Politikat dhe metapolitikat

Qëllimet dhe objektivat

- Metapolitikat dhe politikat si maneifestim i tyre
- MLS si një shembull politike
- Nivelet e sensitivitetit dhe nivelet e autorizimit
- Relacioni i dominimit ndërmjet niveleve
- Qasja e leximit dhe qasja e shkrimit

Përmbajtja

Si e përkufizojmë sigurinë

- Në kapitullin e parë thamë se, në termat më të përgjithshëm, *siguria* duket se ka kuptimin e diç si „mbrojtjes së asesteve kundrejt kërcënimeve“.
- Por kjo çështje është shumë specifike për kontekstin. Siguria është shumë e ndryshme për:
  - një sistem telefoni pa tela
  - një sistem baze të dhënash ushtarake
  - një sistem banke online
- Në qoftë se këto kanë nocione të ndryshme përkatëse sigurie, si specifikohen kërkesat e sigurisë për një sistem të dhënë.

Politikat

- Shpesh, siguria për një sistem të dhënë definohet në terma të një *politike sigurie.*
- *Politikë* është një bashkësi rregullash për implementim të qëllimeve specifike të sigurisë.
- Një mënyrë tjetër për ta menduar është si kontratë ndërmjet disenjuesit/implementuesit të sistemit dhe shfrytëzuesit. Ajo duhet të jetë si e arritshme (e mundur për t'u përcjellur) ashtu edhe adekuate për qëllimet e synuara.

Eksperiment mental

- **Regjistrimet akademike të studentëve ruhen në kompjuterë në universitet. Disenjoni një politikë sigurie për t'i mbrojtur.**
- Do të mund të fillonit duke bërë pyetjet:
  1. Ç'do të thotë „për t'i mbrojtur“?
  2. Cilat janë kërcënimet potenciale?
  3. Cilat nga aspektet vijuese janë të rëndësishme këtu: konfidencialiteti, integriteti, dispozicioni?
     - Po autorizimi dhe mos hedhja poshtë?
  4. Kush janë palët e interesuara, d.m.th. interesat e kujt rrezikohen?
  5. A ka konflikt ndërmjet intereseve të tyre? Si zgjidhen këto konflikte interesash?

Vlerësimi i një politike

- Në qoftë se një politikë është një bashkësi rregullash, si vendosim nëse ato janë bashkësia e duhur e rregullave?
- Një bankë do të mund të kishte të vendosur një politikë me bashkësine vijuese të rregullave, ndërmjet tjerash:
  1. Stafi nuk mund të përdorë numrat e kontove bankiere të klientëve në dokumente/fajla/postime.
  2. Dokumentet që përmbajnë numra kontosh bankiere duhet të shkatërrohen përveç në qoftë se konsiderohen të domosdoshëm.
  3. Dokumentet që përmbajnë numra kontosh dhe që konsiderohen të domosdoshme për mbajtje duhet të mbahen në ruajtje të sigurt.
- Këto rregulla kanë kuptim vetëm në shërbim të një qëllimi më të madh.
  - Cili është ky?

Metapolitika kundrejt politikës

- Një dallim i dobishëm ndërmjet *metapolitikës* dhe politikës:
  - *Metapolitikë:* Qëllimet kryesore të sigurisë të sistemit.
  - *Politikë:* Rafinim specifik për sistemin i metapolitikës adekuat për të ofruar udhërrëfim për zhvilluesit dhe shfrytëzuesit e sistemit.
- Në qoftë se nuk e kuptoni metapolitikën, bëhet e vështirë për justifikuar dhe vlerësuar politikën.
- Shpesh metapolitika do të jetë në terma konfidencialiteti, integriteti dhe dispozicioni.
- Politika do të jetë në terma mekanizmash, si firewall-ë, enkriptim, sirtarës të mbyllur etj.
- Politika është manifestim i metapolitikës.

Pra pse ka politikë?

- Në qoftë se e tëra që na intereson është metapolitika, atëherë pse të merremi fare me politikën?
  1. Metapolitika është shpesh tepër e përgjithshme për të ofruar udhërrëfyes adekuat.
  2. Metapolitika mund të jetë subjekt interpretimesh të shumëfishta.
  3. Mund të ketë politika të shumëfishta të pranueshme që arrijnë qëllimet e sigurisë (të definuara me të njëjtën metapolitikë).
  4. Politika ofron udhëzuesë specifik dhe të imponueshëm për shfrytëzues/zhvillues të sistemit.

Mësime

- Siguria e një sistemi shpesh karakterizohet me anë të një *politike sigurie*, bashkësi rregullash që qeveris me aktivitetet përbrenda sistemit.
- Politika do të duket arbitrare në qoftë se nuk e kuptoni *metapolitikën*, qëllimet gjithëpërfshirëse të sigurisë.

Siguria shumënivelëshe (Multi-level security, MLS)

- Një problem i hershëm sigurie ishte mbrojtja e *konfidencialitetit* brenda një mjedisi ushtarak.
- *Për informacion nivelesh të ndryshme sensitiviteti dhe individë shkallësh të ndryshme besueshmërie, si të kontrollohet qasja informacionit përbrenda sistemit ashtu që të mbrohet konfidencialiteti?*
- Ky problem quhet *Siguria shumënivelëshe (Multi-level security, MLS)* dhe është më i vjetër sesa kompjuterët.

Eksperiment mental MLS

- **Rrethina:** Zyra e Gjeneralit Eisenhower në Europën e v. 1943. Supozoni një rrethinë në të cilën ka
  - *informacion* nivelesh të ndryshme „ndjeshmërie“: plani i luftës, buxheti i mbrojtjes, orari i lojtarëve të bejsbolit, menyja e kafeterisë etj;
  - *individë* që u lejohet qasja pjesëve të zgjedhura të informacionit: Gjen. Eisenhower, ushtarët, kolonelët, sekretarët, shtëpiakët, spiunët etj.
- **Qëllimi:** Kupto çfarë kuptimi do të mund të kishte „siguria“ në këtë kontekst dhe defino një politikë (disa rregulla) për ta implementuar atë.

Vlerësimi i riskut

- **Pyetje:** Çfarë jemi duke mbrojtur? Kundrejt cilave kërcënime?
- **Përgjegjja:** Konfidencialitetin e informacionit – asnjë person i paautorizuar për ta parë një pjesë informacioni nuk mund të ketë qasje në të.
- **Udhëzim shumë i rëndësishëm:** Për këtë eksperiment mental na intereson vetëm *konfidecialiteti,* jo edhe integriteti dhe dispozicioni.

Pyetje mbi konfidencialitetin

- Rikujtoni pyetjet relevante për shqyrtimin e një politike konfidencialiteti:
  - A janë të gjitha të dhënat e mia njësoj të ndieshme? Nëqoftë se jo, si i grupoj dhe kategorizoj të dhënat?
  - Si e karakterizoj kush është i autorizuar dhe çfarë të shohë?
  - Si administrohen dhe kontrollohen autorizimet? Sipas cilave rregulla?
  - A ndryshojnë autorizimet gjatë kohës?

Kategorizimi i të dhënave

- Në zyrën e Gjen. Eisenhower, „hapësira“ relevante e informacionit përmban shumë atome individuale ose faktoide:
  1. Ekipi i bejzbolit ka lojë nesër në orën 15.
  2. Invasioni i Normandisë është caktuar me 6 qershor.
  3. Kafeteria shërben stek viçi dhe tost sot.
  4. Kol. Jones sapo i është rritur paga.
  5. Kol. Smith nuk i është rritur paga.
  6. Britanikët i kanë thyer kodet e Enigmës gjermane.
  7. ...
- Jo i tërë informacioni është njësoj i ndieshëm. *Si e grupojmë dhe e kategorizojmë informacionin në mënyrë të arsyeshme?*

Labelat e sensitivitetit të objektit

- Informacioni parcializohet në kontejnerë të ndarë (dokumente/folderë/objekte/fajla) të etiketuar sipas shkallës së tyre të ndieshmërisë.
- Një pjesë e labelës merret nga një bashkësi linearisht e renditur: **I paklasifikuar, Konfidencial, Sekret, Shumë Sekret.**
- Ekzistojnë poashtu edhe kategori „duhet-ditur“, nga një bashkësi jo e renditur, që shprehim përkatësi ndonjë grupi iteresi, p.sh. **Kripto, Nuklear, Mirëmbajtje, Personel,** etj.

Labelat e sensitivitetit (Vazhdim)

- Idealisht, labela në cilindo folder reflekton ndieshmërinë e informacionit që përmbahet brenda atij folderi. Labela përmban të dyja: një komponentë kierarkike dhe një bashkësi kategorish.
- Për shembull, dy dokumente mund të kenë labelat:

  (Sekret: {Nuklear, Kripto}),
  (Shumë Sekret: {Kripto}).

- Mund të konkludohet se i pari përmban informacion paksa sensitiv që ka të bëjë me kategoritë Nuklear dhe Kripto. I dyti përmban informacion shumë sensitiv në kategorinë Kripto.
- Këto vendime etiketimi i sjell ndonjë oficer sigurie. Si sillen këto është jashë skopit të interesimit tonë.

Informacioni i përzier

- **Pyetje:** Si etiketohet një dokument që përmban „informacion të përzier“?
  - Supozoni se dokumenti përmban edhe informacion sensitiv edhe josensitiv.
    - *Përdor nivelin më të lartë përkatës.*
  - Supozoni se dokumenti përmban informacion relevant edhe për domenin Kripto edhe për atë Nuklear.
    - *Përdor të dyja kategoritë.*
- **Mbi ndryshimin gjatë kohës:** Ndonjëherë sillet vendim që klasifikimi i një dokumenti duhet të ndryshojë. Kjo quhet *ulje* (ose *ngritje*) *klasifikimi.*

Mësime

- Për shembullin tonë MLS, parcializuam informacionin në kontejnerë dhe ofruam labela që relfektojnë sensitivitetin e informacionit.
- Labelat janë të strukturuara, me një komponentë kierarkike dhe një bashkësi kategorish duhet-ditur.
- Një folder me informacion „të përzier“ dhet të etiketohet ashtu që të mbrohet informacioni në nivelin më të lartë të mundshëm kierarkik dhe të mbrohen të gjitha kategoritë e informacionit.

Nivelet e autorizimit

- Le t'i shoqërojmë individëve *nivele autorizimi*, të të njëjtës formë sikurse të niveleve të sesitivitetit të dokumentit.
- Kështu, secili individ ka:
  - një nivel kierarkik sigurie i cili indikon nivelin e besueshmërisë i cili i është lejuar atij;
  - një bashkësi kategorish duhet-ditur që indikojnë domenin e interesit në të cilin ai është i autorizuar të operojë.
- Vërejmë se labelat në dokumente indikojnë sensitivitetin e informatës që përmbahet; „labelat“ në njerëz indikojnë klasat e informacionit që personi është i autorizuar t'u qaset.

Privilegji më i vogël

- Kategoritë duhet-ditur janë refleksion i faktit se edhe brenda një niveli të dhënë sigurie (sikur **Shumë Sekret**) jo çdonjëri nevojitet të dijë çdo gjë. Kjo është një instancë e parimit të privilegjës më të vogël.
- *Parimi i privilegjës më të vogël:* Çdo subjekt duhet pasur qasje në sasinë **minimale** të informacionit të nevojshme për ta kryer punën e vet.
- Parimi i privilegjit më të vogël mund të konsiderohet aksiomë e sigurisë.
  - Pse është i arsyeshëm? Numëroni disa arsye.

Po tani?

- **Pyetje:** Meqë kemi labela për dokumente dhe autorizime për njerëz, si vendosim cilëve njerëz u lejohet qasja në cilët dokumente?
- **Përgjegjja:** Sigurisht që ekziston ndonjë relacion ndërmjet nivelit të subjektit dhe nivelit të objektit. Por çfarë?
- A duhet një njeri me autorizimin e dhënë të jetë në gjendje të lexojë një dokument me sensitivitetin e dhënë?

Autorizimi	Sensitiviteti	Qasja
(Sekret: {Kripto})	**(Konfidencial: {Kripto})**	Po?
(Sekret: {Kripto, Nuklear})	**(Shumë Sekret: {Kripto})**	Jo?
(Sekret: {Nuklear})	**(I paklasifikuar: {})**	Po?

Mësime

- Për të kontroluar qasjen dokumenteve/folderëve nga individë, na nevojiten „labela“ për dytë.
- Për dokumentet labelat indikojnë sensitivitetin e informacionit që përmbajnë.
- Për individët labelat indikojnë autorizimin për të parë klasa të caktuara të informacionit.
- Një individi duhet t'i jepet autorizimi minimal për të performuar punën me të cilën është ngarkuar (privilegji më i vogël).
- Se a duhet një individ të shohë një dokumet specifik varet nga relacioni ndërmjet labelës së dokumentit dhe autorizimit të individit.

Terminologji

- Në tipin e politikës së sigurisë që jemi duke konstruktuar, termat vijues përdoren shpesh:
  - *Objekte:* kontejnerët e informacionit të mbrojtur nga sistemi (dokumente, folderë, fajla, direktoriume, baza të dhënash etj.).
  - *Subjekte:* entitete (shfrytëzues, procese etj.) që ekzekutojnë aktivitete dhe kërkojnë qasje objekteve.
  - *Aksione:* operacione, primitive ose komplekse, të ekzekutuara në emër të subjekteve që mund t'i ndikojnë objektet.
- Subjektet në shembullin tonë MLS janë njerëzit, objektet janë folderat që pëermbajnë informacion, aksion është shikimi i objekteve.

Relacioni: dominon

- Për një bashkësi labelash sigurie (L, C), të përbëra nga nivele kierarkike dhe kategori, përkufizojmë një relacion renditjeje ndërmjet labelave.

Përkufizim

Labela e sigurisë (L_1, C_1) *dominon* labelën e sigurisë (L_2, C_2) në qoftë se

1. $L_1 \geq L_2$ sipas renditjes së niveleve dhe
2. $C_2 \subseteq C_1$.

Shënojmë $(L_1, C_1) \geq (L_2, C_2)$.

- Vëreni se renditja e përkufizuar kështu është një *renditje parciale,* e jo renditje lineare.
  - D.m.th., ekzistojnë labela sigurie A dhe B të tilla që nuk është as $A \geq B$ as $B \geq A$.

Shembull dominimi

- Në tabelën vijuese për cilat çifte labela 1 dominon labelën 2?

Labela 1	Labela 2	Dominon?
(Sekret: {Kripto})	**(Konfidencial: {Kripto})**	Po
(Sekret: {Kripto, Nuklear})	**(Shumë Sekret: {Kripto})**	Jo
(Sekret: {Nuklear})	**(I paklasifikuar: {})**	Po

Veti e sigurisë së thjeshtë

- Vetia vijuese duket ta kapë intuitën tonë se kur një subjekt mund të lexojë një objekt.

Teoremë (Vetia e sigurisë së thjeshtë)

*Kusht i nevojshëm që një subjekti S me autorizim (L_S, C_S) t'i lejohet qasje **leximi** një objekti O me klasifikim sensitiviteti (L_O, C_O) është që $(L_S, C_S) \geq (L_O, C_O)$.*

- A mund të thoni pse është vetëm „kusht i nevojshëm“ e jo edhe „kusht i mjaftueshëm“?
- Në terma operacionalë, një individ që kërkon të shohë një dokument është e nevojshme të tregojë se niveli i tij i autorizimit *dominon* nivelin e ndieshmërisë së dokumentit.

Mësime

- Relacioni i dominimit formalizon relacionin ndërmjet cilave do dy labela sigurie.
- Vetia e sigurisë së thjeshtë tregon si të përdoret dominimi për të vendosur se a duhet të lejohet qasja e leximit.

A na duhet shkrim i sigurt?

- A është vetia e sigurisë së thjeshtë e tëra që na duhet? Si qëndron puna me llojet tjera të qasjes?
- Vetia sigurisë së thjeshtë kodifikon restrikcionet për qasje *leximi.* Po qasja *e shkrimit?*
- Supozojmë se dikush me qasje një dokument Shumë Sekret kopjon informatën në një fletë dhe e vë në një folder Të Paklasifikuar.
  - A është cenuar vetia e sigurisë së thjeshtë? **Jo!** A është cenuar konfidencialiteti? **Qartazi.**

Shkrimi i sigurt

- Në përgjithësi, subjektet në botën e dokumenteve ushtarake janë **persona** të besueshëm që të mos shkruajnë informacion të kalsifikuar aty ku mund të qaset nga palë të paautorizuara.
- Subjektet në botën e kompjutimit janë shpesh **programe** që operojnë në emër të një shfrytëzuesi të besueshëm (dhe me autorizimin e tij).
- Ndonjë program që ekzekuton një shfrytëzues mund të ketë të futur përbrenda kod malicioz (një „kalë troje“ ("trojan horse")) që e bën programin të „rrjedhë“ informacion pa dijen dhe pëlqimin e shfrytëzuesit.

Vetia *

- Kufizojmë qasjen për shkruarje sipas vetisë vijuese:

Teoremë (Vetia *)

*Kusht i nevojshëm që një subjekti S me autorizim (L_S, C_S) t'i lejohet qasje **shkrimi** një objekti O me klasifikim sensitiviteti (L_O, C_O) është që $(L_S, C_S) \leq (L_O, C_O)$.*

- Si ndihmon vetia *?

Vetia * (Vazhdim)

- A është e arsyeshme kjo veti? Mos është tepër restriktive? Mos është tepër lejuese?
  - A mundet një gjeneral komandues me autorizim Shumë Sekret t'i dërgojë me email urdhërat e marshimit një ushtari këmbsorie pa autorizim?
    - Jo!
  - A mundet një dhjetar pa autorizim ta mbishkruajë planin e luftës?
    - Asgjë në rregullat e politikës që formuluam nuk e ndalon, por ky është një problem integriteti!
- Siguria e thjeshtë dhe vetia * ndonjëherë karakterizohen si „lexo tatpjetë“ dhe „shkruaj përpjetë“, respektivisht.
  - Ose, në mënyrë alternative, karakterizohen si „mos lexo përpjetë“ dhe „mos shkruaj tatpjetë“.

Mësime

- Për të shmangur shkeljet e konfidencialitetit nevojitet kontrol mbi operacionet **e leximit** dhe **shkrimit.**
- Vetia * shfrytëzon dominimin për të vendosur se a duhet lejuar qasje shkrimi.
- Kontroli i qasjese së shkrimit është sidomos i rëndësishëm për kompjuterë sepse subjekti mund të jetë një **program** që ekzekutohet në emër të një shfrytëzuesi. Shfrytëzuesi është autorizuar; programi jo.

Ndryshimi i labelave

- Siguria e thjeshtë dhe vetia * u kufizojnë subjekteve qasjen objekteve sipas relacioneve ndërmjet labelave të tyre. Por, çfarë nëse labelat mund të ndryshojnë?
- Supozoni se disi mund të ndryshoni labelën e një objekti nga

  (Shumë Sekret: {Kripto})

  në

  (I paklasifikuar: {})

  pavarsisht nga përmbajtja e objektit.
  - Kjo do të shkelte qartazi konfidencialitetin.
- Rregullat tona të deritanishme nuk e ndalojnë një gjë të tillë.

Vetitë e qetësisë

- Qartazi, na duhet një rregull shtesë që qeverisë me ndryshimin e labelave. Do të mund të zgjedhnim njërën nga vijueset:

Teoremë (Vetia e fortë e qetësisë)

Subjektet dhe objektet nuk i ndryshojnë labelat gjatë jetës së sistemit.

Teoremë (Vetia e dobët e qetësisë)

Subjektet dhe objektet nuk i ndryshojnë labelat në mënyrë që shkelë „frymën“ e politikës së sigurisë.

- A janë këto të dobishmë? A janë tepër kufizuese? Çfarë në qoftë se një shfrytëzuesi i duhet të operojë në nivele të ndryshme gjatë një ditë?

Vetia e dobët e qetësisë

Teoremë (Vetia e dobët e qetësisë)

Subjektet dhe objektet nuk i ndryshojnë labelat në mënyrë që shkelë „frymën“ e politikës së sigurisë.

- Çfarë është domethënia e saj?
  - Supozoni se sistemi përfshin një komandë për të ulur nivelin objektit në mënyrë të pakufizuar. A i cenon kjo qëllimet e sigurisë së thjeshtë ose vetisë *?
  - Supozoni se sistemi përfshin një komandë për të ngritur nivelin objektit në mënyrë të pakufizuar. A i cenon kjo qëllimet e sigurisë së thjeshtë ose vetisë *?
  - Po subjektet? A mund të ndryshojnë nivelet e tyre përpjetë ose tatpjetë.

Bell dhe LaPadula

- Vetia e sigurisë së thjeshtë, vetia * dhe vetia qetësisë formalizojnë një pjesë të madhe të sigurisë shumënivelëshe (MLS).
- Ky formalizim është bërë nga D. Elliott Bell dhe Len LaPadula (1975) dhe quhet *modeli i Bell dhe LaPadula (BLP).*
- Përkundër moshës, BLP është shtyllë e sigurisë moderne kompjuterike dhe akoma shfrytëzohet shumë gjerë si politikë sigurie.

Mësime

- Aftësia për të ndryshouar labelat arbitrarisht mund të shkatërrojë sigurinë, prandaj na duhet një veti *qetësie* për t'u ballafaquar me këtë kërcënim.
- Vetia e sigurisë së thjeshtë, vetia * dhe vetia qetësisë së bashku formojnë bazën e *modelit Bell dhe LaPadula (BLP)* të sigurisë.
- BLP është model i shfrytëzuar gjerë për sigurinë shumënivelëshe.