Originalni naučni rad

UDK 004.451:930.251

DOI 10.7251/SVR1817124M

OPERATIVNI SUSTAVI I KONTROLA PRISTUPA PODACIMA

Doc. dr Marijan Mijatović[1]

Nezavisni univerzitet Banja Luka

Apstrakt: Operativni sustavi predstavljaju jedan kompleks koji je vrlo bitan u kontroli pristupa podacima. U operativnom sustavu računalo predstavlja samo jedan element računalnog sustava koji obavlja osnovne funkcije. Operativnim sustavom uobičajno je da upravlja jedan korisnik, ali isto tako nije isključeno, da njime upravlja i više korisnika. Jedna od glavnih funkcija svakog računalnog sustava je da pohranjuje informacije, ali isto tako da ima adekvatnu zaštitu da te informacije budu maksimalno zaštićene. Kada se govori o kontroli pristupa onda se govori o tri vrste mehanizama kontrole. To su diskretna kontrola, obavezna kontrola pristupa, i kontrola pristupa prema ulogama.

Ključne riječi: *operativni sustavi, informacije, kontrola pristupa*

UVOD

Prilikom pohranjivanja informacija i podataka unutar računalnog sustava, zbog raznih napada i prijetnji, one moraju biti zaštićene. Jedan od načina zaštite pohranjenih informacija je i kontrola prava pristupa od strane operacijskog sustava, a i korisnika. Također, svima je poznato da je kontrola pristupa prisutna je u svakodnevnici svuda oko nas. Nekoliko različitih vrsta informacija se može kontrolirati poput čitanja, pisanja, izvršavanja, brisanja i slično. Za to postoje dva načina kontrole pristupa: politika kontrole pristupa i mehanizmi za kontrolu pristupa. Sama kontrola pristupa odnosi se na skup kontrola kojima se ograničava pristup određenim resursima od strane subjekta ili predmeta.

U ovom radu bit će navedeno što je to pristup podacima te kontrola pristupa podacima uz objašnjenje navedene politike kontrole pristupa i mehanizama za kontrolu pristupa. Također, na početku rada biti će ukratko objašnjeno što je to sam operacijski sustav te će isti biti objašnjen sa aspekta korisnika i aspekta sustava.

[1] e-mail: marijan.mijatovic@nubl.org

OPERACIJSKI SUSTAV

Da bi bilo moguće objasniti što je to operacijski sustav, najprije je potrebno definirati što je to računalni sustav i od čega se on sastoji. Naime, danas postoje razne vrste računala, od osobnih i prijenosnih računala pa do pametnih telefona i raznih drugih uređaja. Svim tim računalima je jednako to što se sastoje od elemenata koji čine računalni sustav. On se sastoji od korisnika, programa, operacijskog sustava i sklopovlja. Računalo je samo element računalnog sustava koji obavlja osnovne funkcije: ulaz, izlaz, obrada, pohrana i upravljanje. Također, računalni sustav dijelimo na sustav sklopovske opreme i sustav programske podrške, poznatiji kao *hardware* i *software*. Nadalje, računalni sustav se dijeli na razne kategorije: osobna računala, mini računala, velika računala i superračunala.

Kao što je ranije navedeno, operacijski sustav je dio računalnog sustava te on bez njega ne može funkcionirati niti obavljati zadane radnje. Operacijski sustav upravlja sustavom na način da obavlja zahtjeve koje mu zadaje program ili korisnik. Pomoću njega je jednostavno koristiti računalni sustav kroz odgovarajuća sučelja. Operacijski sustav djeluje kao posrednih između korisnika i računala te računalnog sklopovlja. Njegova svrha je osigurati okruženje u kojem korisnik može izvršavati programe na prikladan, jednostavan i učinkovit način. Sklopovlje računala mora osigurati odgovarajuće mehanizme kako bi osiguralo ispravno funkcioniranje računala i računalnog sustava i kako bi se spriječilo ometanja pravilnog rada sustava od strane korisničkih programa. Zbog svoje složenosti i veličine, operacijski sustav mora biti izrađen dio po dio te svaki od dijelova mora biti dobro definiran uz pažljivo kreirane ulaze, izlaze i funkcije[2].

Dakle, operacijski sustav je skup osnovnih programa koji omogućuju izvođenje radnih zadataka na računalu i operacija računala. Njegova uloga je olakšati korisniku korištenje računala, zatim učinkovito korištenje svih dijelova računala, višeprogramski rad i mora doprinijeti učinkovitosti sustava. Operacijski sustav se dijeli na funkcije sustava i sučelje prema programima, tzv. API, zatim na jezgru operacijskog sustava i apstrakciju sklopovlja[3].

Postoji nekoliko funkcija operacijskog sustava, odnosno zadaci koje mora moći izvršavati. Glavne funkcije su: upravljanje zadacima obrade, upravljanje podacima, upravljanje ulazom i izlazom, upravljanje memorijom, obrada prekida, dodjeljivanje procesora, zaštita,

OPERACIJSKI SUSTAV SA ASPEKTA KORISNIKA

Sa aspekta korisnika računala, svrha operacijskog sustava je olakšavanje korištenja računala kroz sučelje. U tom slučaju, operacijski sustav je namijenjen isključivo jednostavnoj upotrebi računala s posebnim naglaskom

[2] Silberschatz, Bear, Gagne, 2014

[3] Jelenković, 2017

na izvedbu korisničkih zahtjeva. Točna i brza izvedba korisničkih zahtjeva je važna za samog korisnika te operacijski sustav mora biti za to optimiziran.

Cilj operacijskog sustava sa aspekta korisnika je maksimizirati rad i minimizirati napor korisnika prilikom korištenja računala. Većina sustava je dizajnirana na način da računalnim sustavom upravlja samo jedan korisnik, no u nekim slučajevima može biti i njih više. Kad postoji više korisnika oni dijele resurse tj. memoriju. Operacijski sustav mora biti izrađen na način da omogućuje rukovanje resursima između računala i procesora na učinkoviti način. Nadalje, mora biti osmišljen tako da uzima u obzir upotrebljivost resursa koje dijeli i njihovo adekvatno korištenje. Operacijski sustav daje korisniku osjećaj da se računalni sustav bavi samo izvršavanjem trenutnog zadatka, no vrlo dobro je poznato da se u pozadini obavlja nekoliko drugih procesa. Korisnici koji su povezani preko računalnih mreža sa drugim radnim stanicama i poslužiteljima imaju na raspolaganju određene resurse koje također dijele preko mreža i poslužitelja. U takvom slučaju, operacijski sustav je napravljen kako bi ostvario dobar kompromis između individualne iskoristivosti i iskoristivosti svih resursa[4].

Usluge koje pruža operacijski sustav općenito uključuju učitavanje i izvođenje programskih datoteka, zatim dohvaćanje, pohranjivanje i manipuliranje datotekama, usluge ulaz/izlaz (O/I) kod korištenja pisača i sličnih vanjskih uređaja, zaštitu sigurnosti i integriteta podataka. Također, uključuje i komunikaciju i dijeljenje podataka i programa na višekorisničkim i umreženim sustavima, daje informacije o statusu sustava i njegovim datotekama i pruža podatkovne i druge specijalizirane usluge za korisničke programe (The users view of operating systems, s.a.).

OPERACIJSKI SUSTAV SA ASPEKTA SUSTAVA

Što se tiče aspekta operacijskog sustava od strane samog računalnog sustava, radi se o tome da je operacijski sustav povezan s računalnim sklopovljem, tj. *hardware*-om. Prema tome, zadatak operacijskog sustava je raspodijeliti i alocirati resurse, npr: memorijski prostor, prostor za pohranu datoteka, CPU, I / O uređaja i drugo. Tu operacijski sustav upravlja navedenim resursima i mora odlučiti o tome kako ih dodijeliti specifičnim programima i korisnicima kako bi mogao učinkovito i pravedno upravljati računalnim sustavom. Također, u ovom je slučaju operacijski sustav, sustav kontrole jer mora kontrolirati rad uređaja i korisničkim programa kako bi se spriječile pogreške u radu računala[5].

PRAVA I KONTROLA PRISTUPA

Jedna od glavnih funkcija svakog računalnog sustava je pohranjivanje informacija te je preporučljivo da se takve informacije zaštite od napada, prijetnji i drugih vrsta štete. Pod prijetnjama se smatraju i neovlašteni pristupi od strane raznih korisnika te kontrola istih koju vlasnici računala

[4] Silberschatz, Bear, Gagne, 2014

[5] Ibid

imaju. Zaštita informacija može biti ostvariva na više načina. Prema tome, postoje različita prava pristupa unutar operacijskog sustava koja korisnici imaju prilikom korištenja računala. Postoji nekoliko različitih vrsta operacija koje se mogu kontrolirati: čitanje, pisanje, izvršavanje, brisanje, dodavanje, pregledavanje, preimenovanje, kopiranje, uređivanje[6].

Prava, odnosno kontrola pristupa označavaju prava korištenja određenih resursa u računalnom sustavu. Prema tome, korisno je grupirati datoteke prema važnosti, odnosno odrediti koje datoteke se ne otvaraju ili ne mogu mijenjati od strane neovlaštenog osoblja. To se također odnosi i na programe koji se izvode u operacijskom sustavu. Postoje dva aspekta kontrole pristupa, a to su: politika kontrole pristupa (engl. Access control policies) i mehanizmi kontrole pristupa (engl. Access control mechanisms).

POLITIKA KONTROLE PRISTUPA

Politika kontrole pristupa definira koje podatke je potrebno zaštititi i od koje osobe. Najčešće se postavlja matrica pristupa u kojoj redovi definiraju korisnike, a stupci definiraju datoteke ili direktorije kome koji korisnik može pristupiti. U matrici se može pojaviti vrijednost nula što znači da je zabranjen pristup određenoj datoteci ili direktoriju nekom korisniku. Veća vrijednost od nule definira koja je vrsta pristupa dopuštena određenom korisniku za čitanje, pisanje ili izvršavanje zadataka.

Model prema kojem se definiraju prava pristupa je već spomenuta matrica i pruža okvir za opisivanje kontrole pristupa. Izvorno je matrica prikazivala stanja autorizacije što znači ovlaštenja koja korisnik ima u određenom vremenu u računalnom sustavu. Matrica kao takva daje apstraktni prikaz sustava zaštite. Prvi korak u razvoju sustava kontrole pristupa je identifikacija objekata koji se žele zaštititi, tj. subjekata koji obavljaju zadatke i zahtijevaju pristup objektima i radnje koje se nad njima mogu izvršiti te oni moraju biti zaštićeni. Subjekti, objekti i radnje mogu biti različite ovisno o sustavu ili njihovim primjenama. Ako se uzme za primjer zaštita operacijskog sustava, objekti su obično datoteke, direktoriji ili programi. S druge strane, kod baza podataka objekti mogu biti odnosi ili veze, tj. pohranjene procedure. Subjekti su oni koji izvršavaju zadatke. Na slici u nastavku nalazi se primjer matrice kontrole pristupa.

	Datoteka 1	Datoteka 2	Datoteka 3	Program
Korisnik	Admin Čitanje Pisanje	Čitanje Pisanje		Izvršavanje
Korisnik 2	Čitanje		Čitanje Pisanje	
Korisnik 3		Čitanje		Izvršavanje Čitanje

Slika 1. Matrica kontrole pristupa

[6] Ibid

Općenito je matrica kontrole pristupa velike veličine jer je veliki broj polja prazno. Spremanje matrice kao dvodimenzionalno polje je bespotrebno korištenje memorije stoga postoje tri pristupa implementacije matrice na praktični način: autorizacija, popis kontrole pristupa i sposobnost. Autorizacija govori da popunjeni unosi unutar matrice su prikazani u tablici sa tri stupca koje odgovaraju predmetima, akcijama i objektima. Svaka tablica unutar glavne tablice odgovara autorizaciji. Pristup tablici ovlaštenja koristi se u sustavima baza podataka gdje su ovlaštena pohranjena kao relacijske tablice u bazi podataka.

Popis kontrole pristupa definira spremljenost matrice po stupcima. Svaki je objekt povezan s popisom koji označava za svaki subjekt i radnju koju subjekt može obavljati na objektu. Takav popis kontrole naziva se ACL (engl. Access control list) i ima mnoge prednosti i nedostatke kada se govori o zaštiti operacijskog sustava. Popis kontrole pristupa je prirodni izbor u okruženjima u kojima korisnici upravljaju vlastitom sigurnosnom datotekom te postaju široko rasprostranjeni u Unix sustavima. U Windows operacijskim sustavima se također koriste popisi kontrole pristupa, no s vremenom su oni postali složeniji. Popisi kontrole su jednostavni za implementaciju međutim nisu dovoljno učinkoviti kao način provjere sigurnosti tijekom izvođenja jer operacijski sustavi znaju tko koristi određeni program. Operacijski sustav mora provjeriti popis kontrole pristupa prilikom svakog pristupa datotekama ili mora pratiti aktivna prava pristupa na neki drugi način[7].

U operacijskom sustavu Unix, tj. Linux datoteke ne smiju imati proizvoljne popise za kontrolu pristupa već imaju jednostavne r-w-x atribute za vlasnike datoteka, grupu i ostalo (engl. Public). Atributi r-w-x omogućuju redom čitanje, pisanje i izvršavanje datoteke. Popis kontrole pristupa prikazuje da li se datoteka nalazi u direktoriju i zatim joj je dodijeljen atribut za čitanje, pisanje i izvršavanje. Za razliku od Unixa, kod Windows operacijskog sustava je situacija nešto složenija. Kod njega umjesto čitanja, pisanja i izvršavanja, postoje atributi za preuzimanje vlasništva, promjene dozvola i brisanje što znači da se može podržati fleksibilnije delegiranje. Navedeni se atributi primjenjuju na grupe i korisnike. Atributi nisu uključeni i isključeni kao na Unixu već imaju više vrijednosti pa se može postaviti: *AccessDenied, AccessAllowed*, ili *SystemAudit*. Kada je postavljen *AccessDenied* za nekog korisnika ili grupu, tada nije dopušten pristup bez obzira na to ako je postavljen *AccessAllowed*.

Zadnji pristup je sposobnost koja označava pohranu matrice po redovima. Svakom korisniku je pridružen popis koji se naziva popis sposobnosti i označava da svaki korisnik ima dopuštenje za obavljanje radnje nad određenim objektom. Operacijski sustav također podržava prava pristupa na razini grupa ili uloga te se takve mogućnosti implementiraju unutar aplikacijskog koda[8].

[7] Needham, 2008

[8] Silberschatz, Bear, Gagne, 2014; Samarati, Capitani de Vimercati, 2000.

MEHANIZMI KONTROLE PRISTUPA

Drugi aspekt kod kontrole pristupa su mehanizmi kontrole pristupa te postoje tri vrste, a to su: DAC (engl. Discretionary Access Control), MAC (engl. Mandatory Access Control) i RBAC (engl. Role Based Access Control). Negdje se navodi i četvrta vrsta: RBAC (engl. Rule Based Access Control) te će ona također biti opisana u nastavku.

Diskretna kontrola pristupa (DAC) je model kontrole pristupa koji se temelji na korisnikovoj diskreciji, tj. vlasnik resursa može dati pristupna prava na taj resurs nekim drugim korisnicima na temelju njegove diskrecije. Kako su mehanizmi kontrole pristupa povezani s popisom kontrola pristupa, navedeni ACL u prethodnom poglavlju se odnosi upravo na diskretnu kontrolu pristupa. Kod njega se određuju dozvole za čitanje, pisanje i izvođenje (r-w-x) na Unix operacijskim sustavima. Upravo se Unix temelji na DAC modelu. U takvim operacijskim sustavima se prilikom kreiranja datoteke odlučuje koje privilegije i prava pristupa se želi dati korisnicima kada pristupaju vlasničkoj datoteci, a operacijski sustav donosi odluku o kontroli pristupa temeljem stvorenih privilegija. Pored toga što vlasnik resursa određuje tko ima pristup, on također može mijenjati i izbrisati svaku datoteku u kojoj korisnik ima pristup. Procesi koji dovode do takvih privilegija imaju ovlasti mijenjati ili izbrisati datoteke sustava što predstavlja jedan od nedostatka ovakvog mehanizma.

Obavezna kontrola pristupa (MAC) je model u kojem korisnici, tj. vlasnici nemaju prava i privilegije za pristup svojim datotekama. U ovom slučaju, za razliku od diskretne kontrole pristupa, operacijski sustav je taj koji odlučuje o privilegijama pristupa. U tom su modelu svaki subjekt (predmet, korisnik) i objekt (resursi) kvalificirani i dodijeljena im je sigurnosna oznaka. Sigurnosne oznake predmeta i objekta zajedno sa sigurnosnom politikom određuju može li subjekt pristupiti objektu. One sadrže dva dijela informacija: klasifikaciju i kategoriju. Pod klasifikacijom se definiraju podaci poput vrhunski, tajni, povjerljivi itd. dok u kategoriju spadaju podaci poput pokazatelja razine uprave ili nekog odjela ili projekta na kojem se nalazi objekt. Pravila prema kojem se definiraju prava pristupa subjekta određenom objektu konfigurirane su od strane administratora koji je zadužen za operacijski sustav i podržava sigurnosne tehnologije. Takav model je obično stroži i statičan model kontrole pristupa u usporedbi s diskretnom kontrolom pristupa te je prikladan najčešće za vojne organizacije u kojima je klasifikacija podataka i povjerljivost istih vrlo bitna. Što se tiče operacijskih sustava, na MAC modelu se temelje posebne vrste Unix-a. Dakle, takav model je najstroži od svih modela kontrole pristupa. MAC preuzima hijerarhijski pristup za kontrolu pristupa resursima. Kao takav, svi pristupi objektima strogu su kontrolirani od strane operacijskog sustava temeljenog na konfiguriranim postavkama od strane administratora sustava. Kao što je već ranije spomenuto, korisnici ne mogu promijeniti prava pristupa. Također, svaki korisnički račun na sustavu ima svojstva klasifikacije i kategorije iz istog skupa svojstva koja se primjenjuju na

objekte resursa. Kada korisnik pokuša pristupiti resursu pod obaveznom kontrolom pristupa, operacijski sustav provjerava klasifikaciju i kategorije korisnika i uspoređuje ih sa svojstvima sigurnosne oznake objekta. Ako se sigurnosne oznake korisnika podudaraju sa sigurnosnim oznakama objekta prema MAC modelu, dopušteno je korisniku upravljati resursima. Uz to, važno je da se kategorija i klasifikacija podudaraju. Korisnik s vrhunskom tajnom klasifikacijom ne može pristupiti resursu ako nije član jedne od traženih kategorija za taj objekt. Nadalje, MAC model zahtjeva veliku količinu planiranja prilikom njegova definiranja, no jednom kada je implementiran omogućuje visoki nadzor unutar sustava.

Treći mehanizam je RBAC, odnosno kontrola pristupa prema ulogama. To je model u kojem prava pristupa nekom resursu imaju određeni korisnici ovisno o njihovim ulogama koje posjeduju unutar organizacije. Model je poznat kao nediskretna kontrola pristupa jer korisnik nasljeđuje privilegije vezane uz njegovu ulogu te uz to, nema kontrolu nad ulogom koja će mu biti dodijeljena. Za provedbu modela RBAC postoje dva važna faktora: radi se o najmanjem principu privilegija gdje bi korisnik trebao imati minimalne ovlasti za obavljanje zadataka, i segregacija dužnosti gdje bi trebalo imati više od jednog korisnika za obavljanje važnog zadatka zbog smanjenja rizika od prijevara. Dakle, pristup prava pod ovakvim modelom temelje se na funkciji zadataka korisnika unutar organizacije kojoj pripada određeni računalni sustav. Korisnicima kojima je dodijeljena određena uloga ima prema tome takva prava pristupa. Uloge se razlikuju od grupa do grupa dok se korisnici mogu nalaziti u više grupa. Korisnik može imati samo jednu ulogu u organizaciji. Osim toga, ne postoji način pružanja dodatnih dozvola pojedinačnim korisnicima iznad onih koje imaju dostupne za svoju ulogu.

Zadnja spomenuta vrsta mehanizma kontrole pristupa je RBAC, odnosno kontrola prava pristupa na temelju pravila. Kod tog modela, pristup je odobren ili dopušten objektima na temelju skupa pravila koja su definirana od strane administratora sustava. Kao i kod diskretne kontrole pristupa, svojstva pristupa se pohranjuju u popisima kontrole pristupa (ACL) koji su povezani sa svakim resursnim objektom. Kada određeni predmet ili grupa nastoje pristupiti resursu, operacijski sustav provjerava pravila sadržana u popisu kontrola pristupa za taj objekt. No kao i u MAC modelu, korisnici ne mogu mijenjati kontrolu pristupa već su sva pristupna dopuštenja kontrolirana isključivo od strane administratora sustava[9].

ZAKLJUČAK

Operacijski sustav je dio računalnog sustava i upravlja njime na način da obavlja zahtjeve koje dobiva od strane korisnika ili programa. Preko operacijskog sustava je olakšano korištenje računalnog sustava zbog jednostavnog i pristupačnog grafičkog sučelja za svakog korisnika. Operacijski sustav je zapravo skup osnovnih programa koje omogućuju

[9] Rana, 2011

izvođenje radnji na računalu. Unutar operacijskog sustava moguće su razne operacije poput čitanja, pisanja, brisanja, izvršavanja, uređivanja i slično, a zbog zaštite podataka i informacija pohranjenih na računalu, takve informacije moraju biti zaštićene. Jedan od načina zaštite su i prava i kontrola pristupa.

Kontrola pristupa se razmatra s dva aspekta, politike i mehanizama kontrole pristupa. Što se tiče politike, radi se o modelima prema kojima se definiraju prava pristupa te su oni pohranjeni unutar matrice gdje je definirano koji korisnik može pristupiti kojem objektu, datoteci ili direktoriju. Subjekti, kao i objekti i resursi imaju različita prava ovisno o sustavu i njegovoj primjeni. Tu se još pojavljuje i popis kontrole pristupa gdje je svaki objekt povezan sa subjektom i radnjama koje subjekt može na njemu obavljati. S druge strane, tu su mehanizmi kontrole pristupa koji su povezani s politikom, a razlikuju se četiri vrste: diskretna kontrola pristupa, obavezna kontrola pristupa, kontrola pristupa prema ulogama i kontrola pristupa prema ulogama. Svaki od mehanizama doprinosi definiraju prava pristupa da bi se zaštitili pohranjeni podaci unutar računalnog sustava.

OPERATING SYSTEMS AND DATA CONTROL CONTROL

Marijan Mijatović, PhD

Abstract: Operating systems represent a complex that is very important in access dana control. In the operating system, the computer represents only one element of the computer system that performs basic functions. The operating system is commonly managed by one user, but it is not excluded that it can be managed by multiple users. One of the main functions of each computer system is to store information, but also to have adequate protection to keep this information as fully protected. When we talk about access control, we talk about three types of control mechanisms. These are the discrete control, mandatory access control and role-access control.

Key words: *operating system, information, access control*

LITERATURA

1. Jelenković L. (2017.): *Interni materijali za predavanja iz predmeta Operacijski sustavi*, Fakultet elektrotehnike i računarstva, Sveučilište u Zagrebu. Dostupno na http://www.zemris.fer.hr/~leonardo/os/fer/OS-skripta.pdf 11.1.2018.
2. Needham R. (2008.): *Access Control*, chapter 4., Cambridge Computer Laboratory. Dostupno na https://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c04.pdf 12.1.2018.
3. Pintarić N., Panjkota A., (s.a.): Informatika-programska podrška, Sveučilište u Zadru – odjel za ekonomiju. Dostupno na http://personal.unizd.hr/~apanjkot/vjezbe_inf/vjezbe_3_4.pdf 11.1.2018.
4. Rana M. (2011.): *Types of Access Control Mechanisms*, www.techmahindra.com blog. Dostupno na: https://www.techmahindra.com/sites/blogs/types_of_access_control_mechanisms.aspx 13.1.2018.
5. Samarati P., Capitani de Vimercati S, (2000.): *Access Control: Policies, Models, and Mechanisms*, Italija. Dostupno na https://link.springer.com/content/pdf/10.1007/3-540-45608-2_3.pdf 12.1.2018.

6. Silberschatz A., Bear Galvin P., Gagne G. (2014.): *Operating system concepts essentials*, Second edition, Wiley, United States of America. Dostupno na http://lib.sgu.edu.vn:84/dspace/bitstream/TTHLDHSG/2808/1/Operating_System_Concepts_Essentials.pdf, 11.1.2018.
7. The user view od operating systems (s.a.), chapter 16. Dostupno na http://www.kean.edu/~gchang/tech2920/http___professor.wiley.com_CGI-BIN_JSMPROXY_DOCUMENTDIRECTORDEV+DOCUMENTID&0471715425+DOCUMENTSUBID&1+PRFVALNAME&pdfs_ch16.pdf 11.1.2018.