HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Integrirani okvir za sigurnost i pouzdanost

CCERT-PUBDOC-2001-03-02

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Neformalno, od računalnih sustava se očekuje da "rade kako bi trebalo" ili da "funkcioniraju ispravno". To znači da bi računalni sustavi trebali biti istovremeno sigurni i pouzdani. Povijesno gledajući, neovisno su se razvila dva istraživačka područja vezana uz sigurnost i pouzdanost. Ukratko, sigurnost se razvila na temelju namjernih i neprijateljskih interakcija sa sustavima, koje vode prema neovlaštenom otkrivanju ili modificiranju informacija. Pouzdanost se razvila na temelju razmatranja pitanja pouzdanosti i raspoloživosti. Tradicionalno su se pitanja sigurnosti i pouzdanosti razmatrala odvojeno, tek kasnije pojavili su se pokušaji integracije tih disciplina; jedna metoda definira pouzdanost kao općeniti koncept u kojem je sigurnost samo jedan od atributa, dok druga metoda odabire obrnuti pristup. Posljedice tih predloženih integracija nisu još u potpunosti sagledane. Ovaj dokument čini jedan korak u tom smjeru; u njemu je prikazan integrirani okvir za sigurnost i pouzdanost, te također pokriva mnoge aspekte "potrebne funkcionalnosti" sa korisničke strane. Isto tako je opisano kako se okvir može iskoristiti za višeslojne mjere.
Treći odlomak dokumenta bavi se terminologijom, dok je u četvrtom prikazan trenutno stanje disciplina sigurnosti i pouzdanosti. Postoje mnoge različite opcije o statusu diskusije o konceptima i korištenoj terminologiji, no koncepti i terminologija korištena u dokumentu smatraju se široko prihvaćenim. Pouzdanost je dana u "klasičnoj" formi, sa tradicionalnim načinom integracija sigurnosti. Sigurnost je pak opisana prema različitim aspektima, te su spomenute i neke alternative. U petom odlomku predložen je novi konceptualni okvir, dok šesti odlomak prikazuje istraživanje postojećih mjera sigurnosti/pouzdanosti i naznačava kako bi trebale biti definirane nove mjere temeljeno na modelu sustava.

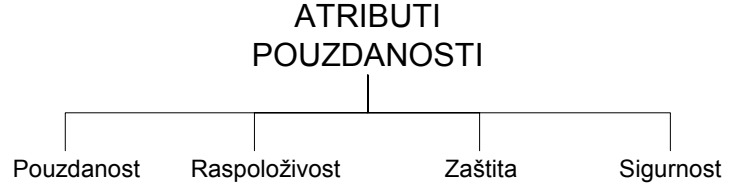
2. Terminologija

Ovaj dokument bavi se novim konceptima, te koristi i stare ali na novi način. Općenito, novi koncepti zahtijevaju nove termine ili redefiniciju starih, pošto je ključno da se oni mogu pravilno adresirati i razumijevati. Očekuje se da onaj tko predlaže novi konceptualni okvir, također predloži odgovarajuću terminologiju, te pojasni povezanost sa uvriježenom terminologijom. Ipak, valja naglasiti da se značenje nekih termina korištenih u ovom dokumentu razlikuje od "normalne" uporabe, no iz konteksta bi trebalo biti jasno koja je interpretacija ispravna.

3. Trenutno stanje

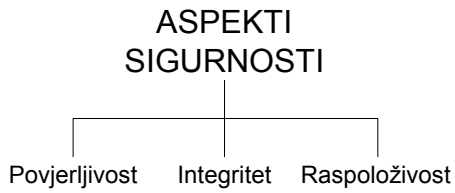
3.1. Pouzdanost nasuprot sigurnosti

Pouzdanost je prvo uvedena kao generički izraz koji je obuhvaćao koncepte poput pouzdanosti, raspoloživosti, mogućnosti održavanja i zaštite, a definirala se u pojmovima "ispunjavanja zadataka" i "pružanjem očekivane usluge". Postoje razne redefinicije originalne inačice, no nakon nekoliko godina rada i analize koncepta pouzdanosti, definirani su sljedeći atributi pouzdanosti; pouzdanost, raspoloživost, zaštitu i sigurnost (slika 1).
Sigurnost se tretira kao jedan od atributa pouzdanosti. Osim sigurnosti, svi ostali atributi odnose se na ponašanje sustava, odnosno uslugama koje sustav daje svom okruženju; zbog toga oni formiraju adekvatnu bazu za pristup proučavanjem ponašanja. Kod pojma sigurnosti situacija je drugačija; ona se definira preko tri različita aspekta: povjerljivosti, integriteta i raspoloživosti (slika 2).



***Slika 1:** Pouzdanost i atributi pouzdanosti*

Zbog toga koncept sigurnosti ne opisuje samo ponašanje sustava (usluge koje sustav pruža okolini; npr. raspoloživost), nego također mogućnost sustava da se odupre vanjskim čimbenicima – napadima (integritet).



Slika 2: *Sigurnost i aspekti sigurnosti*

3.2. Opći koncepti

Zanimljivo je da je u početku bio predložen termin obranjivost sustava kao generalizirani pojam sigurnosti koji je implicirao sigurnost, pouzdanost, raspoloživost i mogućnost praćenja. Predlagač takvog koncepta ne elaborira proširene atribute u analizi operacijskih sustava. Također on opisuje termine preventivnog pristupa nasuprot naknadnog. Tako se pojam preventivnog odnosi na mjere uzete tijekom faze razvoja da se bi se postigao siguran dizajn u smislu specifičnih metoda i formalnih specifikacija, dok naknadni pristup uključuje procjenu sigurnosti kad je sustav operativan, te pokušava ispraviti ranjivosti koje se razotkriju. Ovaj pogled je laički i promatra koncept kroz fazu izrade.

Sljedeći koncept koji se predlaže kao proširenje pouzdanosti, daje procjenu prihvatljivosti sustava umjesto da bude svojstvo sustava. Ovaj koncept prikladan je za velike i složene sustave sa opširnom ljudskom interakcijom koju je teško eksplicitno specificirati, te koja može biti dvosmislena ili nekonzistentna.

Problem osiguranja sigurne neosjetljivosti na pogreške, odnosno povećane pouzdanosti (neosjetljivost na pogreške) i istovremenog očuvanja sigurnosne politike predstavlja još jedan od koncepata. Autor naglašava da kod sustava neosjetljivih na pogreške postoji opasnost ugrožavanja sigurnosti sustava, te predlaže moguća rješenja. Jedna od tih tehnika jest i FRS (eng. Fragmentation-Redundancy-Scattering) koja se može iskoristiti za postizanje neosjetljivosti na neovlaštene aktivnosti.

Jedan općeniti pogled odnosi se na problem povlačenja granice između sigurnosti i ostalih kritičnih zahtjeva, te raspravlja kako osiguranje maksimalne povjerljivosti, integriteta i raspoloživosti ("osigurane usluge") ne obuhvaća dovoljno dobro problem osiguravanja zadovoljavajuće sigurnosti. Predloženo je rješenje temeljeno na nekoliko različitih koncepta sigurnosne politike, koje se temelji na preciznom elaboriranju pojma sigurnosti. Također se kaže da mnogi zahtjevi za integritetom i raspoloživosti ne mogu biti direktno obuhvaćeni sigurnosnom politikom i puno bolje ih je definirati kao zahtjeve druge prirode.

U drugom radu dana je relacija između sigurnosti i zaštite. Autori analiziraju nekoliko primjera u kojima se susrećemo pitanja zaštite i sigurnosti. Definirani su pojmovi kritične sigurnosti i kritične zaštite koji se kasnije koriste za opisivanje apsolutne, odnosno relativne štete.

Konačno postoji i koncept kvalitete ("spremnosti za uporabu") koji u sebi sadrži zadovoljstvo proizvodom i odsustvo nedostataka. Parametar "spremnosti za uporabu" u sebi sadrži raspoloživost, pouzdanost i mogućnost održavanja

3.3. Sigurnosni koncepti

Kako je spomenuto ranije, postoje razne inačice definicije sigurnosti. U nekim slučajevima postoje dodatni aspekti kao uskraćivanje usluge ili vjerodostojnost, u drugim pak postoje druge klasifikacije.

U sustavima baza podataka integritet se odnosi na valjanost i konzistentnost podataka kako je definirano u ograničenjima integriteta, dakle primarne akcije izvodi ovlaštena strana, a sigurnost se odnosit na zaštitu podataka od neovlaštenog otkrivanja, promjene ili brisanja. No isto tako paralelno se koristi i tradicionalna definicija.

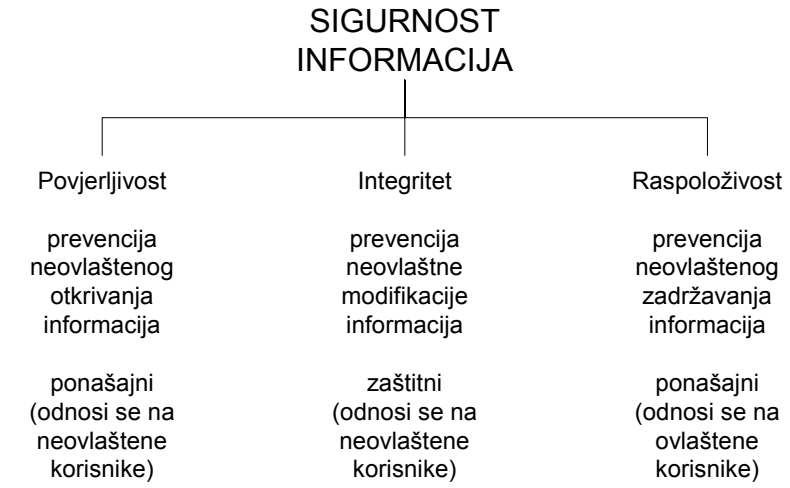
Postoji također velik broj formalnih modela. Jedan od njih je model povjerljivosti, odnosno opis toka informacija u sigurnom sustavu, koji cilja na identifikaciju putova koji mogu dovesti do neodgovarajućeg otkrivanja informacija. Postoji i odgovarajući model integriteta. Formalni sustav

pravila zaštite temelji se na matrici prava pristupa. Matrica se koristi za definiciju prava P subjekta S u odnosu na objekt O.
Također postoji sigurnosni koncept koji se prvenstveno odnosi na povjerljivost. Prvenstveno je razvijen za potrebe američke vojske s namjerom da odgovara sigurnosnoj politici američkog ministarstva obrane. Sigurnosna politika je predstavljena skupom zakona i pravila koja reguliraju kako organizacija upravlja, štiti i distribuira povjerljive podatke. Isto tako ta politika široko se koristi u komercijalnim operacijskim sustavima. Na temelju procedure razvoja i prisutnosti (ili odsutnosti) sigurnosnih mehanizama i metoda, određuje se stupanj zaštite i sustav se svrstava u jednu od sedam kategorija. Sličan koncept koji slijedi općenitije kriterije razvijen je i u Europi, a također postoje alternative i u drugim državama. Postoje također pokušaji internacionalizacije, odnosno prihvaćanja globalnog standarda.

4. Konceptualni prijedlog okvira

4.1. Interpretacija atributa sigurnosti

Ovdje će biti objašnjena interpretacija tri sigurnosna aspekta (povjerljivost, integritet i raspoloživost) u smislu ponašanja i zaštite. Slika 3 prikazuje sigurnost informacija.
Raspoložívost se primarno definira kao mogućnost sustava da pruži uslugu ovlaštenom korisniku, dakle može se promatrati kroz koncept ponašanja. Ovlašteni korisnici su korisnici kojima su namijenjene usluge sustava kako je naznačeno u specifikaciji sustava. Svi ostali korisnici osim ovlaštenih korisnika smatraju se neovlaštenim korisnicima. Iz toga proizlazi da raspoloživost kao sigurnosni aspekt ima isto značenje kao i atribut raspoloživosti kod pouzdanosti.

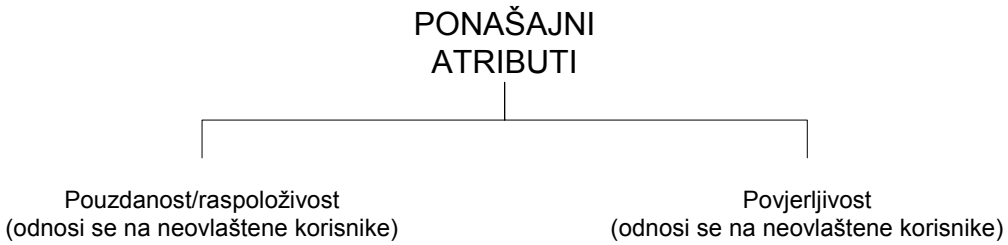


Slika 3: *Sigurnost informacija i aspekti sigurnosti*

Integritet predstavlja prevenciju neovlaštene modifikacije, brisanja ili uništavanja elemenata sustava. Integritet je narušen u slučaju napada, koji obično izvršavaju neovlašteni korisnici, ali koji također može izvršiti i ovlašteni korisnici koji zloupotrebljavaju svoje ovlasti. Zbog toga integritet spada u zaštitnu kvalitetu sustava i karakterizira mogućnost sustava da se odupre napadima.
Povjerljívost jest mogućnost sustava da onemogući neovlaštenim korisnicima pristup povjerljivim informacijama. Dakle i to je koncept ponašanja, ali za razliku od drugih atributa, povjerljivost definira ponašanje sustava u odnosu na neovlaštenog korisnika. U stvarnosti time se definira do koje razine neka informacija treba biti dostupna, odnosno nedostupna neovlaštenim korisnicima. Kao takva provjerljivost je koncept paralelan sa konceptima pouzdanosti, raspoloživosti i zaštite. Povjerljivost se također može promatrati u širem smislu, odnosno kao prevenciju pružanja usluge neovlaštenim korisnicima, čak i ako pružanje takve usluge ne bi značilo štetu za ovlaštene korisnike ili otkrivanje tajnih informacija. Za ovakav prošireni koncept predložen je termin *ekskluzivnost*.

Iz gore navedenog može se zaključiti da se sigurnost može promatrati kao dva koncepta; koncept zaštite i koncept ponašanja. Koncept zaštite odnosi se na oblik neosjetljivosti na pogreške, prvenstveno na neosjetljivost na pogreške uzrokovane namjerno izazvanim pogreškama i napadima. Koncept ponašanja je integralni dio pouzdanosti i ne može se promatrati izvan tih okvira. Taj koncept otkriva dva generička tipa atributa ponašanja: pouzdanosti/raspoloživosti i povjerljivosti (slika 4).

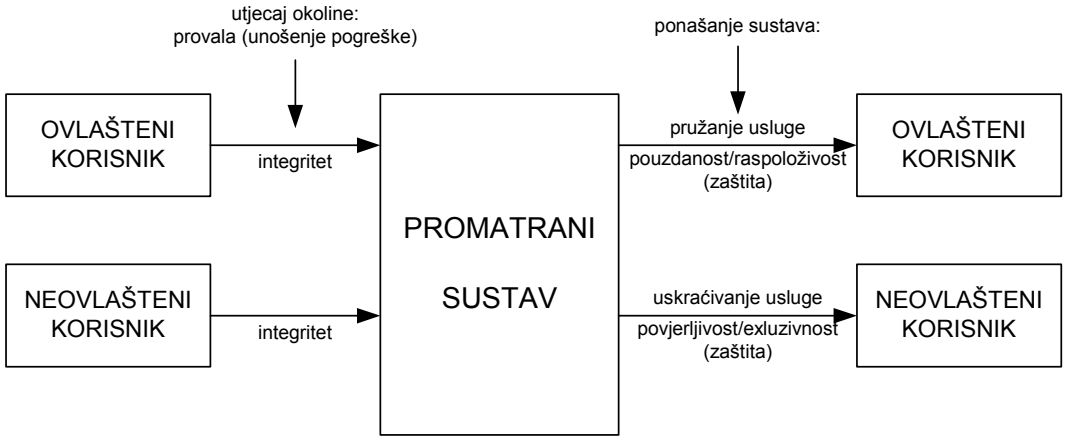
Povjerljivost se odnosi na uskraćivanje usluge neovlaštenim korisnicima, odnosno neovlašteni korisnici ne bi smjeli dobiti informaciju od strane sustava niti ga koristiti na bilo koji drugi način. Pouzdanost i raspoloživost se stapaju pošto se odnose na pružanje usluge korisniku, što ne znači da su to identični atributi. Ti atributi se spajaju jer se odnose na pružanje usluge ovlaštenom korisniku, iako se odnose na različite aspekte pružanja te usluge. Atribut zaštite označava određenu razinu pada sustava, odnosno izostanak fatalnih pogrešaka. Pogreške se mogu odnositi na pouzdanost, odnosno na ovlaštene korisnike i na povjerljivost, odnosno na neovlaštene korisnike.



Slika 4: *Ponašajni atributi pouzdanosti*

4.2. Model sustava

Razmatranja iz prethodnog odlomka mogu se svesti na sljedeći model sustava. Čitav sustav koji se razmatra sastoji se od promatranog sustava i okoline. Općenito, postoje dva načina interakcije sustava i okoline (slika 5).



Slika 5: *Model sustava*

U prvom slučaju interakciju sustava i okoline predstavlja pružanje usluga okolini. To predstavlja ponašanje sustava. Također postoji utjecaj okoline na sustav, što znači da sustav prima informacije iz okoline. Te informacije sastoje se od različitih vrsta interakcije. Najzanimljivija vrsta interakcije je ona koja uključuje propagaciju pogreške u sustav, a posebno namjerne, odnosno zlonamjerne pogreške, tj. kršenje sigurnosti. Pošto su pogreške štetne za sustav, dizajnom sustava nastoji se onemogućiti njihovo pojavljivanje. To svojstvo sustava naziva se integritet i uključuje zaštitne aspekte sigurnosti/pouzdanosti.

Postoje dvije vrste primatelja izlaznih informacija iz sustava; ovlašteni i neovlašteni korisnici. Željeno (radije specificirano) pružanje usluge ovlaštenim korisnicima može se opisati sa atributima

ponašanja; pouzdanosti, raspoloživosti i zaštitom. Rjeđe specificirano, ali još uvijek poželjno svojstvo sustava jest mogućnost uskraćivanja usluge neovlaštenim korisnicima. Ovo svojstvo je također opisano atributima ponašanja; povjerljivosti (za pristup informacijama) i ekskluzivnosti (za korištenje), isto kao i zaštitom.

4.3. Primjer: Trojanski konj

Jedna od prednosti ovog modela jest da pojašnjava relaciju između tradicionalnog poimanja sigurnosti/integriteta i pouzdanosti. Općenito, model odvojeno promatra zaštitne i ponašajne značajke, te daje pojašnjenje relacije među njima. Primjer trojanskog konja normalno se smatra teškim za modeliranje.

Pojavom trojanskog konja u sustavu događa se kompromitacija zaštitnih značajki ("ugrožavanje integriteta", "pad sigurnosti" ili jednostavno "provala"). Kada je trojanski konj u sustavu, sustav je neispravan. Također, trojanski konj može ostati neaktivan neodređeno dugo, te praktički nikad ne uzrokovati neispravno ponašanje sustava, odnosno kompromitirati pouzdanost ili povjerljivost. Uočljivo je da su u ovom slučaju zaštitne značajke ugrožene, ali ponašajne nisu. Korisnik ne bi nikad uočio neispravnost, ukoliko je sam ne bi aktivno tražio.

S druge strane, trojanski konj se može aktivirati nakon nekog vremena uzrokujući time npr. omesti pružanje usluga korisniku. U ovom slučaju dolazi ugrožavanje sigurnosti propagira i uzrokuje ugrožavanje pouzdanosti. Grupiranje tih atributa obično je složeno i ovisi o funkciji sustava i sl.

Također je uočljivo da, isto to ometanje pružanja usluga korisniku koje je uzrokovao trojanski konj, može uzrokovati i neka pogreška software-a ili hardware-a u sustavu. To jasno pokazuje da ulazne i izlazne značajke mogu, ali i ne moraju biti međusobno povezane. Isto tako, to pokazuje da su zaštitne i ponašajne značajke samo djelomično povezane i da je njihovo povezivanje prilično složeno.

5. Mjere razine sigurnosti

Ovo poglavlje odnosi se na neke postojeće pristupe za mjerenje razine sigurnosti i složenih koncepata sigurnosti/pouzdanosti. Uobičajeno prihvaćene i korištene mjere raspoloživosti kao npr. srednje vrijeme između kvarova ili vjerojatnost uspješnog izvršenja se ne spominju. Konačno, pojašnjeno je kako se mogu izvesti mjere temeljene na predloženom modelu sustava.

5.1. Postojeće mjere razine sigurnosti

Danas je klasifikacija prema određenim razinama uobičajen način mjerenja razine sigurnosti. Te klase uglavnom odražavaju statička svojstva sustava i ne uključuju mogućnost slučajnih događaja i ovisnost o operacijskom okruženju na stohastički način, slično kako se uobičajeno opisuje pouzdanost. Sljedeći dio dokumenta raspravlja ta pitanja.

Ne postoje mnoge praktične mjere, a one koje postoje uglavnom se odnose na upade i nedostatke. Postoji tzv. "pokazatelj računanja sigurnosti" koji se proračunava korištenjem Markovljevih lanaca i kojem je zadatak kvantificirati ukupni sigurnosni aspekt sustava neosjetljivog na provale. Racionalizacija koja se koristi prilikom modeliranja Markovljevim lancima podrazumijeva da su kršenja sigurnosti eksponencijalno raspodijeljena, što općenito nije istinito.

Za označavanje efikasnosti mehanizama za otkrivanje neovlaštenih aktivnosti uvodi se koncept "pokrivanja neovlaštenih aktivnosti". No veće pokrivanje neovlaštenih aktivnosti ne znači nužno i veći pokazatelj računanja sigurnosti, koji definira intuitivno očekivanje tog pokazatelja.

Također postoji sličan pokazatelj, "pokazatelj sigurnosne ranjivosti", koji se računa na temelju faktora iz nekoliko područja. Faktori su definirani tako da je njihova prisutnost (ili odsutnost) utječe na opću ranjivost sustava. Na taj način dobivaju se vrijednosti između nule i jedinice. Postoji nekoliko problema vezanih uz ovaj pristup. Glavni nedostatak jest da postoji mogućnost da se utjecaj inicijalnih faktora ne može procijeniti. Općenito, niti svi fizički nedostaci, niti neispravljeni bugovi operacijskog sustava nisu poznati, te kao takvi ne mogu biti procijenjeni i kvantificirani. Konačno, nije potpuno jasno kako treba interpretirati pokazatelj određene razine, te se razine grupiraju u četiri različite klase: "nisko", "umjereno", "visoko" i "izrazito visoko". Čini se vjerojatnim da se takva klasifikacija mogla jednostavno dobiti čisto subjektivnom procjenom značajki pojedinog sustava.

Kompletno drugačiji pristup pak daje metoda kvantitativne procjene operacijske sigurnosti temeljena na novom konceptu koji se naziva "grafom privilegija". Taj koncept predstavlja proširenje i elaboraciju uporabe Petrijevih mreža i matrice prava pristupa.

5.2. Postojeće složene mjere

Postoji alternativni način za mjerenje pouzdanosti i sigurnosti. Pouzdanost se promatra kroz gubitak i rizik koji predstavljaju unificirajuće koncepte u definiciji. Definicija dozvoljava kontekstno-ovisnu procjenu pouzdanosti, pokazujući različite percepcije izloženosti riziku. Nadalje, rizik i gubitak (u jedinici vremena) predložene su mjere pouzdanosti. Rizik se može koristiti u ranijim fazama projektiranja da obuhvati naslijeđenu neodređenost projektiranja, odnosno činjenicu da ne postoji kompletan uvid u konačnu realizaciju sustava. Na taj način mogu se koristiti konvencionalne metode analize rizika. Mjera koja se temelji na gubitku prikladna je za operativnu fazu. Prednost ove mjere jer u tome što se jednostavno može prevesti u ekonomske veličine.
Konačno, postoje mnogi pokušaji mjerenja pouzdanosti, a koji samo mjere neke aspekte pouzdanosti. U tom slučaju pojam pouzdanosti se koristi u suženom smislu. Kod takvih mjera sigurnosni aspekt najčešće je potpuno zanemaren. Npr. neki modeli promatraju pouzdanost i raspoloživost kroz novi koncept "izvršenja zadatka", dok drugi pak promatraju samo pouzdanost i zaštitu. Još jedan primjer sukcesivne operacijske periode modelira Markovljevim procesima, te koristi kao mjeru pouzdanosti. Cijela analiza se temelji na činjenici da postoje tri vrste stanja: funkcionalno (operativno), nefunkcionalno (ispravljiv kvar), kompletno nefunkcionalno (fatalni kvar). Zanimljivo je primijetiti da postoji sličnost sa ranije opisanim ponašajnim modelom. No tako izvedena mjera je prije mjera kombinacije pouzdanosti i raspoloživosti nego mjera koja bi također opisivala sigurnost i zaštitu.

5.3. Mjere ponašajne i zaštitne sigurnosti

Konceptualni okvir opisan u odlomku 4.2 daje način integracije aspekata koji su opisuju sigurnost i pouzdanost na način koji razjašnjava razliku između štetnog utjecaja na sustav i sustava koji ne funkcionira. Tako postoje atributi koji opisuju mogućnost sustava da se odupre štetnim utjecajima okoline koji se nazivaju zaštitnim atributima, te atributi koji opisuju mogućnost sustava da ispuni određenu funkciju koji se nazivaju ponašajnim atributima.
Iz toga proizlazi da se mjere koje se definiraju za sustav mogu također podijeliti na ponašajna i zaštitne mjere. Bilo je pokazano kako se aspekt povjerljivosti može uklopiti u ponašajnu mjeru čim se napravi razlika između uskraćivanja usluge ovlaštenom korisniku i uskraćivanja usluge neovlaštenom korisniku, te da takve tradicionalne metode modeliranja pouzdanosti mogu biti iskorištene za izvođenje *ponašajne mjere*.
Zaštitna mjera predstavlja mogućnost sustava da se odupre provalama i drugim štetnim utjecajima na sustav. Zaštitne mjere su mnogo slabije razvijene od ponašajnih. Naravno postoje pokušaji modeliranja zaštitnih atributa korištenjem provalnih procesa. Smisao toga je povezivanje zaštitnih svojstava sustava sa težinom izvršenja uspješnog napada odnosno provale u sustav. Mogući način za realizaciju toga jest izvođenje planiranih napada, te sakupljanje relevantnih podataka o procesu provale tijekom toga.
Također valja primijetiti da postoji još jedna značajka sustava koju bi valjalo ocijeniti kvantitativno jest *ispravnost* sustava. Nije poznat niti jedan pokušaj mjerenja tog aspekta sustava, iako u načelu to ne bi trebalo biti nemoguće. Takva mjera posebno bi bila primjenjiva u sustavima baza podataka.
Konačno, valja istaknuti da tri gore opisane mjere nisu međusobno neovisne, iako opisuju različite aspekte sustava. Redukcija zaštitnih mogućnosti sustava će normalno, ali ne i nužno utjecati na neispravnost sustava. Također, neispravnost može, ali ne uvijek, dovesti do krivog ponašanja.

6. Zaključak

U dokumentu je prikazan prijedlog novog pristupa pitanjima sigurnosti i pouzdanosti. Pristup se temelji na ideji da se računalni sustav može opisati ponašajnim i zaštitnim pojmovima. Ponašajna točka gledišta se odnosi na ponašanje sustava, odnosno kako sustav utječe na svoju okolinu, što se očituje u aspektima pouzdanosti i raspoloživosti. Zaštitna točka gledišta opisuje kako zaštiti sustava od neželjenog djelovanja okoline. Korištenjem tog pristupa, pokazano je kako se aspekti

tradicionalnog promatranja sigurnosti mogu integrirati sa postojećim konceptima pouzdanosti i interpretirati kao zaštitne ili ponašajne značajke.
Između ponašajnih značajki sustava razlikuje se povjerljivost, koja za razliku od ostalih značajki koje opisuju relacije između sustava i ovlaštenih korisnika, opisuje relaciju između sustava i neovlaštenih korisnika. Zaštita se interpretira kao pod-atribut, te opisuje podskup ponašajnih pogrešaka, dajući mogućnost sustava da izbjegne katastrofalne posljedice. Integritet se objašnjava kao koncept za prevenciju pogrešaka, pri tome promatrajući namjerne vanjske pogreške ili napade na sustav. Konačno, na kraju je naglašeno kako se novi koncepti mogu kvantitativno opisati, odnosno mjeriti.