Kontrolli i qasjes

Qëllimet dhe objektivat

- Politikat për kontroll të qasjes dhe modelimi i tyre si një matricë eksplicite (ACM)
- Siguria e mbështetur në grillë dhe kufizimi i rrjedhës së informacionit brenda grillës
- Bartja e informacionit me anë të manipulimit të kanaleve të fshehta
- klasifikimi, detektimi dhe ballafaqimi me kanale të fshehta

Përmbajtja

Politikat e kontrollit të qasjes

- Modeli Bell dhe LaPadula është një shembull *politike e kontrollit të qasjes.*
- Ideja themelore është të prezantohen rregulla që kontrollojnë çfarë qasjesh (d.m.th. *aksionesh*) mund të ndërmarrin *subjektet* kundrejt *objekteve*

MAC dhe DAC

- BLP është një sistem *mandator* për kontroll qasjeje, për dallim nga sistemet diskrecionale.
- *Kontrollet mandatore të qasjes (MAC):* rregullat zbatohen për çdo qasje të synuar, jo në diskrecion të ndonjë shfrytëzuesi të sistemit;
- *Kontrollet diskrecionale të qasjes (DAC):* zbatimi i rregullave mund të shmanget ose modifikohet nga disa shfrytëzues.
- D.m.th., për politikën BLP asnjëherë nuk lejohet asnjë qasje përveç se kur plotëson vetinë e sigurisë së thjeshtë ose vetinë *.
- Për kontrast, sistemi për mbrojtje të fajlave të një sistemi operativ, p.sh. Windows, implementon DAC meqë mbrojtjet e një fajli mund të modifikohen nga pronari i fajlit.

Matrica e kontrollit të qasjes

- Në përgjithësi, çfarëdo politike për kontroll të qasjes mund të paraqitet me një *matricë për kontroll të qasjes (access control matrix, ACM).* Për të gjithë subjektet dhe objektet e sistemit, matrica tregon në mënyrë eksplicite çfarë qasjesh lejohen për secilin çift subjekt/objekt.

	objekti_1	...	objekti_k
subjekti_1	A_i, A_j		$\varnothing$
...			
subjekti_n	A_l		A_i, A_m

Matrica e kontrollit të qasjes për BLP

- Supozojmë se kemi një BLP sistem me saktësisht 3 subjekte dhe 3 objekte me labelat e vijuese. Supozojmë poashtu se $H > L$.

Subjekti	**Niveli**	**Objekti**	**Niveli**
Subj_1	$(H, \{A, B, C\})$	Obj_1	$(L, \{A, B, C\})$
Subj_2	$(L, \{\})$	Obj_2	$(L, \{\})$
Subj_3	$(L, \{A, B\})$	Obj_3	$(L, \{B, C\})$

- Matrica përkatëse e kontrollit të qasjes është dhënë në vijim.

	Obj_1	Obj_2	Obj_3
Subj_1	R	R	R
Subj_2	W	R, W	W
Subj_3	W	R	$\varnothing$

Matrica e kontrollit të qasjes për BLP (Vazhdim)

- Sikur me secilën politikë të kontrollit të qasjes, do të mund të përkufizohej një ACM për një sistem të madh BLP. Sidoqoftë, matrica do të ishte tepër e madhe për shumicën e sistemeve realistike.
- Matrica në BLP është implicite në rregullat (siguria e thjeshtë dhe vetia *), kështu që lejimet e qasjes mund të kompjutohen aty për aty.

Mësime

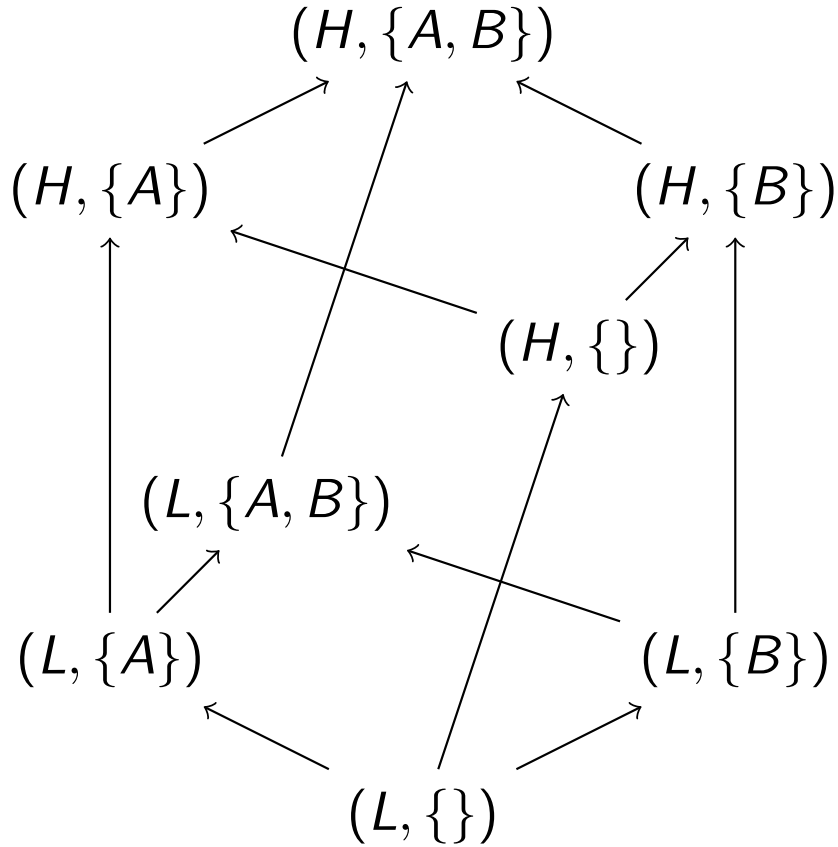
- BLP është një shembull i një klase politikash të quajtura *politika për kontroll të qasjes.*
- BLP është poashtu një shembull politike *mandatore* për faktin se rregullat zbatohen për çdo qasje të synuar.
- Çdo politikë e kontrollit të qasjes mund të modelohet si një matricë eksplicite (*ACM*).

Siguria mbështetur në grilë

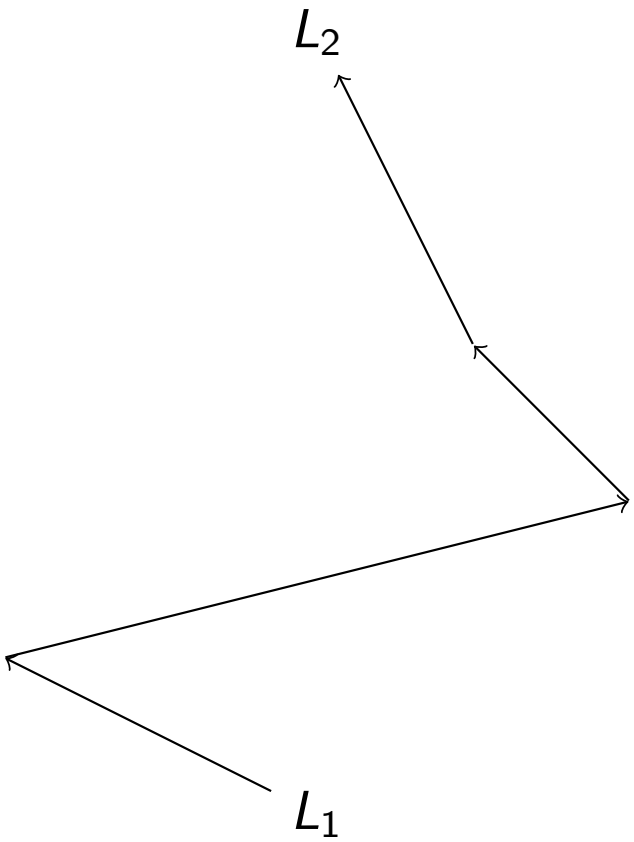
- Rikujtoni se bashkësia labelave në sistemin MLS formon një renditje parciale nën relacionin e dominimit. Vlejnë pohimet vijuese:
  - Çdo dy elemente kanë kufirin më të vogël të sipërm (supremum ose bashkim).
  - Çdo dy elemente kanë kufirin më të madh të poshtëm (infimum ose takim).
- Kështu, bashkësia e labelave formon një strukturë algjebrike të quajtur *grilë* (*lattice*).

Një grilë

- Supozojmë një sistem BLP me nivele kierarkike $\{H, L\}$ (me $H > L$) dhe kategori $\{A, B\}$.
- Në grafin e drejtuar që paraqet grilën rezultuese shigjetat paraqesin (disa nga) relacionet e dominimit ndërmjet labelave.
  - Në qoftë se në grafin ka ndonjë shteg prej L_1 në L_2, atëherë $L_1 \leq L_2$.
- Për ta thjeshtësuar, figura nuk përfshin shigjetat refleksive ose transitive.



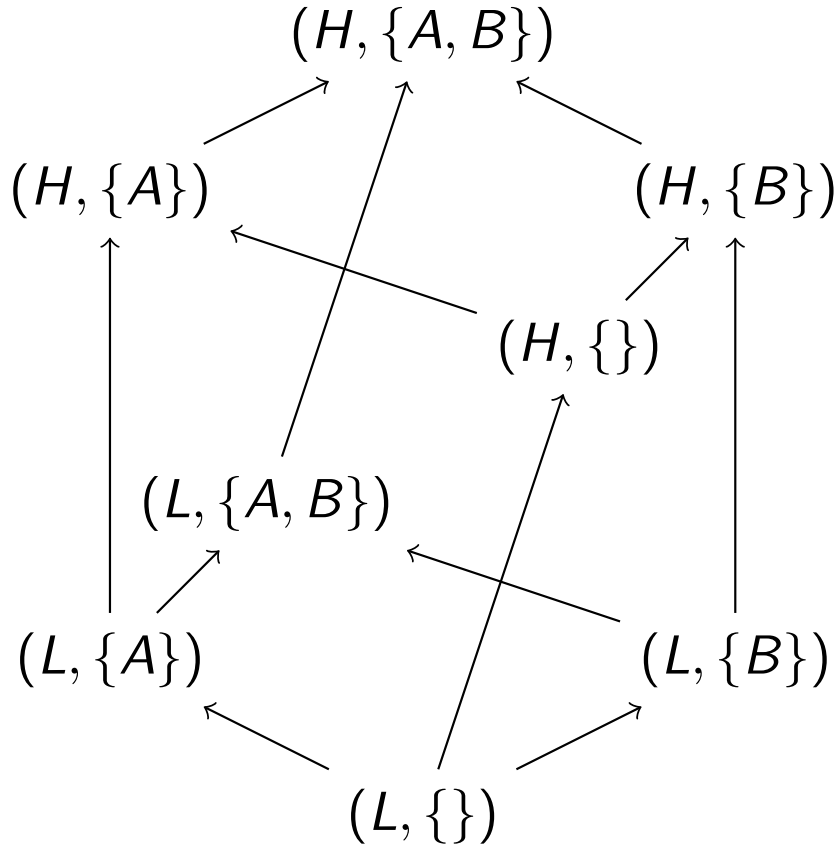
BLP metapolitika



- Një shteg në grafin prej L_1 në L_2 do të thotë se „informacioni lejohet të rrjedhë“ prej nivelit L_1 te niveli L_2.
- Kjo mund të ndodhë në njërën nga dy mënyrat:
  1. një subjekt i nivelit L_2 mund të lexojë një objekt të nivelit L_1, ose
  2. një subjekt i nivelit L_1 mund të shkruajë një objekt të nivelit L_2.
- Në qoftë se nuk ekziston shteg prej L_1 në L_2, atëherë siguria e thjeshtë ndalon 1 dhe vetia * ndalon 2.

Pra, cila është metapolitika?

- Rikujtoni se metapolitika është bashkësi qëllimesh kryesore të sigurisë të sistemit.
- Kështu, për çdo sistem Bell dhe LaPadula duam që informacioni të rrjedhë vetëm „përpjetë“ në grilën e niveleve të sigurisë.
  - Informacioni mund të rrjedhë prej L_1 në L_2 vetëm në qoftë se $L_2 \geq L_1$.
- Çfarëdo rrjedhe tjetër indikon shkelje të qëllimeve të sigurisë.



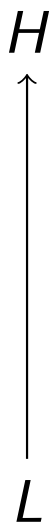
Qëllimi kryesor

- Metapolitika e një BLP sistemi është të krufizojë rrjedhën e informacionit ndërmjet niveleve të ndryshme.
- Rikujtoni se metapolitika është ajo për çfarë vertet brengosemi nga pikëvështrimi i sigurisë.
- Kështu në qoftë se mund të ndërtojmë një sistem i cili plotëson rregullat e BLP por prapseprap shkel metapolitikën, atëherë BLP rregullat duhet të mos mjaftojnë.

Mësime

- BLP është një bashkësi rregullash të kontrollit të qasjes: siguria e thjeshtë, vetia *, ndonjë version i qetësisë.
- Bashkësia e BLP labelave formon një grilë sipas relacionit të dominimit; politika e tillë është një instancë e *sigurisë së mbështetur në grilë.*
- Qëllimi kryesor i BLP (metapolitika) është të kufizohet rrjedha e informacionit ndërmjet niveleve të ndryshme të sigurisë brenda grilës.
- Metapolitika na ofron një menyrë për të vlerësuar se a e kryen punën mirë politika (rregullat e BLP).

A është BLP e sigurt?



- Shqyrtojmë grilën e thjeshtë të labelave në diagram, ku $H > L$. Nuk ka kategori duhet-ditur.
- Në qoftë se kjo paraqet një BLP grilë, atëherë rrjedha e informacionit është e lejuar prej L në H, por jo anasjelltas. Kjo është metapolitika e këtij sistemi të thjeshtë.
- Në qoftë se mund të instancojmë këtë sistem ashtu që plotësohet BLP, por rrjedha e informacionit të shkelë metapolitikën, atëherë diçka qartazi nuk shkon.

Një sistem i thjeshtë BLP

- Shqyrtojmë një sistem të thjeshtë që ka operacionet READ dhe WRITE me semantikat vijuese:
  - READ(S, O): në qoftë se ekziston objekti O dhe $L_S \geq L_O$, atëherë kthe vlerën e tij aktuale; përndryshe kthe zero.
  - WRITE(S, O, V): në qoftë se ekziston objekti O dhe $L_S \leq L_O$, atëherë ndrysho vlerën e tij në V; përndryshe bëj asgjë.
- Këto operacione janë qartazi instanca të pranueshme të operacioneve READ dhe WRITE për një BLP politikë.

Një sistem i thjeshtë BLP (Vazhdim)

- Supozojmë se dëshirojmë t'i shtojmë sistemit dy operacione të reja CREATE dhe DESTROY me semantikat vijuese:
  - CREATE(S, O): në qoftë se nuk ekziston kudo në sistemin objekt me emrin O, atëherë krijo një objekt O të ri në nivelin L_S; përndryshe bëj asgjë.
  - DESTROY(S, O): në qoftë se ekziston objekt me emrin O dhe $L_S \leq L_O$, atëherë shkatërro atë; përndryshe bëj asgjë.
- Këto operacione duket të plotësojnë rregullat e BLP, por a janë „të sigurta“ nga standardi i metapolitikës? Pse?

Shembull kanali të fshehur

- Në këtë sistem një subjekt me nivel të lartë S_H mund t'i sinjalizojë një bit informacion një subjekti me nivel të ultë S_L si vijon:

S_H transmeton 0	S_H transmeton 1
Create($S_H, F0$)	// Bëj asgjë
Create($S_L, F0$)	Create($S_L, F0$)
Write($S_L, F0, 1$)	Write($S_L, F0, 1$)
Read($S_L, F0$)	Read($S_L, F0$)
Destroy($S_L, F0$)	Destroy($S_L, F0$)

- Në rastin e parë, S_L sheh vlerën 0; në rastin e dytë S_L sheh vlerën 1.
- Kështu, S_H mund t'i sinjalizojë një bit informatë S_L duke ndryshuar sjelljen e tij.

Pa çka?

- Kujt i bëhet vonë në qoftë se një bit rrjedh tatpjetë?
  - Mjafton të tregohet se BLP nuk garanton që plotësohet metapolitika.
  - Në qoftë se S_L dhe S_H mund t'i koordinojnë aktivitetet e tyre S_H mund t'i transferojë sasi të çfarëdoshme informacioni S_L, për kohë të mjaftueshme.
- Në një politikë të kontrollit të qasjes si BLP objektet janë **të vetmet** entitete të pranuara për të bartur informacion.
- Për kanalin e mësipërm „informacioni“ nuk është përmbajtja e ndonjë objekti. Ai ndodhet në përgjegjjen e pyetjes: A mund S_L të lexojë një objekt të quajtur O?

Kanalet e fshehta

- Në qoftë se S_L **kurdoherë** sheh rezultate të ndryshueshme në varësi të akcioneve të ndryshueshëm të S_H, kjo do të mund të shfrytëzohej për të dërguar një bit inormacion prej S_H në S_L, gjë që shkel metapolitikën.
- Një mekanizëm i tillë quhet *kanal i fshehtë.*

Mësime

- Një politikë e kontrollit të qasjes kufizon rrjedhën e informacionit nga subjektet që lexojnë ose shkruajnë objektet.
- Mund të ekzistojnë tipare tjera të sistemit të cilat do të mund të manipuloheshin ashtu që të bartin informacion.
- Kanalet e tilla quhen *kanale të fshehta.*

Përkufizimi

Përkufizim (Kanal i fshehtë)

Kanal i fshehtë është një shteg për rrjedhje ilegale të informacionit ndërmjet subjekteve në një sistem, duke përdorur resurse të sistemit të cilat nuk ishin disenjuar për t'u shfrytëzuar për komunikim ndër subjektesh.

- Vëreni disa karakteristika të këtij përkufizimi:
  - Rjedhje informacioni që shkel metapolitikën e sigurisë **edhepse jo domosdoshmërisht politikën**
  - Rrjedhja është ndërmjet subjekteve brenda sistemit; dy shfrytëzues njerëz të cilët bisedojnë pranë kafesë nuk është një kanal i fshehtë
  - Rrjedhja ndodh përmes resurseve të sistemit (atributeve të fajlave, flamurëve, orëve, etj.) që nuk janë destinuar për kanale komunikimi.

Kanal i fshehtë 1

- Përpjekja e qasjes nga S_L një resursi të nivelit të lartë kthen njërin nga dy mesazhet e gabimit: `Resource not found` ose `Access denied`. Duke modifikuar statusin e resursit, S_H mund të dërgojë një bit informacion për çdo përpjekje qasjeje të S_L.
- Ky është një *kanal i fshehtë ruajtjeje,* sepse S_H regjistron informacion brenda gjendjes së sistemit.

Kanal i fshehtë 2

- Një sistem operativ mund të jetë implementuar ashtu që të izolojë proceset në makina virtuale të veçuara. Ato ndajnë procesorin në baza intervalesh kohore. Proceset alternohen duke shfrytëzuar CPU-në ashtu që secilit i lejohen t njësi të kohës procesorike. Sidoqoftë, një proces mund të lirojë CPU-në para kohe.
- Një proces p mund t'i dërgojë një bit informacion një procesi q ose duke shfrytëzuar alokimin e vet total ose duke liruar procesorin menjëherë. Procesi q mund të lexojë bitin duke konsultuar orën sistemore për të parë sa kohë ka kaluar nga orari i tij i fundit.
- Ky është një *kanal i fshehtë kohe* sepse informacioni është regjistruar në renditjen ose kohëzgjatjen e ngjarjeve në sistemin.

Kanal i fshehtë 3

- Proceseve p dhe q nuk u lejohet të komunikojnë, por ata ndajnë qasjen të njëjtit disk drajv. Algoritmi skenues servison kërkesat sipas renditjes së cilindrit që aktualisht është më i afërti kokës për lexim.
- Një proces p ose i qaset cilindrit 140 ose 160. Një proces q kërkon qasje cilindrave 139 dhe 161. Kështu q merr vlerat nga 139 dhe pastaj 161, ose nga 161 dhe pastaj 139, varësisht nga leximi më i fundit i p.
- A është ky një kanal i fshehtë ruajtjeje apo kohe?

Kanal i fshehtë 4

- Një *kanal i fshehtë implicit* është ai i cili shfrytëyon rrjedhën e kontrollit të një programi. Për shembull, shqyrtoni fragmentin vijues të një programi:

  $h := h \bmod 2;$
  $l := 0;$
  if $h = 1$ **then**
  $l := 1;$
  end if

- Vlera rezultuese e l varet nga vlera e h.
- Ekzistojnë vegla të sofistikuara për rrjedhë informacioni për gjuhë të veçanta të cilat kontrollojnë këto lloj varësish në gjuhë prorgamuese.

Tipet e kanaleve të fshehta

- Mund të dallohen shumë tipe kanalesh të fshehta, varësisht nga atributi i manipuluar:
  - *Kohe:* sa kohë i është nevojitur një kompjutimi?
  - *Implicite:* çfarë rrjedhe kontrolli merr një program?
  - *Terminimi:* a terminohet një kompjutim?
  - *Probabiliteti:* çfarë është distribuimi i ngjarjeve të sistemit?
  - *Të shterrimit të resurseve:* a është ndonjë resurs i pamjaftueshëm?
  - *Fuqie:* sa energji konsumohet?
- Në praktikë, shumë kërkues dallojnë vetëm kanale të fshehta ruajtjeje dhe kohe.

Mësime

- Kanal i fshehtë është çdo shteg informacioni ndërmjet subjekteve i cili përdor resurse të sistemit të cilat muk ishin të disenjuara për t'u shfrytëzuar për komunikim ndër subjektesh.
- Një dallim i dobishëm është ndërmjet kanaleve të fshehta të ruajtjes dhe atyre të kohës, edhepse klasifikimi jo gjithmonë është i qartë për kanale specifike.

Pa çka? (Vazhdim)

- Rikujtoni përkufizimin e një kanali të fshehtë.
- Mund të kemi përshtypjen se kanalet e tilla do të ishin aq të ngadalshme saqë nuk na bëhet vonë për to.
- **Një gjë e tillë nuk është e vërtetë.** Kanalet e fshehta në procesorë realë operojnë në mijëra bit për sekond, pa ndonjë ndikim të ndieshëm në procesimin e sistemit.

Kanalet e fshehta (Vazhdim)

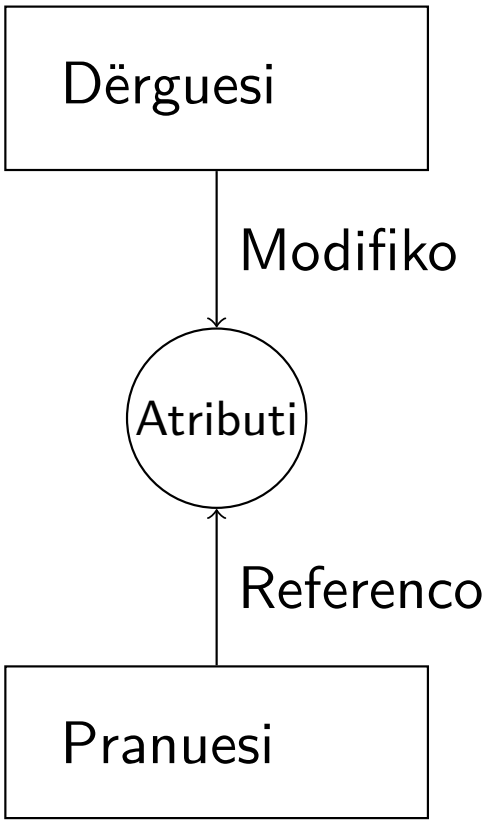
- Karakterikstika të rëndësishme të një kanali të fshehtë janë:
  - *Ekzistenca:* a është kanali prezent apo jo?
  - *Gjerësia e brezit:* sa informacion mund të transmetohet për sekond?
  - *Zhurma:* a mund të transferohet informacioni pa humbje ose shtrembërim?
- Zakonisht është e pamundur për sistem realistike që të eliminohen të gjithë kanalet e fshehta potenciale.

Ballafaqimi me kanale të fshehta

- Pasi të jetë identifikuar një kanal i fshehtë janë të mundura disa përgjegjje:
  - Të eliminohet duke modifikuar implementimin e sistemit
  - Të reduktohet gjerësia e brezit duke futur zhurmë në kanalin
  - Të monitorohen për shabllonat e përdorimit të tij të cilët indikojnë se është duke u përpjekur ta shfrytëzojë.
    - Kjo quhet *detektim i ndërhyrjes* (*intrusion detection*).

Shfrytëzimi i një kanali të fshehtë ruajtjeje

- Çfarë duhet të vlejë ashtu që një dergues dhe një pranues të shfrytëzojnë një kanal të fshehtë ruajtjeje?
  - Të dytë, dërguesi dhe pranuesi, duhet të kenë qasje në ndonjë atribut të një objekti të ndarë.
  - Dërguesi duhet të jetë në gjendje të modifikojë atributin.
  - Pranuesi duhet të jetë në gjendje të referencojë (shohë) atë atribut.
  - Duhet të ekzistojë një mekanizëm për inicializimin e të dyja proceseve dhe për sekuencializimin e qasjeve të tyre në resursin e ndarë.



Shfrytëzimi i një kanali të fshehtë kohe

- Që një dergues dhe një pranues të shfrytëzojnë një kanal të fshehtë kohe duhet të vlejë si vijon:
  - Të dytë, dërguesi dhe pranuesi, duhet të kenë qasje në ndonjë atribut të një objekti të ndarë.
  - Të dytë, dërguesi dhe pranuesi, kenë qasje në referencë kohore (orë sistemore, tajmer, renditje ngjarjesh).
  - Dërguesi duhet të jetë në gjendje të kontrollojë tempimin e detektimit të një ndryshimi në atributin e pranuesit.
  - Pranuesi duhet të jetë në gjendje të referencojë (shohë) atë atribut.
  - Duhet të ekzistojë një mekanizëm për inicializimin e të dyja proceseve dhe për sekuencializimin e qasjeve të tyre në resursin e ndarë.

Mësime

- Karakteristika të rëndësishme të një kanali të fshehtë janë: ekzistenca, gjerësia e brezit, zhurma.
- Ballafaqimi me kanale të fshehta mund të përfshijë: eliminimin, kufizimin e gjerësisë së brezit, monitorimin.
- Duhet të plotësohen disa kushte për ekzistencën e një kanali të fshehtë.

Detektimi i kanaleve të fshehta të ruajtjes

- *Metodologjia e resurseve të ndara* (*Shared Resource Matrix Methodology, SRMM*): Ndërtohet një tabelë e cila përshkruan komandat e sistemit dhe efektin e tyre potencial në atributet e ndara të objekteve.

	READ	WRITE	DESTROY	CREATE
ekzistenca e fajlit	R		M	M
madhësia e fajlit	R	M	M	M
niveli i fajlit	R		M	M

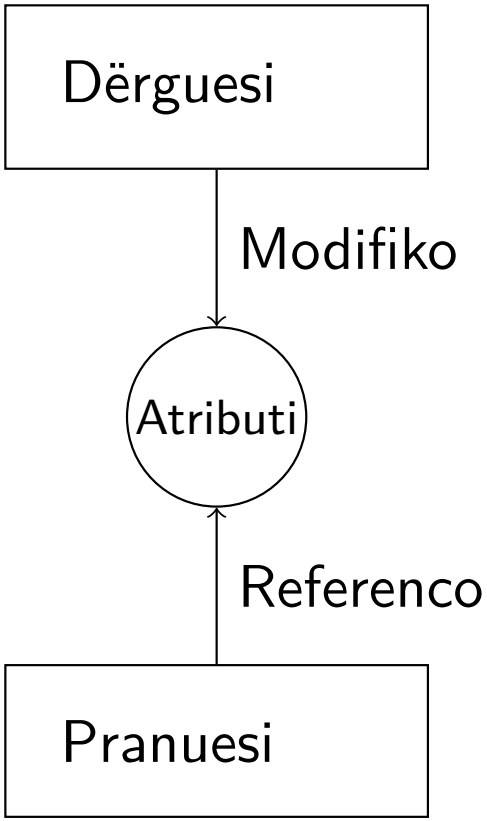
- R ka kuptimin se operacioni referencon (jep informacion mbi) atributin **nën ndonjë rrethanë.** M ka kuptimin se operacioni modifikon atributin **nën ndonjë rrethanë.**
- Vëreni se një gjë e tillë funksionon për kanale të fshehta ruajtjeje por jo edhe për kanale të fshehta kohe.

Një hollësi e SRMM

- Supozojmë se kemi operacionin vijues:
  - CREATE(S, O): në qoftë se nuk ekziston kudo në sistemin objekt me emrin O, atëherë krijo një objekt O të ri në nivelin L_S; përndryshe bëj asgjë.
- Për atributin **ekzistenca e fajlit**, a duhet apo jo të vejmë R për këtë operacion? Keni parasysh: pas këtij operacioni **dijmë** se fajli ekziston. Pse?
- Kjo nuk mjafton. Nuk është e rëndësishme që **dijmë** diçka mbi atributin; çfarë është e rëndësishme është që operacioni të na **thotë** diçka mbi atributin.

Puna me SRMM

- Në qoftë se R dhe M paraqiten në të njëjtin rresht, kjo indikon një kanal të fshehtë **potencial.** Pse?
- SRMM nuk i identifikon kanalet e fshehta, pro sygjeron ku të kërkohen ato.
- Çdo matricë e resurseve të ndara është **për një sistem specifik.** Sistemet tjera mund të kenë semantika tjera për operacionet.



Kanalet e fshehta dhe analiza e sistemit

- Si mund të përdoret kjo metodologji?
  1. Përdor një politikë të kontrollit të qasjes, si BLP, për të kontrolluar rrjedhat standarde të informacionit.
  2. Përdor një teknikë të veçantë, si SRMM, për të identifikuar kanalet e fshehta.
  3. Ballafaqohu me kanalet e fshehta duke i mbyllur, kufizuar ose monitoruar ato.

Mësime

- Metodologjia e matricës së resurseve të ndara ofron një mënyrë sistematike për të investiguar kanalet e fshehta potenciale.
- Mirëpo, shfrytëzimi efektiv i saj kërkon shumë njohuri mbi semantikën dhe implementimin e operacioneve sistemore.
- Analiza e kanaleve të fshehta mund të përdoret për të mbyllur disa nga vrimat e sigurisë të një politike të kontrollit të qasjes si BLP.