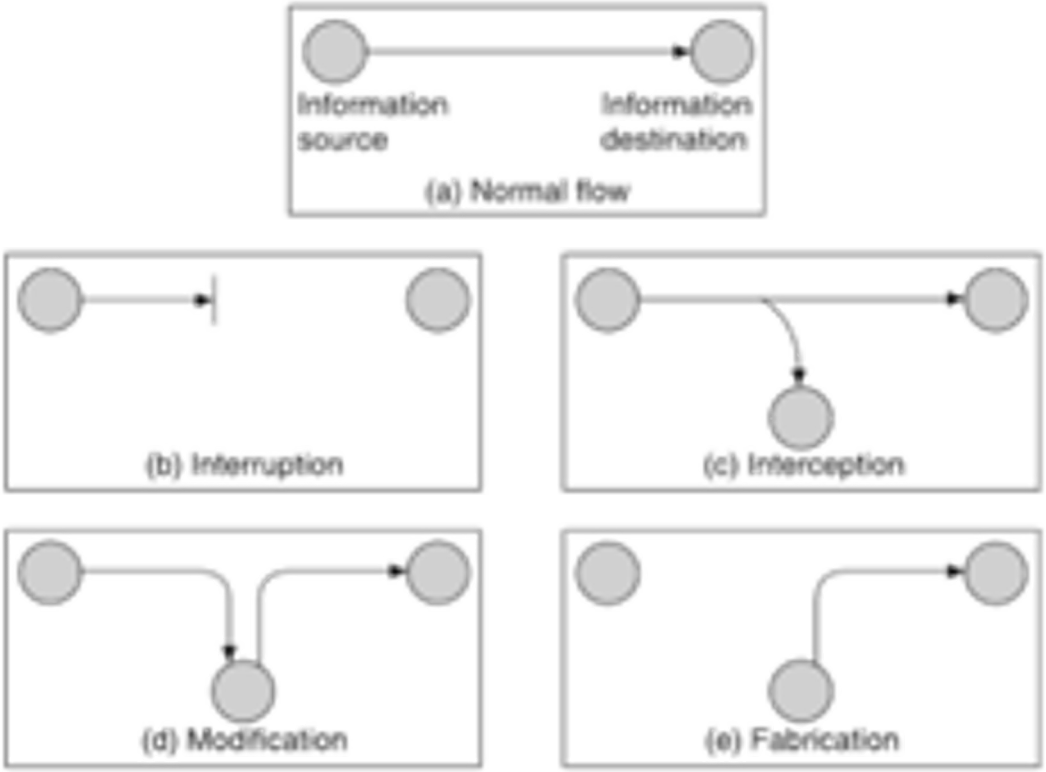
Aktiboak, mehatxuak eta erasoak



Aktiboak, mehatxuak eta erasoak

- Segurtasunaren aurkako mehatxuak (II):

Informazio fluxu normala eta segurtasunaren aurkako mehatxuak

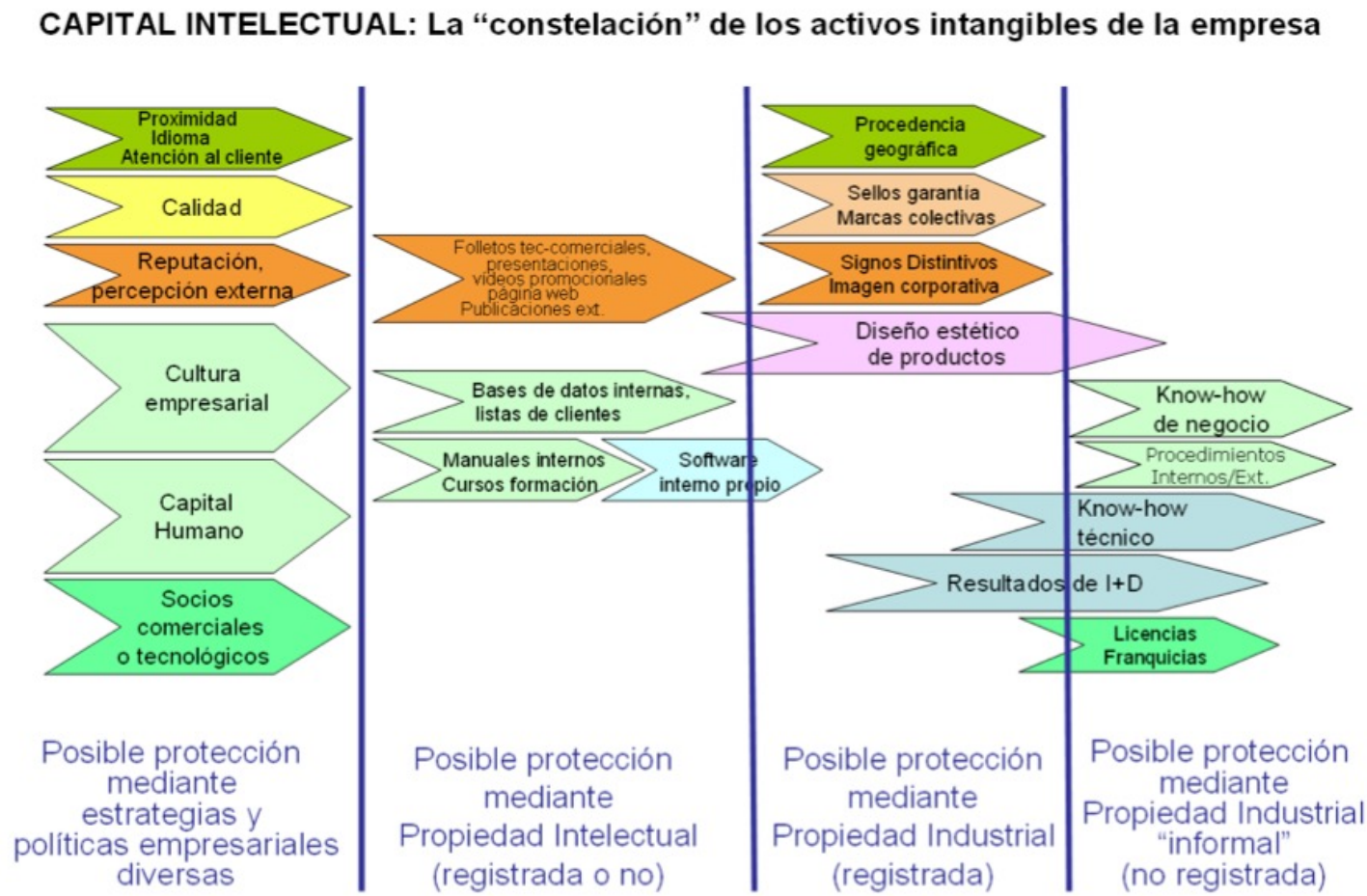


Mehatxuak eta aktiboak

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.		
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines	Messages are destroyed or deleted. Communications lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

[Iturria: Business Data Communications, 6/e. Stallings and Case]

Beste aktibo inmaterialak



[Iturria:https://www.oepm.es/export/sites/oepm/comun/documentos_relacionados/sobre_oepm/Aula_de_Propiedad_Industrial/InstruccionesRealizacionInventarioActivosIntangibles_version_agosto_2012.pdf]