Kapitulli 1

Siguri kompjuterësh

Detyra për ushtrime

1. Çfarë masash sigurie vëni në përdorim në laptopin tuaj?
2. Çfarë është rendësia e të mësuarit mbi sigurinë kompjuterike?
3. Shpjegoni asimetrinë ndërmjet mbrojtësit dhe kundërshtarit në siguri.
4. Përkufizoni riskun.
5. Përmendni dhe shpjegoni një risk që e pranoni, një që e evitoni dhe një risk që e transferoni.
6. Përshkruani një metapolitikë të mundshme për një rrjet telefonie mobile.
7. Shpjegoni dallimin ndërmjet labelave të konfidencialitetit për dokumente dhe labelave të konfidencialitetit për njerëz.
8. Tregoni se relacioni i dominimit ndërmjet labelave të konfidencialitetit nuk është renditje e plotë (por e pjesëshme).
9. Formuloni joformalisht çfarë thotë vetia e thjeshtë e sigurisë.
10. Formuloni joformalisht çfarë thotë vetia * e sigurisë.
11. Supozoni se do të ndërtoni një sistem (biblioteke) në të cilin të gjithë subjektet kanë qasje leximi të gjitha fajleve por nuk kanë qasje shkrimi për asnjërin. Çfarë nivelesh do t'i jepnit subjekteve dhe objekteve?
12. Supozoni se keni nivelet kierarkike L, H me $L < H$, dhe vetëm një kategori A. Vizatoni grilën.
13. Cilat nga thëniet vijuese janë, me gjasë, **jo** të sakta.
    (a) Mbrojtja kompjuterike është asimetrike; kundërshtari ka përparësinë.
    (b) Siguria e përkryer është e arritshme për sisteme komplekse.

(c) Siguria e kompjuterëve ka të bëjë, në fakt, me menazhim e riskut.

(d) Për dallim nga shumica e fushave teknologjike, siguria përfshin ballafaqim me një kundërshtar malicioz.

(e) Ndonjë nga të mësipërmet është e pasaktë.

14. Cilat nga thëniet vijuese mbi kanalet e fshehta janë **jo** të sakta.

(a) Një kanal i fshehtë mund të lejojë informacionin të rrjedhë në kundërshti me metapolitikën e sistemit.

(b) Një kanal i fshehtë shfrytëzon një resurs (atribut) kompjuteri jo të disenjuar për komunikim ndërmjet subjektesh.

(c) Një kanal i fshehtë ekziston në qoftë se H mund të bëjë diçka për të ndryshuar pamjen e sistemit për L. (Supozoni se labela e sigurisë së H dominon atë të L.)

(d) Të gjitha të mësipërmet janë të sakta.

15. Supozoni se keni një sistem me tri subjekte dhe tri objekte, me nivele sigurie si në vijim. Këtu $H > L$. Sistemi implementon një model Bell-

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

LaPadula të sigurisë. Plotësoni të drejtat e qasjes (R dhe/ose W) që lejohen nga modeli për secilin çift subjekt/objekt në matricën vijuese të kontrollit të qasjes.

	Obj_1	Obj_2	Obj_3
Subj_1			
Subj_2			
Subj_3			

16. Supozoni se është definuar politika MLS (e konfidencialitetit) me dy rregullat vijuese:

(a) Një subjekt s mund të lexojë një objekti o atëherë dhe vetëm atëherë kur $l(o) \leq l(s)$

(b) Një subjekt s mund të shkruajë në një objekt o atëherë dhe vetëm atëherë kur $l(s) \leq l(o)$, dhe pastaj $l'(s) = \max(l(s), l(o))$, ku $l'(s)$ është niveli i ri i konfidencialitetit të subjektit pas shkrimit.

A do të ishte kjo një politikë e arsyeshme konfidencialiteti? Filloni me „Po“ ose „Jo“ dhe pastaj arsyetoni përgjegjjen tuaj.

17. Në një sistem BLP supozoni se çdo subjekt do të mund të ngriste nivelin e vet. A do të shkelte kjo vetinë e qetësisë së dobët? (Filloni përgjegjjen me „Po“ ose „Jo“. Arsyetoni përgjegjjen tuaj.)

18. Supozoni se keni një sistem me tri subjekte dhe tri objekte, me nivele **integriteti** si në vijim.

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

Këtu $H > L$. Sistemi implementon politikën e integritetit rigoroz të Biba-s. Plotësoni të drejtat e qasjes (R dhe/ose W) që lejohen nga modeli për secilin çift subjekt/objekt në matricën vijuese të kontrollit të qasjes.

	Obj_1	Obj_2	Obj_3
Subj_1			
Subj_2			
Subj_3			

19. Supozoni se keni një sistem me tri subjekte dhe tri objekte, me nivele konfidencialiteti të dhëna në detyrën 15 dhe me nivele integriteti të dhëna në detyrën 18. Supozoni se edhe nivelet e konfidencialitetit edhe të integritetit plotësojnë relacionin $H > L$. Sistemi implementon një politikë Bell-LaPadula të konfidencialitetit dhe një politikë të integritetit rigoroz të Biba-s. Një qasje për lexim ose shkrim lejohet vetëm në qoftë se lejohet qasja përkatëse nga të dyja: edhe rregullat e BLP edhe rregullat e integritetit rigoroz. Plotësoni të drejtat e qasjes (R dhe/ose W) që lejohen nga kombinimi i dy politikave të sigurisë për secilin çift subjekt/objekt në matricën vijuese të kontrollit të qasjes.

	Obj_1	Obj_2	Obj_3
Subj_1			
Subj_2			
Subj_3			

20. Supozoni se keni një sistem BLP sigurie me katër subjekte S_1, S_2, S_3 dhe S_4 dhe një objekt O me nivele konfidencialiteti si në vijim.

Subjekti	**Niveli**	**Objekti**	**Niveli**
S_1	$(L, \{A, B\})$	O	$(H, \{B\})$
S_2	$(H, \varnothing)$		
S_3	$(L, \{A, B, C\})$		
S_4	$(H, \{B, C\})$		

Supozoni se $H > L$.

(a) Paraqitni metapolitikën e sigurisë së mbështetur në grilë duke vizatuar grilën përkatëse.

(b) Cilat nga subjektet mund të lexojnë O?

(c) Cilat nga subjektet mund të shkruajnë O?

21. Një sistem ofron mbrojtje duke zbatuar polikikën Bell-LaPadula. Një haker gjen një mënyrë për të futur një virus në sistemin në nivel të çfarëdoshëm sigurie. Qëllimi i tij është ta përhap sa më tepër që të jetë e mundur duke infektuar objekte tjera në sistemin. A duhet virusi të futet në një objekt në nivelim më të ultë të sistemit (që dominohet nga të gjitha nivelet tjera) apo në nivelim më të lartë të sistemit (që dominon të gjitha nivelet tjera)? Shpjegoni.