Integriteti

Qëllimet dhe objektivat

- Domethënia dhe parimet themelore të integritetit si aspekt i sigurisë së kompjuterëve
- Dallimet dhe qasjet e përbashkëta ndërmjet konfidencialitetit dhe integritetit
- Metapolitika e integritetit
- Modelet e Biba-s si politika të integritetit

Përmbajtja

Kuptimi i sigurisë së kompjuterëve

- Rikujtoni se siguria e kompjuterëve është përshkruar të përbëhet së paku nga
  - *Konfidencialiteti:* kush mund **të lexojë** informacion?
  - *Integriteti:* kush mund **të shkruajë** ose **të modifikojë** informacion?
  - *Dispozicioni:* çfarë mekanizmash sigurojnë që resurset janë në dispozicion kur të nevojiten?
- Modelet e konfidencialitetit, si BLP, janë të dobishme por qartazi të kufizuara.
- **Si mund t'i zgjerojmë modelet e shqyrtuara për të trajtuar çështjet e integritetit?**

Integriteti

- Integriteti është nocion më i paqartë dhe më i varur nga konteksti sesa konfidencialiteti.
  - Kush është i autorizuar të furnizojë dhe të modifikojë të dhëna?
  - Si të parcializohen dhe të mobrohen asetet?
  - Si të detektohen dhe/ose të korrigjohen ndryshimet e gabuara ose të paautorizuara të të dhënave?
  - A mund të ndryshojnë autorizimet gjatë kohës?
- Për dallim nga konfidencialiteti, **një program mund të dëmtojë integritetin pa interaksion me botën e jashtme, thjesht duke kompjutuar të dhëna në mënyrë jokorrekte.**

Eksperiment mental mbi integritetin

- Supozoni se jeni duke blerë në shitore dhe në standin ngjitur vëreni titullin: „Jashtëtokësoret u zbarkuan në disa metropola botërore". **A i besoni?**
- Reaksioni juaj mund të jetë i ndryshëm varësisht se a është publikimi në:
  1. **The New York Times:** Uau! A është e mundur të ketë ndodhur?
  2. **The Wall Street Journal:** Konspiratorët djathtistë përpiqen sërish të shesin armë!
  3. **Koha ditore:** Qartazi e kanë sajuar!
- Çfarë ndryshon në të tria rastet?
  - Vlerësimi juar mbi **inegritetin** e burimit

Labelat e integritetit

- Sikur që vepruam me konfidencialitetin, mund të shoqërojmë *labela integriteti:*
  - Labela e një *objekti* karakterizon shkallën e „besueshmërisë“ së informacionit që përmbahet në atë objekt.
    - Thashethëmet e dëgjuara në treg duhet të kenë kredibilitet më të ulët sesa një raport nga një panel ekspertësh.
  - Labela e një *subjekti* karakterizon besueshmërinë në aftësinë e tij për të prodhuar/përpunuar informacion.
    - Një aplikacion i çertifikuar mund të ketë më tepër integritet sesa një freeware i shkarkuar nga Interneti.

Disa parime të integritetit

- Intuitivisht, integriteti ka të bëjë me atë **sa i beson një entiteti të prodhojë, mbrojë ose modifikojë të dhëna.**
- Integriteti ka aspekte dhe parime të operimit jo aq relevante me sigurinë shumënivelëshe (MLS):
  - *Separimi i detyrës:* disa subjekte **të ndryshme** duhet të përfshihen për të kompletuar një funksion kritik.
  - *Separimi i funksionit:* një subjekt i vetëm nuk mund të kompletojë role komplementare brenda një procesi kritik.
  - *Auditimi:* rikuperimi dhe dhe llogaridhënia kërkojnë mbajtjen e një gjurme auditimi.
- Shpesh kontrollet komerciale të sigurisë janë diskrecionale, procedurale dhe të decentralizuara para se mandatore dhe të centralizuara.

Çështje komerciale

- Në rrethina komerciale çështjet e integritetit janë shpesh më të rëndësishme sesa çështjet e konfidencialitetit.
- Për shembull, S. Lipner (Microsoft) përshkruan çështjet e integritetit të cilat do të mund të gjindeshin në një rrethinë procesimi komercial të të dhënave:
  1. Shfrytëzuesit nuk do të shkruajnë programe të veta, por do to shfrytëzojnë softuerin ekzistues të produkcionit;
  2. Programuesit zhvillojnë dhe testojnë aplikacionie në një sistem jo-produkcioni, mbase duke shfrytëzuar të dhëna fiktive.
  3. Lëvizja e aplikacioneve nga zhvillim në produkcion kërkon një proces special.
  4. Ky proces duhet të jetë i kontrolluar dhe i audituar.
  5. Menazhuesit dhe auditorët duhet të kenë qasje në gjendjen e sistemit dhe fajlat logues të sistemit.

Mësime

- Integriteti ka të bëjë me atë se sa i besojmë një entiteti të prodhojë, mbrojë ose modifikojë të dhëna.
- Ndryshe nga konfidencialiteti, shkeljet e integritetit nuk kërkojnë domosdoshmërisht akcion të jashtëm.
- Në disa aplikacionie, veçanërisht në botën komerciale, integriteti është më i rëndësishëm se konfidencialiteti.

Labelat e integritetit (Vazhdim)

- Supozojmë se u shoqërojmë *labela integriteti* subjekteve dhe objekteve në sistemin tonë.
  - Labela e integritetit duhet të reflektojë besueshmërinë e subjektit për të prodhuar/përpunuar informacion dhe besueshmërinë e informacionit në objektin.
- **Vërejtje e rëndësishme:** Labelat e integritetit nuk janë edhe labela autorizimi. Në një sistem që zbaton edhe integrietin edhe konfidencialitetin subjektet/objektet duhet të kenë labela për secilin.
- Për shembull, një informacion mund të jetë me vlefshmëri të dyshimtë por shumë i ndieshëm, ose shumë i besueshëm dhe me ndieshmëri të vogël.

Struktura e labelve të integritetit

- Si duken labelat e integritetit? Labelat e integritetit mund të duken sikur labelat e BLP konfidencialitetit.
  - Një komponentë **kierarkike** jep nivelin e besueshmërisë.
  - Një bashkësi **kategorish** jep listën e domeneve të kompetencës relevante.
- Për shembull, një profesor i fizikës mund të ketë labelën e integritetit

  (Ekspert: {Fizikë})

  që do të thotë se ka shkallë shumë të lartë kredibiliteti **në fushën e tij të ekspertizës.**
  - Por, nuk ka ndonjë arsye të veçantë për t'i besuar mendimit të tij në çështje politike ose të zoologjisë.

Relacioni i dominimit

- Meqë labelat e integritetit të njëjtën strukturë sikur labelat e konfidencialitetit, zbatohet relacioni i dominimit. Përkufizohet saktësisht sikur të konfidencialiteti.

Përkufizim

Labela e integritetit $i_1 = (L_1, C_1)$ *dominon* labelën e integritetit $i_2 = (L_2, C_2)$ në qoftë se

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

Shënojmë $i_1 \geq i_2$.

Shembull dominimi

- Supozojmë se kemi bashkësinë e renditur të niveleve kierarkike: **Fillestar**, **Student**, **Ekspert**. Cilat nga çiftet vijuese të labelave janë të tilla që Labela 1 dominon Labelën 2?

Labela 1	Labela 2	Dominon?
(Ekspert: {Fizikë})	**(Student: {Fizikë})**	Po
(Fillestar: {Fizikë, Letërsi})	**(Ekspert: {Fizikë})**	Jo
(Student: {Letërsi})	**(Fillestar: {})**	Po

Metapolitika e integritetit

- Sikur te MSL, dëshirojmë të definojmë një politikë kontrolli të qasjes që implementon qëllimet e sigurisë së integritetit të sistemit. Por, si t'i definojmë rregullat.
- Rikujtoni te MSL, rregullat e BLP ishtin në të vertetë të disenjuara për të kufizuar **rrjedhën e informacionit** brenda sistemit. Kjo ishte metapolitika e konfidencialitetit.
- Pra, **cila është metapolitika e integritetit?**
- **Përgjegjje e mundur:** Mos lejo që informacioni i keq „të kontaminojë" informacionin e mirë.
  - Një formulim alternativ është: **Mos lejo që informacioni të „rrjedh përpjetë" përnga integriteti.**

Metapolitika: implikacionet

- Në analogji me BLP, informacion i keq (i integritetit të ultë) mund të rrjedhë në objekt informacioni të mirë (të integritetit të lartë) në qoftë se:
  - një subjekt me integritet të ultë shkruan informacion të keq në objekt me integritet të lartë; ose
  - një subjekt me integritet të lartë lexon informacion të keq nga një objekt me integritet të ultë.
- Kështu, në analogji me rregullat BLP, një subjekt nuk duhet të lejohet „të shkruajë përpjetë“ përnga integriteti dhe „të lexojë tatpjetë“ përnga integriteti.

Mësime

- Integriteti mund të trajtohet në analogji me konfidencialitetin dhe të konstruktohen labela sikur me BLP.
- Por, konfidencialiteti dhe integriteti janë çështje ortogonale: duhet të trajtohen veçmas.
- Një metapolitikë e mundshme e integritetit është: **informacioni nuk duhet të rrjedhë përpjetë përnga integriteti.**

Modelet e integritetit të Biba-s

- Ken Biba (1977) propozoi tri politika të ndryshme integriteti të kontrollit të qasjes:
  1. Politika e integritetit të nivelit minimal (The Low Water Mark Integrity Policy)
  2. Politika e unazës (The Ring Policy)
  3. Integriteti rigoroz (The Strict Integrity)
- Të gjitha supozojnë shoqërimin e subjekteve dhe objekteve me *labela integriteti,* në mënyrë analoge sikur me nivelet e autorizimit në BLP.
- Vetëm integriteti rigoroz pati ndikim afatgjatë. Pikërisht ky referohet si „modeli Biba“ ose „integriteti Biba“.

Politika e integritetit rigoroz

- Politika e integritetit rigoroz është politikë mandatore e kontrollit të qasjes dhe është dualja e BLP:

Teoremë (Vetia e integritetit të thjeshtë)

*Kusht i nevojshëm që një subjekti S me besueshmëri $i(S)$ t'i lejohet qasje **leximi** një objekti O me besueshmëri $i(O)$ është që $i(S) \leq i(O)$.*

Teoremë (Vetia * e integritetit)

*Kusht i nevojshëm që një subjekti S me besueshmëri $i(S)$ t'i lejohet qasje **shkrimi** një objekti O me klasifikim sensitiviteti $i(O)$ është që $i(S) \geq i(O)$.*

- Çfarë domethënie ka të thuhet se integriteti Biba është „dual" me BLP?

Interpretimi i rregullave

- Integriteti i thjeshtë ka kuptimin që një subjekt mund të lexojë vetëm objekte të nivelit të vet ose më të lartë të integritetit.
- Vetia * i integritetit ka kuptimin që një subjekt mund të shkruajë vetëm objekte të nivelit të vet ose më ultë të integritetit.
- Kuptimi i këtyre rregullave është që integriteti i një subjekti nuk mund të kontaminohet duke lexuar informacion të keq (të integritetit më të ultë); një subjekt nuk mund të kontaminojë informacion më të besueshëm (të integritetit më të lartë) duke shkruar në të.

ACM e integriteti rigoroz

- Meqë integriteti rigoroz është një politikë e kontrollit të qasjes, mund të paraqitet si matricë e kontrollit të qasjes.
- Supozojmë se $H > L$ janë nivelet kierarkike të integritetit.

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	W	W	W
Subj_2	R	R, W	R
Subj_3	R	W	$\varnothing$

Kombinimi i BLP dhe integritetit rigoroz

- Për të mbrojtur konfidencialitetin **dhe** integritetin mund të përdoren edhe BLP edhe politika e integritetit rigoroz e Biba-s.
  1. Do të nevojiteshin labela konfidencialiteti dhe labela integriteti për të gjithë subjektet dhe objektet.
  2. Një qasje lejohet vetëm në qoftë se lejohet nga të dyja: edhe rregullat e BLP edhe rregullat e integritetit rigoroz.
- **Shkruani matricën përkatëse të kontrollit të qasjes.**

Mësime

- Politika e integritetit rigoroz e Biba-s është një politikë integriteti mandatore e kontrollit të qasjes dhe është duale me BLP.
- Qëllimi i saj është të pengojë informacionin të rrjedhë përpjetë përnga integriteti.
- Meqë konfidencialiteti dhe integriteti janë ortogonale ndërmjet veti kërkojnë bashkësi të ndryshme labelash dhe mund të zbatohen veçmas ose së bashku.

Modelet e integritetit të Biba-s (Vazhdim)

- Rikujtojmë se tri politikat e integritetit të Biba-s të kontrollit të qasjes:
  1. Politika e integritetit të nivelit minimal (The Low Water Mark Integrity Policy)
  2. Politika e unazës (The Ring Policy)
  3. Integriteti rigoroz (The Strict Integrity)
- Dallimi kryesor ndërmjet tyre është sasia e besimit e investuar në subjekte.
- Integriteti rigoroz vë shumë pak besim në subjekte dhe kufizon të gjitha leximet dhe shkrimet për të siguruar që informacioni kurrë nuk rrjedh përpjetë përnga integriteti.

Politika e integritetit e nivelit minimal e Biba-s

- Në përgjithësi, një politikë është *e nielit minimal* në qoftë se një atribut është monoton rritës, dhe është *e nielit maksimal* në qoftë se një atribut është monoton zvogëlues, por mund të „resetohet“ në ndonjë moment.
- Politika e nivleit minimal e Biba-s ka dy rregullat vijuese:
  1. Në qoftë se S lexon O, atëherë $i'(S) = \min(i(S), i(O))$, ku $i'(S)$ është niveli i ri i integritetit i subjektit pas leximit.
  2. Subjekti S mund të shkruajë objektin O vetëm atëherë kur $i(s) \geq i(O)$.
- Çfarë është supozimi bazë mbi subjektet në këtë politikë? A konsiderohen ata sado pak të besueshëm?

Politika e integritetit e nivelit minimal

- Potencialisht, politika e integritetit e nivelit minimal pa nevojë zvogëlon monotonisht nivelin e integritetit të një subjekti.
- Ky lloj efekti quhet *shkarje labele* dhe mund të rezultojë me një analizë tepër konservative.

Politika e integritetit e unazës

- Fokusohet në modifikim dhe zgjidh disa probleme të politikës së nivelit minimal.
- Politika e integrimit e unazës ka vetëm rregullën:
  1. Subjekti S mund të shkruajë objektin O vetëm atëherë kur $i(s) \geq i(O)$.
- Pra, çdo subjekt mund të lexojë çdo objekt, pa marrë parasysh nivelet e integritetit.
- Çfarë është supozimi bazë mbi subjektet në këtë politikë?

Mësime

- Në politikën e nivelit minimal të Biba-s niveli i integritetit i një subjekti bie në qoftë se lexon informacion të integritetit të ulët.
- Politika e unazës vë më tepër besim mbi subjektet, duke supozuar se një subjekt mund të filtrojë në mënyrë përkatëse informacionin të cilin e pranon.
- Të tri politikat e integritetit të Biba-s parandalojnë subjektin që të shkruajë përpjetë përnga integriteti.