Sigurnost Debian operacijskog sustava

Bobovec, Domagoj

Master's thesis / Diplomski rad

2016

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Rijeka, Faculty of Humanities and Social Sciences / Sveučilište u Rijeci, Filozofski fakultet u Rijeci**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:186:540462

SVEUČILIŠTE U RIJECI

FILOZOFSKI FAKULTET

ODSJEK ZA POLITEHNIKU

SIGURNOST DEBIAN OPERACIJSKOG SUSTAVA

- DIPLOMSKI RAD -

Domagoj Bobovec

Mentor: Doc.dr.sc. Božidar Kovačić

Rijeka, 2016.

Sveučilište u Rijeci
Filozofski fakultet
ODSJEK ZA POLITEHNIKU
u Rijeci
Sveučilišna avenija 4.

Povjerenstvo za završne i diplomske ispite

U Rijeci, 30. 4. 2016. god.

DIPLOMSKI ZADATAK

Pristupnik: **Domagoj Bobovec**

Zadatak: **Sigurnost Debian operacijskog sustava**

Rješenjem zadatka potrebno je obuhvatiti sljedeće:

1. Uvodni dio - Općenito o Linux operacijskim sustavima
2. Opisati povijesni razvoj operacijskih sustava Linux i objasniti osnovne funkcije operacijskog sustava Debian
3. Objasniti pojam sigurnosti operacijskog sustava i načine implementacije sigurnosti
4. Objasniti implementaciju sigurnosti u operacijskom sustavu Debian, sa posebnim osvrtom na zaštitu usluge elektroničke pošte
5. Navesti alate za implementaciju sigurnosti u operacijskom sustavu Debian i objasniti način korištenja jednog alata.
6. Metodički dio:
   - analizirati nastavni program srednje strukovne škole u sadržaju teme diplomskog rada
   - napisati pripremu za izvođenje nastave za pripadnu razinu kvalifikacije u skladu s HKO (Hrvatski klasifikacijski okvir).
7. Zaključak.

U diplomskom se radu treba obvezno pridržavati **Uputa za izradu diplomskog rada.**

Zadatak uručen pristupniku: **4.4.2016**

Rok predaje diplomskog rada: **23.9.2016**

Datum predaje diplomskog rada: **23.9.2016**

PREDSJEDNIK POVJERENSTVA ZA DIPLOMSKE ISPITE: **ZADATAK ZADAO:**

Prof.dr.sc. Zvonimir Kolumbić **Doc.dr.sc.Božidar Kovačić**

I. AUTOR

Ime i prezime: Domagoj Bobovec

Mjesto i datum rođenja: Koprivnica, 19. 11. 1988.

Adresa: Ferdinandovac, Dravska 20 A

FILOZOFSKI FAKULTET ODSJEK ZA POLITEHNIKU

II. DIPLOMSKI RAD

Naslov: Sigurnost Debian operacijskog sustava

Title: Security of Debian operating system

Ključne riječi: operacijski sustavi, Linux, Debian, sigurnost, GnuPG

Keywords: operating systems, Linux, Debian, security, GnuPG

Broj stranica: 45

Ustanova i mjesto gdje je rad izrađen: FILOZOFSKI FAKULTET, ODSJEK ZA POLITEHNIKU

Stečen akademski naziv: **Magistra edukacije politehnike i informatike**

Mentor rada: **Doc. dr. sc. Božidar Kovačić**

Obranjeno na **Filozofskom fakultetu, odsjeku za politehniku u Rijeci**

dana _____

Oznaka i redni broj rada: _____

IZJAVA

Izjavljujem da sam diplomski rad „Sigurnost Debian operacijskog sustava“ izradio samostalno koristeći se vlastitim znanjem i navedenom literaturom.

U radu mi je savjetima i uputama pomogao voditelj i mentor diplomskog rada, doc. dr. sc. Božidar Kovačić, te mu se na tome iskreno zahvaljujem.

Također se zahvaljujem svim profesorima koji su mi držali predavanja ili mi na bilo koji način pomogli svojim znanjem, uputom ili savjetom. Također se zahvaljujem tajnici Odjela za politehniku na pomoći prilikom studiranja.

Na kraju se zahvaljujem svojoj obitelji na svesrdnoj pomoći, podršci i odricanju, te svim kolegama koji su na bilo koji način pridonijeli mom završetku studiranja.

Domagoj Bobovec

_____

SAŽETAK

Diplomski rad pod naslovom „Sigurnost Debian operacijsog sustava“ podijelio sam na šest područja. Uvodno sam opisao problematiku Linux operacijskih sustava i dao pregled njegovih distribucija i grafičkih okruženja.

Iduće područje se bavi poviješću Linux operacijskih sustava, te općenito opisuje Debian operacijske sustave, te navodi njegove osnovne funkcije.

Sljedeće poglavlje se bavi pojmom sigurnosti, vrstama napada na sigurnost te načinima implementacije sigurnosti. Opisuje se na koji se način Linux operacijski sustav može obraniti od napada.

Zatim se bavimo implementacijom sigurnosti u Debian operacijski sustav te detaljno opisujemo na koji način možemo osigurati sigurnost emaila koristeći GnuPG alat. Implementacija sigurnosti emaila sustava korištenjem GNU Privacy Guarda. Opisujemo postavljanje ključa, stvaranje certifikata opoziva, te kriptiranje i dekriptiranje.

Na kraju je metodički dio u kojemu radimo analizu nastavnog programa srednje strukovne škole te pripremamo za nastavu za predmet „Sustavna programska potpora“ za 4. razred tehničke škole, smjer tehničar za elektroniku.

POPIS SLIKA

Slika 1. Tux – službena maskota Linux kernela……..……..…..3

Slika 2. Ken Thompson i Dennis Ritchie……..…….6

Slika 3. Richard Stallman i Linus Torvalds……..…..9

Slika 4. Debian 7.9 s KDE grafičkim okruženjem……10

Slika 5. Debian logotipovi: (a) vir iznad duhove boce (službeni);

(b) samostalni vir (javna upotreba)……...….11

Slika 6. Unix kernel…….……13

Slika 7. Struktura Linux sustava…….…..14

Slika 8. Slanje digitalnih dokumenta……...….16

Slika 9 Proces slanja elektroničke pošte……...……22

Slika 10 Logotip GnuPG programa …….……23

Slika 11. Shematski prikaz obrazovanja u RH…….……30

SADRŽAJ

Izjava ……..I
Sažetak ……..……II
Popis slika ……..……III
1. UVOD ……..……..….. 1
1.1 Općenito o operacijskim sustavima……..……...2
1.2 Općenito o Linux operacijskim sustavima……..….3
1.3 Pregled distribucija i grafičkih okruženja Linux operacijskih sustava……...4
2. DEBIAN OPERACIJSKI SUSTAV…….……..…6
2.1. Povijest razvoja Linux operacijskih sustava……....…….…..6
2.2. Općenito o operacijskom sustavu Debian…….……..…...…10
2.3 Osnovne funkcije Debian Operacijskog sustava…….…..….13
3. SIGURNOST OPERACIJSKOG SUTAVA……..……..15
3.1 Pojam sigurnosti operacijskog sustava……...15
3.2. Implementacija sigurnosti operacijskog sustava……...16
4. IMPLEMENTACIA SIGURNOSTI U OPERACIJSKOM SUSTAVU DEBIAN……..18
4.1.Metode napada……...18
4.2. Zaštitne police……..….19
4.3. Standardni mehanizmi zaštite pod UNIX/Linux sistemom……..…20
4.4 LILO i datoteka /etc/lilo.conf…….21
4.5. Zaštita sigurnosti elektroničke pošte…….…22
5. ALATI ZA IMPLEMENTACIJU SIGURNOSTI U DEBIAN OPERACIJSKOM SUSTAVU…….23
5.1. Implementacija sigurnosti emaila sustava korištenjem GNU Privacy Guarda……..23
5.2. Postavljanje GnuPG ključa……24
5.3. Stvaranje certifikata opoziva……..25
5.4. Učitavanje ključeva drugih korisnika…….…26
5.5 Potvrda identiteta…….....26
5.6. Enkripcija i dekripcija poruka sa GnuPG-om…….28
6. METODIČKI DIO……..29
6.1. Analiza nastavnog programa srednje strukovne škole……..…..29
6.1.2 Obrazovanje za zanimanje Tehničar za računalstvo……..32
6.2. Priprema za izvođenje nastave za pripadnu razinu kvalifikacije u skladu s HKO……..33
7. ZAKLJUČAK……44
8. POPIS LITERATURE…….45

UVOD

Tema diplomskog rada je sigurnost Debian operacijskog sustava. U ovome radu obradio sam pojam i vrste operacijskih sustava. Zatim sam se fokusirao na Linux operacijske sustave. Predstavio sam povijesni razvoj Linux operacijskih sustava i nihovih grafičkih okružnja. Zatim sam govorio općenito o svojstvima Debian operacijskog sustava, te naveo njegove osnovne funkcije. Prikazao sam način implementacije sigurnosti u Debian operacijskom sustavu. Praktično sam obradio zaštitu emaila pomoću alata GNU Privacy Gurad. Njegova svrha je kriptiranje i dekriptiranje emaila.

Na poslijetku sam napravio analizu programa srednje strukovne škole, prikazao strukturu obrazovanja. Na kraju sam se usmjerio za zanimanje Tehničar za računalstvo te za njega izradio pripremu za izvođenje nastave za pripadnu razinu kvalifikacije u skladu s HKO.

1.1 Općenito o operacijskim sustavima

Operacijski sustav (operating system, OS) je naziv za skup programa koji upravljaju računalnim sustavom. Aktivnosti su mu usmjerene na upravljanje hardverom i aplikativnim softverom. S korisničkog gledišta ima ulogu sučelja putem kojeg korisnik koristi računalo. Svrha operacijskih sustava je osigurati okruženje u kojem će korisnici izvršavati svoje programe. Kao primarni cilj operacijskih sustava može se navesti pojednostavljenje upotrebe računala za samog korisnika, dok je sekundarni cilj koristiti hardver što je moguće učinkovitije. Često su ova dva cilja bila suprotstavljena – u prošlosti se važnijim smatrala efikasnost nego ugodnost korištenja računala od strane korisnika. Ta se situacija promijenila zahvaljujući brzom širenju računalne tehnologije ne samo na znanstvenike i računalne entuzijaste nego i na obične građane. Novi operacijski sustavi žele biti što je moguće lakši za korištenje krajnjem korisniku (engl. user–friendly).

Datoteke unutar operacijskog sustava su povezane tako da su pohranjene u direktorij. Hijerarhijska struktura direktorija unutar operacijskog sustava se još naziva i stablo. Oni direktoriji koji se nalaze u nekom drugom direktoriju se nazivaju poddirektoriji ili subdirektoriji. Često se veze između direktorija opisuju i izrazima roditelj (engl. parent) i dijete (engl. child). Direktorij u kojem su sadržani svi direktoriji prisutni u u datotečnom susstavu, a da se on sam ne nalazi niti u jednom direktoriju se zove se korijenski ili root direktorij.

Prema obliku hijerarhijske strukture operacijski sustavi se mogu podijeliti na:

- višekorijenske operacijske sustave i
- jednokorijenske operacijske sustave

Višekorijenski operacijski sustavi, kao što im ime govori, imaju više korijenskih direktorija. Primjer su operacijski sustavi Windows kod kojega su particije označene npr: C:\ , D:\ , E:\ … Jednokorijenski operacijski sustavi koriste unificirani datotečni sustav, odnosno svi se uređaji za pohranu nalaze pod istim stablom direktorija. Primjer su Unix i njemu slični operacijski sustavi poput Linux-a. Vrh stabla datotečnog sustava je kao što sam već spomenuo korijen, a označava se znakom / .

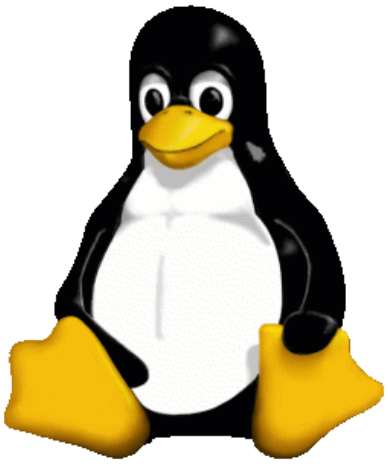
1.2 Općenito o Linux operacijskim sustavima

Linux je prvotno naziv za jezgru ili kernel računalnoga operacijskog sustava sličnog Unixu. Ipak, danas se taj naziv najčešće odnosi na cijeli operacijski sustav, što je dio kontroverze oko samog imena. Naime, operacijski sustav je nastao kad je Linux jezgra uklopljena u GNU operacijski sustav umjesto nedovršene jezgre imena Hurd. Zbog toga postoji nesuglasica gdje dio Zaklade za slobodan softver zahtjeva da je ispravan naziv GNU/Linux, dok većina zajednice zajedno sa tvorcem jezgre to odbacuje. Zbog jednostavnosti u ovom radu ću operacijski sustav jednostavno zvati Linux.

Operacijski sustav Linux se može definirati kao višekorisnički, višeprocesni operacijski sustav sa potpunim skupom UNIX kompatibilnih alata, projektiran tako da poštuje relevantne POSIX standarde. To su sustavi koji podržavaju tradicionalnu UNIX semantiku te potpuno implementiraju standardni UNIX mrežni model. [1]

Linux je slobodni softver otvorenog koda, što znači da ga svatko može besplatno koristiti, kopirati i modificirati. Za razliku od komercijalnog softvera baziranog na autorskim pravima, Linux-ov je kod javno raspoloživ i može biti modificiran po potrebama korisnika. Zbog toga razvoju operacijskih sustava Linux može pridonijeti bilo tko, i razvija se suradnjom entuzijasta i volontera širom svijeta. Može se reći da su Linux operacijski sustavi najfleksibilniji i najefikasniji, pa čak i najperspektivniji operacijski sustavi baš zbog toga jer ih je moguće prilagoditi vlastitim željama svakog korisnika.

Osim u osobnim računalima Linux operacijski sustavi su našli primjenu u mobilnim uređajima, igraćim konzolama, automobilima, pa i kućanskim aparatima.



Slika 1. Tux – službena maskota Linux kernela [2]

1.3 Pregled distribucija i grafičkih okruženja Linux operacijskih sustava

Zbog toga što je Linux operacijski sustav slobodan softver razvijeno je na stotine različitih distribucija prilagođenih pojedinim korisniku, poduzeću ili serveru. Većina distribucija ima grafičko okruženje, dok neke distribucije namijenjene programerima i sistemskim administratorima koriste tradicionalno UNIX okruženje. Svaka od distribucija ima svoje prednosti i mane.

Deset najpopularnijih Linux distribucija sortiranih od najpopularnijeg su [3]:

- Linux Mint – distribucija bazirana na Ubuntu, razvija mnogo „minty“ alata;
- Ubuntu – nastao iz Debiana, preporučljiv početnicima, mnogo dokumentacije;
- Debian – veoma stabilan i temeljito testiran, spor razvoj novih verzija, ne preporuča se početnicima;
- Mageia – nastalo iz Red Hat, superiorni administracijski alati, preporuča se početnicama;
- Fedora – os također nastao iz Red Hat-a, inovativan i siguran, više za developere;
- openSuse – intuitivni konfiguracijski alati, prilagođen krajnjim korisnicima, privlačna grafička sučelja;
- Arch Linux – odlično upravljanje softverom i mogućnosti prilagodbe superiorna dokumentacija, ponekad nestabilan;
- CentOS – Nastao iz Red Hat-a, vrlo stabilan i temeljito testiran, manjka najnovije Linux tehnologije, spor razvoj novih verzija;
- PCLinuxOS – Nastao iz Mandrake-a, prilagođen korisnicima koji prelaze s Windows u Linux okruženje;
- Slackware Linux – visoko tehnička, „čista“ distribucija, ograničen broj izvršnih programa;
- FreeBSD – visoke performanse i stabilnost, ograničena hardverska podrška, ne preporuča se početnicima

Što se tiče grafičkih okruženja, također postoji veliki izbor. Za razliku od tema u operacijskom sustavu Windows, svako grafičko okruženje izgleda i ponaša se različito od drugog. Neka od njih su hardverski zahtjevnija od drugih. Ipak, jezgra Linuxa je odvojena od grafičkog okruženja, te ako se i sruši određena aplikacija, to neće utjecati na sam operacijski sustav.

Najpopularnija grafička okruženja za Linux su:

- GNOME (trenutačno najpopularnije);
- KDE, (možda trenutačno najnaprednije);
- XFCE (hardverski nezahtjevno);
- LXDE (hardverski nezahtjevno);
- Cinamon (izvedenica GNOME-a);
- Unity (hardverski najzahtjevnije)…

2. DEBIAN OPERACIJSKI SUSTAV

2.1. Povijest razvoja Linux operacijskih sustava

Počeci Linux operacijskog sustava vezani su za UNIX operacijski sustav koji se može smatrati njegovom pretečom. UNIX je nastao firmi Bell Laboratories gdje su ga razvili znanstvenici Ken Thompson i Dennis Ritchie. 1969. godine Thompson je provodio eksperimente sa datotečnim sustavom na računalu PDP_7 te je rezultat bio UNIX operacijski sustav. Prvi radni UNIX sustav pisan je u asembleru te je bio izrađen 1971. godine. 1973. je od početka napisan u programskom jeziku C. Ta nova verzija je bila za trećinu veća od verzije UNIX-a u asembleru. Ipak, bila je puno lakša za razumijevanje, prepravljanje i instaliranje.

Do 1974. godine bilo je u upotrebi oko 150 instalacija UNIX-a. Iste godine je prekretnicu u širenju UNIX operacijskih sustava pokrenulo instalacija UNIX-a na 16-bitno miniračunalo PDP_11/70 sa 768Kx8 memorijskih lokacija. Kao masovna memorija su korišteni diskovi kapaciteta 2×200 Mb.[4]

Slika 2. Ken Thompson i Dennis Ritchie [5]

1980. godine UNIX je bio instaliran na oko 2000 računala diljem svijeta. Ta je brojka sredinom 1980-ih godina porasla na stotine tisuća računala širokog spektra, te oko 1500 sveučilišta. UNIX operacijski sustavi su napravili proboj, te su se koristili od mikroračunala do

superračunala. U to vrijeme stotinjak kompanija su razvijale aplikacije za UNIX, a sam operacijski sustav je proizvodilo sedamdesetak. Sredinom 1990-ih godina broj instalacija UNIX-a diljem svijetu narastao je na milijune instalacija. U to vrijeme koristio je mrežno sučelje TCP/IP, grafičko sučelje X Window System i veliku količinu javno dostupnih aplikacijskih programa. Zbog toga postaje postaje poznat kao operacijski sustav za koji vrijede svojstva kao što su prenosivost (eng. portability), prilagodljivost (eng. scalability) i suradnja (eng. interoperability).[4]

Prenosivost je mogućnost instalacije operacijskog sustava na različite sklopovske platforme. Prilagodljivost znači da operacijski sustav može raditi na različitim vrstama računala; od skromnijeg kućnog, sve do superračunala. Pod suradnjom se misli na razmjenu informacija između računala i čovjeka.

Nakon 1977. godine razvoj UNIX operacijskih sustava se dijeli u tri smjera[4]:

- Prvi je bio usavršavanje i nastavak razvoja u AT&T Bell Laboratories što je rezultiralo UNIX System V operacijskim sustavom kao normom. Osnovna ljuska u UNIX System V sustavu je „Bourne Shell“.

- Drugi je razvoj UNIX-a na Sveučilištu Berkeley (UCB) u Kaliforniji. Tamo se UNIX razvijao na računalima VAX_11/780 te su mu dodali programsku podršku za virtualnu memoriju. Ova inačica UNIX-a poznata je kao 3BSD (eng. Berkeley Software Distribution). Nove inačice su razvile razna poboljšanja i modifikacije poput kontrole procesa u prvom planu ili foreground-u te u pozadini ili background-u, ljusku za posredovanje između korisnika i operacijskog sustava BSD shell, zaslonski editor (vi) te automatsko „podizanje“ sustava nakon prekida rada.

- Treći je prilagodba i razvoj UNIX operacijskih sustava za različita računala. Javljaju se razne ideje kako koristiti UNIX na računalima koja nemaju svu potrebnu sklopovsku opremu, uglavnom zbog komercijalnih razloga. Jedne inačice UNIX-a su podskup funkcija i svojstava koje ima originalni UNIX (npr. TNIX),dok druge oponašaju osnovne ideje UNIX operacijskih sustava poput hijerarhijske organizacije datoteka i sl. (npr. CROMIX). Na kraju se je pojavila težnja za normiranjem UNIX-a, uglavnom kod proizvođača računalne opreme. Cilj je bio da korisnik, bez obzira koje računalo koristi, osjeća se u istom UNIX-ovom okruženju. Također, javljaju se različite interesne skupine korisnika koje nastoje zaštititi svoje interese.

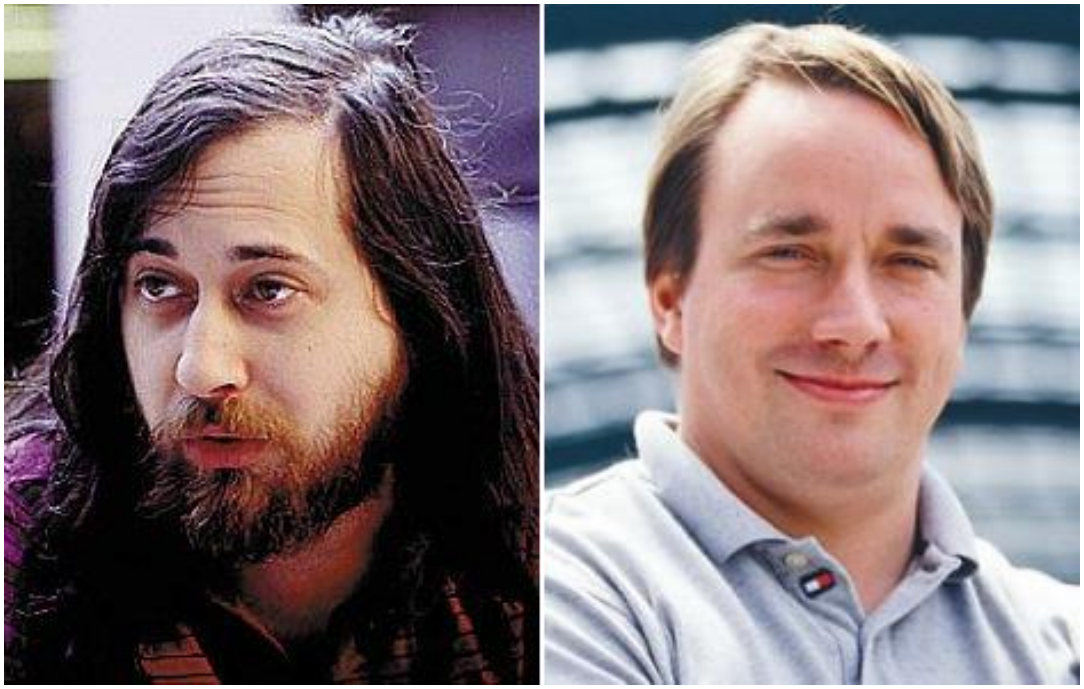
Vrlo važna osoba koja je pridonijela razvoju Linux operacijskih sustava je Richard Stallman. On se odlučio suprotstaviti trendu pretvaranja Unix-a u vlasnički softver. Stallman je počeo svoju programersku karijeru na MIT-u u Laboratoriju za umjetnu inteligenciju, kada je još bio student na Harvardu. Tada je tamo bila prisutna hakerska zajednica u kojoj se slobodno dijelio programski kod. Kada su tvrtke prestale objavljivati izvorni kod svojih programa, ta se zaejdnica počela raspadati. To je Stallmana uvjerilo da korisnik mora imati slobodu mijenjanja izvornog koda programa koje koristi. Započeo je rad na slobodnom operacijskom sustavu sličnom Unix-u, te su mu se pridružili mnogi programeri. Tako je nastao projekt GNU (engl. GNU's Not Unix) koji znači GNU nije Unix. Stallman je 1983. godine napustio MIT te utemeljio Zakladu za slobodni softver (engl. Free Software Foundation, FSF). Ona i danas postoji i najutjecajniji je zagovornik slobodnog softvera.

Neovisno o GNU projektu, tada student Linus Benedict Torvalds izradio je Linux operacijski sustav za vlastite potrebe. Odlučio se za taj potez, jer se na Minix operacijskom sustavu radi licence nije mogao mijenjati ili prilagoditi izvorni kod. Započeo je s pisanjem terminal emulatora kojeg je koristio za spajanje na veće UNIX sustave na svome fakultetu. Taj je terminal napredovao te je prerastao u kernel. Prvu verziju je 1991. godine objavio na Internetu uz poznatu izjavu u kojoj sumnja da će Linux ikada prerasti u nešto veće [6]:

Od: torvalds@klaava.Helsinki.FI Linus Benedict Torvalds)
Newsgroup: comp.os.minix
Predmet: Što biste najviše željeli vidjeti na minixu?
Sažetak: mala anketa za moj novi operativni sustav
ID-poruke:<1991Aug.25.205708.9541@klaava.Helsinki.FI)
Datum:25. Aug 91 20:57:08 GMT
Ustanova: Sveučilište u Helsinkiju
Pozdrav svim korisnicima minixa -
Radim na (besplatnom) operacijskom sustavu (samo hobi, neće biti
nešto veliko i profesionalno kao gnu) za 386(486) AT klonove. Sustav se od
travnja polako krčka i polako ulazi u završnu fazu. Volio bih vaše mišljenje
o tome što volite/ne volite u minixu, budući da mu je moj OS donekle sličan
(isti fizički raspored datoteka (zbog praktičnosti)
između ostalog) Trenutno sam prenio bash(1.08) i gcc (1,40)
i izgleda da stvari rade.To znači da ću kroz nekoliko mjeseci
uspjeti dobiti nešto iskoristivo i volio bih znati što bi ljudi najviše htjeli. Svi
prijedlozi su dobrodošli, ali ne mogu obećati da ću ih i uključiti. :-)
Linus (torvalds@kruuna.helsinki.fi)
PS. Da-na njemu nema minix koda i koristi višenitni datotečni sustav.
NIJE portabilan (koristi 386 prebacivač zadataka) i vjerojatno nikada neće podržavati ništa osim AT hard diskova,
budući da imam samo takav :-(.

Naravno, ispostavilo se da je imao krivo. Linux jezgra je uklopljena u GNU operacijski sustav, te je na taj način nastao novi operacijski sustav. Kao što sam već ranije spomenuo, to je kasnije dovelo do kontroverze oko imena operacijskog sustava. U počecima Linux se upotrebljavao kao eksperimentalni sustav koji su koristili računalni entuzijasti i studenti. Šira komercijalna upotreba nije postojala. S nastankom Apache Web Servera to se promijenilo, jer je Linux u kombinaciji s njim pružio pouzdan i besplatan operacijski sustav za pogon mnoštva web stranica.

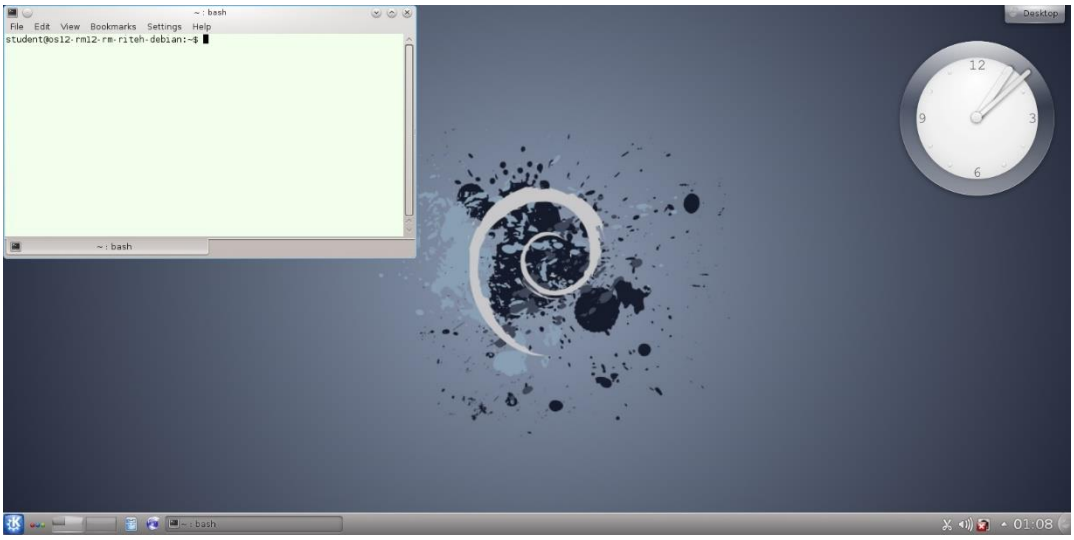
Danas Linux operacijski sustav podržava razne procesorske arhitekture te je dominantan na tržištu servera i superračunala. Najzanimljivije svojstvo Linuxa je to što je besplatan operacijski sustav koji je razvijan putem Interneta suradnjom dobrovoljaca, te svatko može pridonijeti njegovom razvoju. [4]



Slika 3. Richard Stallman i Linus Torvalds [7]

2.2. Općenito o operacijskom sustavu Debian

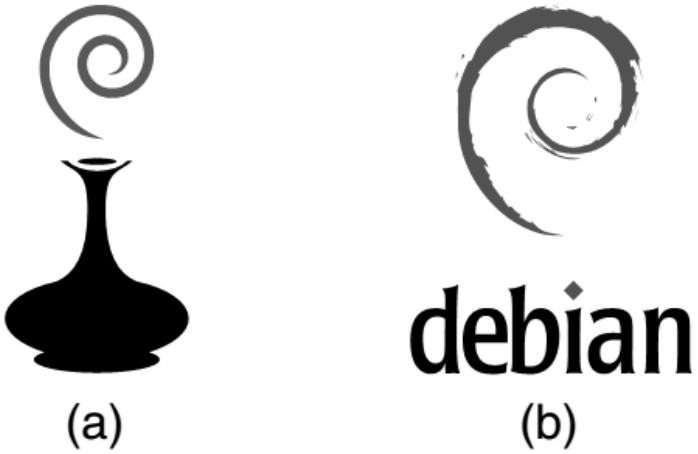
Debian je Unix-u sličan Linux operacijski sustav. Baziran je na Linux kernelu i besplatnom softveru, velikim dijelom iz GNU projekta. Osnovao ga je Ian Murdock 1993. godine kao posve nekomercijalni projekt koji razvijaju stotine programera u slobodno vrijeme. To su volonteri koji ne primaju nikakvu naknadu za svoj rad. Prilikom stvaranja Debiana Ian Murdock je imao jesne ciljeve koje je izrazio u Debian Manifestu. Operacijski sustav kojeg je razvijao morao je imati dvije glavne značajke. Prva je kvaliteta, i razvitak Debiana s najvećom pažnjom tako da bude vrijedan Linux kernela. Druga značajka je nekomercijalna distribucija, dovoljno uvjerljiva da se natječe s glavnim komercijalnim distribucijama. Prema njegovom uvjerenju, te dvije značajke su se mogle ostvariti samo otvaranjem Debianovog razvojnog procesa, poput Linux i GNU projekta. Na taj način povratna informacija kolega konstantno unaprjeđuje proizvod.[8]



Slika 4. Debian 7.9 s KDE grafičkim okruženjem

Ime Debian je nastalo kao spoj imena Iana Murdocka i njegove tadašnje djevojke, a kasnije žene Debre. Debtra + Ian = Debian. Debian operacijski sustav ima u stvari dva loga. Službeni Debian logotip je crveni vir koji lebdi iznad duhove boce, te se koristi samo za službene dijelove Debian projekta te od strane Debian razvojnog tima u službenim funkcijama. Neslužbeno, projekt ili operacijski sustav može predstavljati samo vir koji je znan kao Logotip za slobodno korištenje (engl. Open Use Logo). Ispisani naziv „Debian“ je opcionalan za oba logotipa. Prikaz obje vrste Debian logotipa prikazan je na slici 5. Svrha logotipa je zaštita

Debianovog vlasništva od bilo kakve upotrebe koja bi mogla naškoditi njegovoj reputaciji. Dizajnirao ih je Raul M. Silva ss kojim je sudjelovao u natjecanju 1999. godine. Raul nikad nije dao službenu izjavu o značenju ili simbolizmu logotipa, te se pojavilo nekoliko teorija: da boca predstavlja kolektiv programera, a rezultat je magični vir koji simbolira Debian operacijski sustav; da vir predstavlja zatvorenost kruga i ujedno fleksibilnost spirale kao što operacijski sustav mora biti fleksibilan; da vir predstavlja kako Debian u sebe uvlači svakovrstan softver, a boca pripada korisnog Debian Duha. Brice Perens je ponudio sljedeće objašnjenje: Radi se o „magičnom dimu“ koji izlazi iz elektroničke komponente kada pregori; a kada dim ode komponenta više ne radi. Debian predstavlja „magični dim“ koji omogućava da računalo radi. [9]



Slika 5. Debian logotipovi: (a) vir iznad duhove boce (službeni);

(b) samostalni vir (javna upotreba) [9]

Debian održava tri glavne grane odnosno ditribucije koje su redovito održavane [10]:

- Stabilna – sadrži zadnju službeno objavljenu distribuciju Debiana. Trenutno je to verzija 8.6, kodnog imena *jessie*. Objavljena je 17. rujna 2016.
- Testna – grana koja će postati sljedeće glavno izdanje kad se dovrši sve testiranje na bugove. Glavna prednost korištenja ove distribucije je to da sadrži novije verzije softvera. Trenutna testing distribucija je *stretch*.
- Nestabilna – distribucija koja je trenutno još u fazi razvoja. Trenutna se zove *sid*.

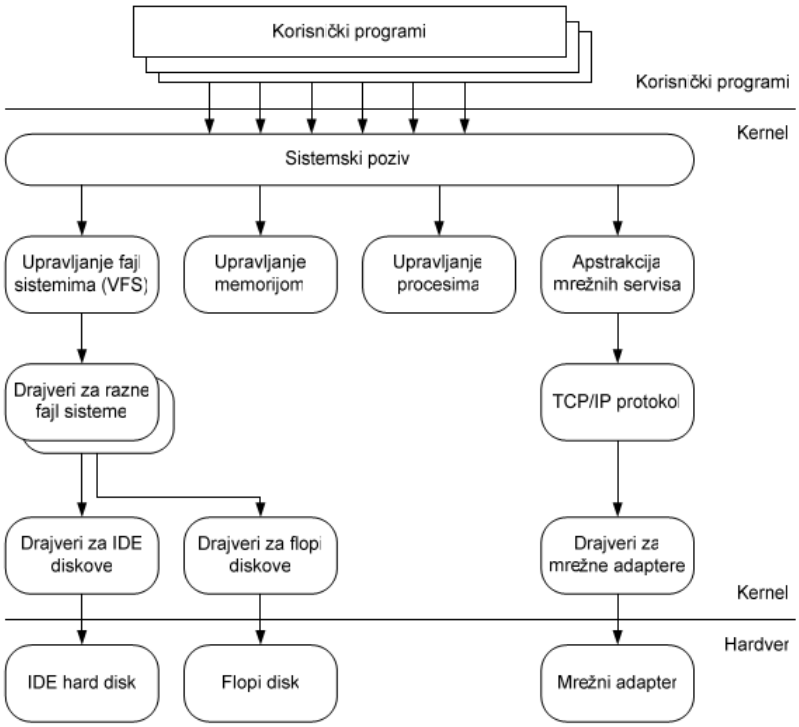
Integracija na ovaj način, te stabilizacija paketa i funkcionalnosti, zajedno s dobro organiziranim mehanizmom kontrole kvalitete osigurala je Debianu reputaciju najbolje testirane distribucije i distribucije s najmanje bugova. Ipak, dugotrajan i kompleksan način razvoja operacijskih sustava ima svoje lošije strane. Stabilne verzije Debiana nisu baš aktualne, i brzo stare jer se nove stabilne verzije izdaju svake 1-3 godine. Visoka demokratična struktura Debiana vodila je Debian u kontroverzne odluke i međusobnu borbu među programerima, što je uzrokovalo stagnaciju i opiranje uvođenju radikalnijih promjena koje bi Debian pokrenule naprijed. Također je vrlo konzervativan u svojoj podršci velikom broju procesorskih arhitektura. Debian je u vremenu od jednog desetljeća postao jedan od, ako ne najveći projekt softverske suradnje ikad. Razvijan od više od 1000 programera, njegov repozitorij sadrži više od 20 000 programskih paketa, te je zaslužan za stvaranje 120 drugih na Debianu temeljenih distribucija. Sa ovim brojkama ne može se usporediti niti jedan drugi Linux operacijski sustav.

2.3 Osnovne funkcije Debian Operacijskog sustava

Operacijski sustav Debian se sastoji se od kernela, sistemskog softvera, korisničkih aplikacija, programskih prevoditelja i njihovih odgovarajućih biblioteka (GCC - GNU C Compiler i C biblioteka za Linux), te dokumentacije. [1]

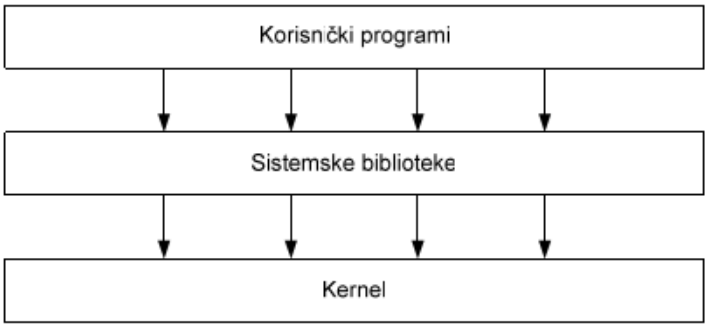
Jezgra operacijskog sustava je kernel koji čija je uloga izvršavanje procesa. Također joj je zadaća dodjela memorije i drugih resursa, te osiguravanje mehanizama za ostvarivanje usluga operacijskog sustava. Zadaća kernela je također zaštita korisničkih procesa od direktnog pristupa hardveru. Pristupaju mu korištenjem sistemskih poziva kernela, a time se dobiva jedna vrsta zaštite između samih korisnika. Sistemske aktivnosti poput pristupa hardveru obavljajus istemski programi, koji su na razini kernela tj. sustavnom načinu rada (engl. supervisory mode). Ostali programi, rade na razini iznad kernela. Tu razinu zovemo korisnički način rada. Sistemski i operacijski programi se razlikuju u svojoj namijeni. Aplikacije se koriste za određene aktivnosti i (npr. obrada fotografije), a namjena sistemskih programa je rad sa sustavom i administracija.

Kod većine UNIX operacijskih sustava aplikacije se direktno obraćaju kernelu, koristeći sistemski poziv, što je prikazano na slici 6:



Slika 6. Unix kernel [1]

Kod operacijskih sustava Linux sistemski pozivi se preko sistemskih biblioteka upućuju kernelu. Sistemske biblioteke definiraju standardni set funkcijea preko koga aplikacije komuniciraju s kernelom. Ova metoda komunikacije prikazana je na slici 7:



Slika 7. Struktura Linux sustava [1]

Osnovne funkcije Debian operacijskog sustava baziranog na Unix-u su [11]:

- upravljanje prekidnim sustavom (engl. interrupt handling)
- raspoređivanje programa u memoriji (engl. dispatching)
- upravljanje računalnim resursima (engl. resource management)
- alokacija memorijskog prostora (engl. program allocation)
- upravljanje datotečnim sustavom (engl. file management)
- upravljanje procesima (engl. job control)
- zaštita i pouzdanost (engl. system reliability)

3. SIGURNOST OPERACIJSKOG SUTAVA

3.1 Pojam sigurnosti operacijskog sustava

Sigurnost operacijskog sustava podrazumijeva mjere kontrole i sprječavanja nedozvoljenog pristupa podacima korisnika. Zaštita u operativnom sustavu usmjerena je na kontrolu korištenja resursa pri izvođenju procesa [12].

Prijetnje usmjerene prema podacima korisnika usmjerene su na:

- Tajnost podataka – sprječavanje pristupa podacima korisnika
- Integritet podataka – sprječavanje izmjene podataka korisnika
- Dostupnost usluga sustava – sprječavanje uskraćivanja usluga sustava krajnjim korisnicima

Moguća mjesta upada u sustav [12]:

- Korištenje podataka datoteka koje se više ne koriste – podaci ostaju u memoriji neko vrijeme te je čitanjem memorijskih adresa moguće doći do podataka
- Korištenje nedozvoljenih sistemskih poziva ili dozvoljenih sistemskih poziva sa nedozvoljenim parametrima
- Lažni proces logiranja – proces simulira postupak logiranja te upisuje podatke korisnika koji se logira u posebnu datoteku
- Prekidanje postupka logiranja – pokušava se „zbuniti“ sustav kako bi se proces logiranja prihvatio kao uspješan
- Suradnja sa administratorom sustava – prijateljski dobivena dozvola pristupa sustavu uz izbjegavanje standardne procedure dobivanja pristupa sustavu
- Neovlašteni pristup podacima o korisnicima sustava u uredu firme.

Ipak, sigurnost ne može spriječiti gubitak podataka u sljedećim slučajevima:

- Atmosferski utjecaji i elementarne nepogode (požar, poplava, potres itd.)
- Hardverska i softverska greška
- Ljudska pogreška

3.2. Implementacija sigurnosti operacijskog sustava

Sigurnost operacijskog sustava moguće je implementirati na različite načine . Prvi način koji ću prikazati je korištenje kriptografije.

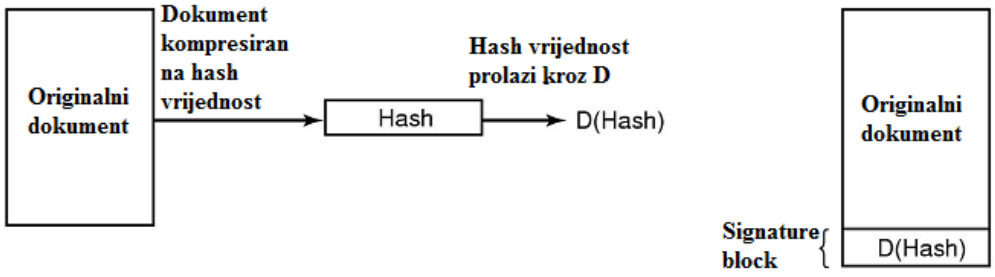
U osnovi kriptografijom prevodimo tekst iz plaintext oblika (originalni dokument) u ciphertext oblik (kodirani dokument) na način koji autoriziranim osobama omogućuje povratak teksta u plaintext oblik.

Kodiranje se koristi za [12]:

- Kriptiranje upotrebom tajnog kjuča
- Kodiranje javnim ključem
- Digitalni potpisi.

Kriptiranje upotrebom tajnog ključa podrazumijeva poznavanje ključa za kriptiranje za osobu koja šalje podatke i osobu koja prima podatke. Kodiranje javnim ključem omogućuje slanje dokumenata primatelju bez poznavanja privatnog ključa primaoca. Javni ključevi korisnika su javno dostupni i koriste se za slanje podataka korisnicima, ali samo korisnik koji ima privatni ključ može otvoriti dokument. Digitalni potpisi koriste se za provjeru autentičnosti podataka poslanih u digitalnom obliku. Pri slanju dokumenata koristi se algoritam za kodiranje (MD5 ili SHA) kako bi se dobila hash verzija dokumenta, zatim se korištenjem privatnog ključa dobiva signature blok D(hash). Primatelj korištenjem MD5 ili SHA algoritma otvara dokument i ako je sa njim suglasan korištenjem javnog ključa pošiljatelja provjerava ispravnost ključa pošiljatelja.

Kriptiranje upotrebom javnog ključa je prikazano na slici 8:



Slika 8 Slanje digitalnih dokumenta [12]

Provjera autentičnosti korisnika izvodi se primjenom [12]:

- passworda
- biometrije
- mjere sigurnosti.

Primjena password-a označava korištenje para login-password za svakog korisnika. Podaci o paru login-password pohranjeni su u posebnu datoteku i pri provjeri korisnika pristupa se pretraživanju datoteke sa podacima o loginu i passwordu kako bi se pronašao zapis koji odgovara upisnim podacima korisnika. Login je u datoteku upisan jednako njegovoj stvarnoj vrijednosti, a password je kodiran i ne odgovara stvarnom passwordu korisnika čime se sprječava doznavanje passworda za korisnike sustava. Pri pokušaju otkrivanja lozinke koristi se ping za detektiranje aktivnih računala, a zatim telnet za provjeru pristupa sustavu. Kombiniranjem različitih kombinacija znakova za login i password nastoji se otkriti login i password koji dozvoljava pristup računalu. Nakon toga pokušavaju se dobiti administratorske ovlasti i podesiti sustav prema osobnim potrebama.

Biometrijom se provjeravaju svojstva korisnika sustava koja se specifična za svaku osobu (npr. otisak prsta ili dlana, zjenica oka, boja glasa). U pravilu se biometrija provodi u kombinaciji s passwordom.

Mjere sigurnosti mogu se odnositi na valjanost passworda u određenom vremenu dana ili određenom danu u tjednu, zatim pri uspostavi veze korisnika može se veza prekinuti i pozvati korisnika kako bi se otkrila lokacija korisnika koji pristupa sustavu itd.

4. IMPLEMENTACIA SIGURNOSTI U OPERACIJSKOM SUSTAVU DEBIAN

Opći cilj informacijskih sustava je osigurati informacije koje su vjerodostojne i dostupne uvijek kada su potrebne. Sveobuhvatna zaštitna polica informacionih sustava može pomoću da se osigura raspoloživost vjerodostojnih informacija isključivo ovlaštenim korisnicima.

4.1.Metode napada

Za uspješno administriranje mreže izuzetno je važno razumjeti prirodu potencijalnih napada na sustav, odnosno mrežu. Sustav se može napasti na mnogo načina: jednostavnim "rubber-hose" metodama, odnosno ucjenjivanjem administratora (razne psihofizičke metode ucjene i iznuđivanja informacija se u praksi pokazuju kao vrlo uspješne), kao i sofisticiranim metodama tipa buffer-overflow (prepunjenje bufera). U najčešće korištene vrste napada na sustav spadaju neautorizirani pristup i eksploatacija poznatih slabosti programa, najčešće mrežnih servisa (telnet, rlogin, rexec). Neautorizirani pristup je vrsta napada koja obuhvaća neautorizirano korištenje resursa računala (najčešće procesorskog vremena i podataka). Najčešće korištene metode eksploatacije slabosti programa su DoS, spoofing i sniffing. Administrator može najbolje zaštititi mrežu od napada ove vrste korištenjem mrežne barijere (firewall). Dodatno, svi mrežni servisi koji nisu pouzdani trebaju biti isključeni ili zamijeenjeni alternativnim paketom (na primjer, telnet se može zamijeniti paketom ssh). [1]

DoS - denial of service (odbijanje usluga) kao napad izaziva prestanak rada servisa ili programa, time se drugima onemogućava rad sa tim servisima ili programima. DoS napad se može izvršiti na mrežnom sloju slanjem zlonamjernih datagrama kojima se izaziva raskid mrežne konekcije. Ovi napadi se mogu izvršiti i na aplikacijskom sloju, slanjem specijalnih naredbi programu, što kao posljedicu ima prestanak rada programa.

Spoofing je podržavanje akcija napada od strane servera ili aplikacije - napad prati IP adrese u IP paketima i predstavlja se kao drugo računalo. Kako DNS ne provjerava odakle dolaze informacije, napadač može izvršiti spoof napad dajući pogrešnu informaciju (ime računala od povjerenja) DNS servisu. Najbolja zaštita od ovog napada je sprječavanje rutiranja datagrama sa neispravnim izvorišnim adresama.

Sniffing je metoda u kojom se specijalnim programima (sniffer) presreću TCP/IP paketi koji prolaze kroz određeno računalo i po potrebi pregleda njihov sadržaj. Kako se kroz mrežu obično kreću podaci koji nisu šifrirani, snifer može dosta jednostavno doći do povjerljivih informacija.

4.2. Zaštitne police

Zaštitne police svakog ozbiljnog informacijskog sustava uključuju sljedeće nivoe zaštite [1]:

- Zaštita fizičkog pristupa sustavu (engl. Physical Access Security). Radi se o fizičkoj zaštiti opreme za konekciju na mrežu (server, ruter itd.) od pristupa osobama koje im ne bi smjele pristupati.

- Zaštita prijavljivanja na sustav (engl. Login & Password Security). Korisnik koji želi imati pristup nekoj radnoj stanici ili serveru, treba posjedovati korisničko ime i lozinku. Sistemski administratori mogu zahtijevati od korisnika lozinku mijenjaju periodično.

- Zaštita sistema datoteka (engl. Filesystem Security). Na ovoj razini se određuje tko može pristupiti kojim podacima te što može raditi sa njima. Sistemski administrator postavlja zaštitu na datotečnom sustavu baziranom na korisnicima, grupama i pravima pristupa. Svakom direktoriju i datoteci se dodjeljuje pravo pristupa. Nivo pristupa objektima se dodjeljuje na temelju danih prava.

- Zaštita od virusa (engl. Virus Protection). Koristi se antivirus softver kao zaštita od virusa. Prednost Linux sustava je da često tvorci virusa nisu dobro upoznati s Linux operacijskim sustavom te rijetko kreiraju UNIX viruse.

- Zaštita udaljenog pristupa sustavu (Remote Access Security). Zadaća sistemskog administratora je osigurati udaljeni pristup korisnicima, ali mora također osigurati zaštitu od neželjenog pristupa

- Internet vatrozid (firewall). Uloga vatrozida je zaštititi Internet stranice od zlonamjernog napada.

- Rezervne kopije podataka (Data Backups). Ovdje se radi o redovnom stvaranju kopija podataka kako bi smo se zaštitili od posljedica gubitka istih u slučaju nesreće.

- Plan restauracije u slučaju teških nesreća (Disaster Recovery Plan). Radi se o zaštitnim mjerama kako bi se u slučaju nesreće mogli povratiti izgubljeni podatci.
- Statistika (Audits). Sistemski administratori proučavajući statistiku mogu utvrditi stvarno stanje zaštite, utvrditi njezine dobre i loše strane tako da mogu napraviti promjene gdje je potrebno.

4.3. Standardni mehanizmi zaštite pod UNIX/Linux sistemom

Glavna uloga sistemske zaštite je zabraniti pristup korisnicima koji na njega nemaju pravo. Potrebno je očuvati informacije u izvornom stanju te spriječiti svaki oblik napada.

Standardni mehanizmi zaštite UNIX sustava su [1]:

- Lozinka i korisnički nalog koji sprječavaju pristup podacima neautoriziranim osobama.
- Postavljanje vlasničkih odnosa i prava pristupa. nakon kreiranja svaka datoteka i direktorij imaju svoj vlasnički odnos i pravo pristupa. Posebni korisnički nalog (root) dozvoljava administratoru neograničen pristup čitavom UNIX sustavu, bez obzira na pristupno pravo. Root korisnik često se zove i superuser jer samo on može izvršavati naredbu za administraciju sustava ili mijenjati sadržaje kritičnih datoteka poput /etc/password.
    - Kontrola udaljenog pristupa (remote login). Linux operacijski sustavi imaju specijalne programe (ipchains i iptables) koji mogu služiti kao kontrola (firewall). Ovi prometa s pomoći adrese tj. određuju pristup nekom sustavu ili njegovoj grupi.

4.4 LILO i datoteka /etc/lilo.conf

LILO je najviše korišten Linux boot loader, tj. program čija je zadaća puniti memoriju sa kernelom os-a. LILO podiže kernel sa prijenosnih i hard diskova, pa može poslužiti i kao boot manager za druge operacijske sustave.[1]

Najznačajnija LILO konfiguracijska datoteka je /etc/lilo.conf. Sljedeće tri direktive koje se mogu navesti u ovoj datoteci mogu značajno povećati sigurnost LILO programa [1]:

- *timeout=00* određuje period čekanja na podizanje podrazumijevanog izbora operacijskog sustava. C2 nivo sigurnosti zahtjeva da ovaj period bude 0 ukoliko se podiže samo jedan operacijski sustav. Ukoliko se timeout postavi na vrijednost 0, LILO prompt će biti nedostupan

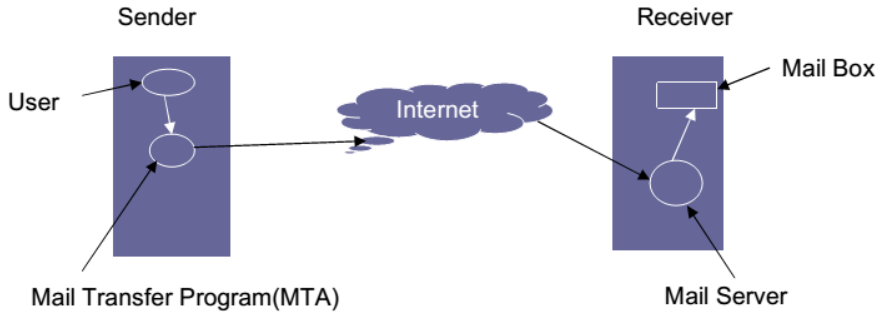
- *password=pass* direktiva štiti sliku kernela lozinkom. Ukoliko se direktiva password navede lozinku pass. LILO lozinke su osjetljive na mala i velika slova

- *restricted* ukoliko je ova direktiva navedena u datoteci /etc/lilo.conf, LILO će zahtijevati lozinku samo u slučajevima učitavanja slike kernela sa dodatnim parametrima iz LILO komandne linije. Direktiva se navodi zajedno sa direktivom password za svaku sliku kernela posebno.
  Napomena: korišenje direktive password bez direktive restricted je loša praksa. U tom slučaju je nemoguće izvesti reboot proceduru sa udaljenog računala, jer LILO zahtjeva lozinku koja se može unijeti samo sa tastature servera. Direktiva restricted dozvoljava reboot sa udaljenog računala, jer se lozinka zahtijeva samo ako se navedu dodatni parametri.

4.2. Zaštita sigurnosti elektroničke pošte

Elektronička pošta je najstariji način za razmjenu poruka na Internetu. Postoji još od ranih sedamdesetih godina dvadesetog stoljeća. Starija je od samog Interneta i jedan o njegovih pokretača. Poruke elektroničke pošte se razmjenjuju takozvanim „spremi i proslijedi“ načinom, što znači da svaki poslužitelj sprema poruke i prosljeđuje ih kad je sljedeći poslužitelj dostupan. Na taj se način izbjegava potreba za stalnom dostupnosti svih poslužitelja i korisnika, te oni moraju biti istovremeno dostupni samo djelić vremena koji je potreban za razmjenu poruka. Poruka koja se prosljeđuje sastoji se od dva dijela – zaglavlja i tijela. U zaglavlju se nalaze polja za informacije: primatelji, pošiljatelj, naslov, vrijeme i ostale informacije o poruci. U tijelu se nalazi sama poruka, obično tekst. Razmjenjivanje između poslužitelja vrši se SMTP protokolom, dok klijenti obično pristupaju protokolima POP i IMAP, ili nekim od vlasničkih protokola. U današnje vrijeme uobičajeno je da se elektroničkoj pošti može pristupiti i preko Web sučelja. Kako je elektronička pošta stari sustav, tako ima niz problema; sama po sebi nema nikakav način provjere pošiljatelja, cijeli sustav za razmjenu vrši se nekriptiranim porukama, i ono što je danas možda najpoznatiji problem, često je zatrpana neželjenim porukama, takozvanim spamom. Neki od tih problema riješeni su, razmjena se danas uglavnom kriptira, razvijene su metode za osiguranje povjerljivosti i neporecivosti poput PGP-a. Ipak, spam i dalje čini ogroman dio razmijenjenih poruka.

Na slici ispod prikazan je proces slanja elektroničke pošte:



Slika 8 Proces slanja elektroničke pošte [1]

Elektroničku poštu je moguće zaštititi korištenjem GnuPG programa, što je detaljno obrađeno u sljedećem poglavlju.

5. ALATI ZA IMPLEMENTACIJU SIGURNOSTI U DEBIAN OPERACIJSKOM SUSTAVU

5.1. Implementacija sigurnosti emaila sustava korištenjem GNU Privacy Guarda

GNU Privacy Guard (GnuPG ili GPG), je kriptografska implementacija javnog ključa. Razvio ga je Werner Koch, a prva verzija 1.0.0 je objavljena 1990. godine. GnuPG je kao što mu ime govori dio GNU projekta te je financiran i od strane Njemačke vlade. Služi kao besplatna zamjena za Symantec PGP kriptografski softver alat. On omogućuje prijenos informacija između stranaka i koristi se da potvrdi da je podrijetlo poruke zaista pravo.

Slika 9 Logotip GnuPG programa [13]

Problem s kojim se mnogo korisnika suočava je kako komunicirati sigurno i potvrditi identitet strane s kojom se komunicira. Mnoge ideje koje su pokušavale odgovoriti na njega zahtjevaju, bar u nekom trenutku, prijenos lozinke ili drugih načina identifikacije putem nesigurnog medija.

Da se doskoči tome problemu, GnuPG se oslanja na koncept sigurnosti znan kao enkripcija javnog ključa. Ideja je podijeliti etape enkripcije i dekripcije prijenosa u dva odvojena dijela. Na taj način moguće je slobodno distribuirati enkripcijski dio, sve dok se osigura dekripcijski dio. Na taj način jednosmjerni prijenos poruke može biti stvoren i kriptiran od bilo koga-ali može biti dekriptiran samo od strane namijenjenog korisnika (onog s privatnim dekripcijskim ključem). Ukoliko obje strane stvore javni/privatni par ključeva i razmjene javne

enkripcijske ključeve, mogu jedan drugome enkriptirati poruke. U tom slučaju svaka strana ima svoj vlastiti privatni ključ i javni ključ drugog korisnika.

Iduća pogodnost ovog sustava je da primatelj može „potpisati“ poruku svojim privatnim ključem. Javni ključ koji ima primatelj množe biti korišten da potvrdi da je potpis zaista poslan od navedenog korisnika. To može spriječiti treću stranu od „spoofinga“ identiteta nekome. Također osigurava da je poruka primljena u potpunosti, bez štete ili korupcije na njoj.

5.2. Postavljanje GnuPG ključa

Ukoliko GnuPG nije instaliran na Debian operacisjki sustav to se jednostavno može učiniti sljedećom naredbom:

sudo apt-get install gnupg

Da bi započeli korištenje GnuPG- a i enkriptirali svoju poruku trebamo stvoriti par ključeva.To možemo učiniti sljedećom naredbom:

gpg --gen-key

To će nas provesti kroz nekoliko pitanja koja će konfigurirati naše ključeve. Na sljedećem primjeru ih je moćuće vidjeti sa nekim odgovorima:

- Please select what kind of key you want: **(1) RSA and RSA (default)**
- What keysize do you want? **Veličina ključa** ***4096***
- Key is valid for? ***0***
- Is this correct? **Portvrda (da ili ne)** ***y***
- Real name: **unesite pravo ime**
- Email address: **your_email@address.com**
- Comment: **Opcionalni komentar koji će biti vidljiv u potpisu**
- Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? **Izmjena unosa ili potvrda *O***
- Enter passphrase: **Unesite sigurnu lozinku ovdje (velika i mala slova, brojevi i simboli obavezni)**

Ovdje ćemo trebati generirati ključeve koristeći entropiju. To je termin koji opisuje količinu nepredvidljivosti koja postoji u sustavu. GnuPG koristi tu entropiju kako bi stvorio nasumičan skup ključeva. Taj proces može potrajati duže vrijeme ovisno o tome koliko aktivnim možete učiniti svoj sustav.

5.3. Stvaranje certifikata opoziva

Potrebno je imati način poništavanja svoga para ključeva u slučaju sigurnosnog proboja ili , gubitka tajnog ključa. To je moguće učiniti uz pomoć GnuPG-a. To je potrebno napraviti unaprijed, čim je izrađen par ključeva, a ne kad nam treba . Gneriramo ga unaprijed i držimo na sigurnoj, odvojenoj lokaciji u slučaju da je naše računalo neoperativno ili pokvareno. Unesite naredbu:

gpg --gen-revoke your_email@address.com

Tada ćete biti upitani za razlog opoziva ključa. Možete odabrati bilo koju od danih opcija, ali zbog toga što to radimo unaprijed, nije potrebno specificirati. Nakon toga ćete biti ponuđeni da date svoj komentar i na kraju potvrdite svoje akcije. Tada će certifikat opoziva biti generiran na vašem ekranu. Kopirajte ga i spremite na posebnu lokaciju ili ispišite za kasniju upotrebu. Primjer certifikata opoziva se nalazi ispod: [14]

```
Revocation certificate created.

Please move it to a medium which you can hide away; if Mallory gets
access to this certificate he can use it to make your key unusable.
It is smart to print this certificate and store it away, just in case
your media become unreadable.  But have some caution:  The print system of
your machine might store the data and make it available to others!
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.11 (GNU/Linux)
Comment: A revocation certificate should follow

iQIfBCABAgAJBQJX6Y2fAh0AAAoJEFzfz00qe0JViTsP/jdhWeY+Wgb0S5dzAQoU
zoVMUEzRTAFj3RoHvGe2cHZOXKrYDRHt/QeQDe98FrVXuNYSAQF7SI4JNNsfdLlb
k9meUHqmB6f4vPkjzzQpKHbWhAClc1REWDJ1/cU+3jxoYuv2qXEwOpa7Ldh8Spsr
Vx0ufaqfX8Yctp/Q3TUatg/qSgjEs5cvhnvT8rfDKp3Uwa1TAL9sCMCa8y/M2Jjp
HygDMjI9+l1+9HoFcflJ1SjGKwfkPvau5lJ2M6D99JgOcyyKtkJBtq+VrZqDDQ/a
+I/yQVJkVUnJ1qRuBAwMiKXe5dWcBKni4S+oRgyESkH+fztP1UCY6qTWsrKzJykB
OyxMnSo1bdiYgdvTpNL+NTG1OQUQG171VzrGpU6IlG/49SVxv7b1OBQkNg/579P1
d43rZoppKbBzHOx7ZQUQYu3WiR2RSHhu8KsXLik+aZCQZHP1f1xHCdv0x+XUQxkd
wBD2R4kZxUBxMHI/CMYm1qTjoTa3Q5FmuSbwKnbawzKC98WgCxyuFoatk9Yvu7Ei
U5AzsdZjlgzzgq7sp11lwyscuI94KUcavw7JQZWp/HXk0gQl1bmdHo4B46vgK4Rm
T0ra4O06M9esW4PJ/cvGji9aKQ0cYVA/PiHj7rp+zUBuuBkGhJ7jzjWt6OMOSEtT
EiCPcjevUQDI8/BZvKevPYkV
=khyo
-----END PGP PUBLIC KEY BLOCK-----
```

5.4. Učitavanje ključeva drugih korisnika

Gnu PG bi bio poprilično beskoristan da ne prihvaća javne ključeve od drugih ljudi s kojima želimo komunicirati. Moguće je učitati nečiji javni ključ na razne načine. Ukoliko ste nabavili nečiji javni ključ u tektualnom obliku, GnuPG ga može uvesti korištenjem sljedeće naredbe:

gpg --import name_of_pub_key_file

Također je moguće da je osoba s kojom želite komunicirati učitala svoj ključ na javni server. Ovi serveri javnih ključeva se koriste kao skladište javnih ključeva za ljude širom svijeta.Popularni server ključeva koji sinkronizira svoju informaciju s mnoštvom drugih servera je „MITpublic key server“ Možete ga potražiti putem sljedeće web stranice:

http://pgp.mit.edu/

Također moguće pretražiti server ključeva iz GnuPG-a sljedećom naredbom:

gpg --keyserver pgp.mit.edu --search-keys search_parameters

5.5 Potvrda identiteta

Postoje situacije u kojima je potrebno potvrditi identitet druge osobe i njihovog ključa. Na sreću, moguće je potvrditi "fingerprint". Fingerprint je moguće nabaviti unosom sljedeće naredbe:

gpg --fingerprint your_email@address.com

Rezultat bi trebao biti sličan primjeru [14]:

```
pub   4096R/311B1F84 2013-10-04
      Key fingerprint = CB9E C70F 2421 AF06 7D72  F980 8287 6A15 311B 1F84
uid                  Test User <test.user@address.com>
sub   4096R/8822A56A 2013-10-04
```

Potpisivanjem ključa poručujete da da vjerujete ključu kojega ste primili i da je potvđreno da je od one osobe od koje je i trebao biti. Da bi potpisali ključ unesemo:

gpg --sign-key email@example.com

Također biste trebali poslati natrag potpisan ključ. To je moguće unosom sljedećeg:

gpg --export --armor email@example.com

Po primitku novog potpisanog ključa, oni ga mogu uvesti, dodajući potpisane informacije koje smo stvorili u svoju GnuPG bazu podataka. To će učiniti unosom sljedećeg:

gpg --import file_name

Nema ničeg opasnog za vas ili vaš sustav u tome da drugi ljudi znaju naš ključ. Zbog toga, može nam koristiti da ga učinimo jednostavno dostupnim. Moguće ga je poslati svima zahtijevajući to od GnuPG sustava:

gpg --armor --export your_email@address.com

Rezultat je sljedeći [14]:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.11 (GNU/Linux)

mQINBFJPCuABEACiog/sInjg0O2SqgmG1T8n9FroSTdN74uGsRMHHAOuAmGLsTse
9oxeLQpN+r75Ko39RVE88dRcW710fPY0+fjSXBKhpN+raRMUKJp4AX9BJd00YA/4
EpD+8cDK4DuLlLdn1x0q41VUsznXrnMpQedRmAL9f9bL6pbLTJhaKeorTokTvdn6
5VT3pb2o+jr6NETaUxd99ZG/osPar9tNThVLIIzG1nDabcTFbMB+w7wOJuhXyTLQ
JBU9xmavTM71PfV6Pkh4j1pfWImXc1D8dS+jcvKeXInBfm2XZsfOCesk12YnK3Nc
u1Xe1lxzSt7Cegum4S/YuxmYoh462oGZ7FA4Cr2lvAPVpO9zmgQ8JITXiqYg2wB3
. . .
```

Možete ga kopirati i zaljepiti na prikladan medij. Ukoliko to želite možete ga ručno objaviti na nekom serveru. Također je to moguće učiniti putem GnuPG sučelja.

Provjerite svoj ID unosom sljedeće naredbe:

gpg --list-keys your_email@address.com

Podebljani dio je ID vašeg ključa:

```
pub   4096R/311B1F84 2013-10-04
uid                  Test User <test.user@address.com>
sub   4096R/8822A56A 2013-10-04
```

Da bi učitali svoj ključ na određeni server ključeva, koristite sljedeću sintaksu:

gpg --send-keys --keyserver pgp.mit.edu key_id

5.6. Enkripcija i dekripcija poruka sa GnuPG-om

Kriptirati poruke je moguće korištenjem „*--encrypt*“ zastavice za GnuPG. Osnovna sintaksa bi izgledala na način:

gpg --encrypt --sign --armor -r person@email.com name_of_file

Dekripciju poruka izvršavamo po primitku poruke jednostavno pozivanjem GnuPG-a na poruku datoteke kao na primjer:

gpg file_name

Sotver će nas sam ažurirati. Također je moguće pritisnuti „CTRL-D“ da naznačimo kraj poruke koju će GnuPG za nas dekriptirati.

Da bi ispisali koje GnuPG ključeve imamo od drugih ljudi, možete zadati sljedeću naredbu:

gpg --list-keys

Također popis možete ažurirati pomoću:

gpg --refresh-keys

Ako želimo povući informaciju sa isključivo jednog servera po našoj želji, to možemo učiniti pomoću:

gpg --keyserver key_server --refresh-keys

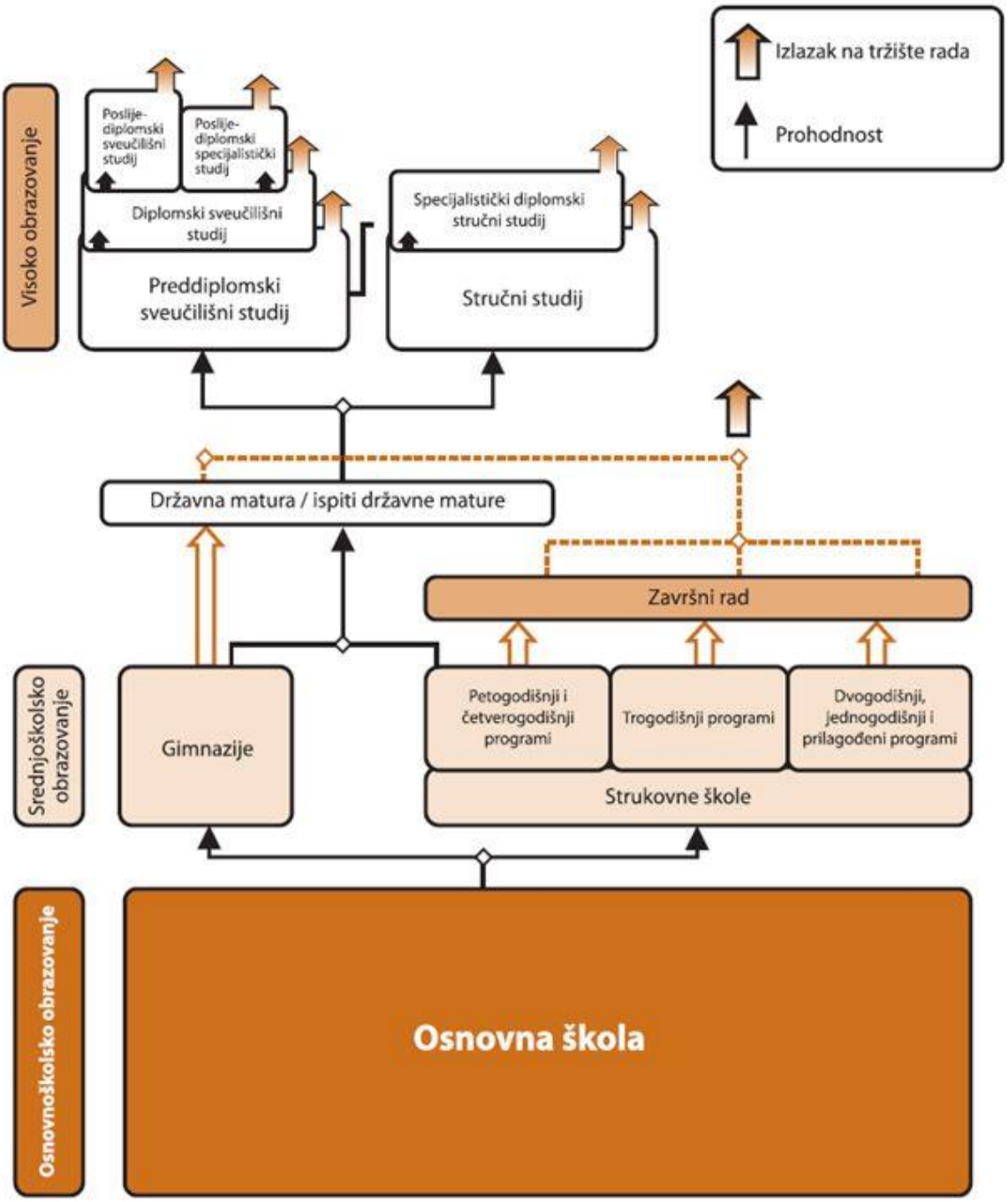
Pravilno korištenje GnuPG-a će nam osigurati sigurnu komunikaciju sa mnoštvom ljudi putem email-a. To je naročito korisno kad baratamo sa osjetljivim informacijama, ali i svakodnevnim porukama. GnuPG enkripcija je korisna samo kada obadvije strane koriste dobre sigurnosne navike, i budne su oko druge strane.

6. METODIČKI DIO

6.1. Analiza nastavnog programa srednje strukovne škole u sadržaju teme diplomskog rada

U Republici Hrvatskoj sustav školovanja se dijeli na predškolski odgoj, osnovno obrazovanje, srednje obrazovanje te visokoškolsku naobrazbu. Srednje škole dijelimo na gimnazije, umjetničke, te strukovne škole. Gimnazije mogu biti opće ili specijalizirane, te najmanje traju četiri godine. Umjetničke škole se dijele prema vrsti programa koji nude, te također najmanje traju četiri godine. Strukovne škole nude učenicima stjecanje strukovnih kompetencija za tržište, te traju od jedne, do četiri godina; u iznimnim slučajevima pet.

Strukovno obrazovanje pohađa oko 71% ukupne srednjoškolske populacije. Jednogodišnji i dvogodišnji programi čine oko 0.5% ukupne srednjoškolske populacije, te se radi o nižoj stručnoj spremi, te pomoćnim zanimanjima. Trogodišni programi čine oko 26% ukupne srednjoškolske populacije, te su namijenjeni zanimanjima u industriji i obrtništvu. Četverogodišnje programe pohađa najviše učenika strukovnog obrazovanja, te oko 45% ukupne srednjoškolske populacije. Radi se o tehničkim i sličnim zvanjima.



Slika 10. Shematski prikaz obrazovanja u RH [15]

Pet je ključnih ciljeva reforme strukovnog obrazovanja i osposobljavanja predviđeno Strategijom razvoja strukovnog obrazovanja (2008.–2013.):

1. razviti kvalifikacije temeljene na kompetencijama i rezultatima učenja
2. trajno usklađivati obrazovanje s potrebama tržišta rada
3. izgraditi sustav strukovnog obrazovanja i osposobljavanja koji omogućava cjeloživotno učenje i mobilnost
4. definirati uloge nastavnika u sustavu orijentiranom na rezultate učenja
5. uspostaviti sustav osiguranja kvalitete

Agencija za strukovno obrazovanje i obrazovanje odraslih za školsku godinu 2013./2014. daje mogućnost iskazivanja interesa strukovnih škola za provedbu 25 paketa strukovnih kurikuluma programiranih u skladu s novom metodologijom. Paketi obuhvaćaju standard zanimanja, standard kvalifikacije i strukovni kurikulum.

Nastava u strukovnim školama se izvodi temeljem sljedećih dokumenata:

1. Zakon o odgoju i obrazovanju u osnovnoj i srednjoj školi
2. Zakon o strukovnom obrazovanju
3. Zakon o udžbenicima za osnovnu i srednju školu
4. Nastavni planovi i programi srednjih strukovnih škola
5. Pravilnik o početku i završetku nastave i trajanju odmora učenika
6. Pravilnik o načinu, postupcima i elementima vrednovanja učenika u osnovnoj i srednjoj školi.
7. Nacionalni okvirni kurikulum
8. Hrvatski kvalifikacijski okvir

6.1.2 Obrazovanje za zanimanje Tehničar za računalstvo

Zanimanje tehničar za računalstvo obuhvaća praktična znanja i vještine potrebne za obavljanje poslova iz područja ljudskih djelatnosti povezanih s projektiranjem, izradbom i održavanjem manje složenih relacijskih baza podataka i računalnih programa, nadziranjem i dijagnosticiranjem te evidentiranjem i otklanjanjem hardverskih i softverskih problema, educiranjem i pomaganjem korisnicima u rješavanju njihovih problema, konfiguriranjem i održavanjem računala, lokalne računalne mreže, računalnih i informacijskih sustava.[16]

Središnja i integrirajuća kompetencija ovog zanimanja objedinjuje poslove [16]:

- rada na računalu (npr. programiranje)
- pripreme i obrade podataka (npr. računalni operater)
- kontrole, pripreme i obrade podataka
- oblikovanje baza podataka
- administracije baza podataka
- projektiranja informacijskih sustava
- operatera na vanjskoj računalnoj opremi (npr. računalne mreže)
- sistemskog inženjerstva nižeg stupnja složenosti, uključujući administraciju operacijskih sustava i računalnih mreža
- osiguranja kvalitete
- edukacije krajnjih korisnika
- marketinga i prodaje u području ICT-ja
- druge srodne poslove.

6.2. Priprema za izvođenje nastave za pripadnu razinu kvalifikacije u skladu s HKO

S V E U Č I L I Š T E U R I J E C I

FILOZOFSKI FAKULTET RIJEKA

ODSJEK ZA POLITEHNIKU

Ime i prezime: Domagoj Bobovec

P R I P R E M A Z A I Z V O Đ E NJ E N A S T A V E

Škola: Strukovna škola Đurđevac

Mjesto: Đurđevac

Razred: 4.

Zanimanje: Tehničar za računarstvo

Nastavni predmet: Sustavna programska potpora

Kompleks: 1. Operacijski sustavi

Metodička (nastavna) jedinica: **1. Operacijski sustavi**

- Uloga operacijskog sustava
- Funkcije i karakteristike operacijskog sustava
- Raščlanjivanje operacijskog sustava na operacijske razine

**Datum izvođenja: 9. rujan, 2016.

S A D R Ž A J N I P L A N

Podjela kompleksa na teme (vježbe, operacije)

(Uz svaku temu /vježbu, operaciju/ navedite broj nastavnih sati i podvucite onu koja se u pripremi obrađuje)

Redni broj	**Kompleks: 1. Operacijski sustavi** Naziv tema u kompleksu	Broj sati	
		teorija	vježbe
1	Uloga operacijskog sustava	1	2
2	Funkcije i karakteristike operacijskog sustava	1	2
3	Raščlanjivanje operacijskog sustava na operacijske razine	1	2

Karakter teme (vježbe, operacije) – metodičke jedinice

Informativni karakter – stjecanje znanja o osnovnim pojmovima iz operacijskih sustava.

PLAN VOĐENJA ORGANIZACIJE NASTAVNOG PROCESA

Cilj (svrha) obrade metodičke jedinice:

(Navedite ŠTO OD UČENIKA OČEKUJETE na kraju, nakon obrade nastavne građe, zbog čega se građa obrađuje)

Cilj obrade metodičke jedinice je upoznati učenika sa poviješču i vrstama operacijskih sustava, njihovom strukturom i konceptima vezanim uz njih.

Ishodi učenja (postignuća koja učenik treba ostvariti za postizanje cilja):

(Posebno upišite koja znanja; koje vještine i umijeća, te koju razinu samostalnosti i odgovornosti učenik treba steći nakon obrade nastavne teme. Ishode formulirati jasno i jednoznačno kako bi se mogli nedvojbeno provjeriti evaluacijom.)

ZNANJE I RAZUMIJEVANJE *(obrazovna postignuća)*:

Učenik će:

- izreći definiciju pojma operacijskog sustava
- definirati zadatke operacijskih sustava
- opisati povijesni razvoj operacijskih sustava
- opisati razliku Linux i Windows operacijskih sustava
- objasniti što je to proces
- objasniti što je to zastoj

VJEŠTINE I UMIJEĆA *(funkcionalna postignuća)*:

- prepoznati korisnička sučelja operacijskih sustava

SAMOSTALNOST I ODGOVORNOST *(odgojna postignuća)*:

- razviti odgovoran odnos prema informatičkoj opremi
- aktivno surađivati s nastavnikom i učenicima prilikom obrade gradiva

Dio sata	Faze rada i sadržaj	Metodičko oblikovanje	Vrijeme
Uvodni dio	-Uvođenje u novi sat i motivacija učenika	-dijalog s učenicima o operacijskim sustavima	5 min
Glavni dio	-obrada nastavne jedinice vezane za operacijske sustave	- predavanje o operacijskim sustavima - prikaz Windows i Linux operacijskih sustava -predavanje o procesima i zastojima	35 min
Završni dio	-ponavljanje obrađenog gradiva pomoću pripremljenih pitanja	-evaluacija obrađenog nastavnog gradiva	5 min

Posebna nastavna sredstva, pomagala i ostali materijalni uvjeti rada:

Nastavna sredstava:

- Powerpoint prezentacija

Nastavna pomagala:

- stolno ili prijenosno računalo za nastavnika

- LCD projektor

Metodički oblici koji će se primjenjivati tijekom rada:

Uvodni dio sata:

- razgovorom s učenicima uvesti učenike u novu temu:

vrste operacijskih sustava, čemu operacijski sustavi služe

Glavni dio sata:

- predavanje o operacijskim sustavima :

    povijesni razvoj, uloga i zadaća

- prikaz Windows i Linux operacijskog sustava

- predavanje o procesima i zastojima

Završni dio sata:

- evaluacija obrađenog nastavnog gradiva pomoću pitanja

- Sistematizacija obrađenoga sadržaja najaviti novu teme za sljedeći sat.

Izvori za pripremanje nastavnika:

1. Andrew S. Tanenbaum: Modern Operating Systems, Prentice Hall, 2001.

2. Andrew S. Tanenbaum: Operating Systems, Design and Implementation, Prentice Hall, 1997.

3. Silberschatz, Galwin: Operating system concepts, Addison Wesley, 1994

Izvori za pripremanje učenika:

- S. Ribarić, Arhitektura računala RISC i CISC, Školska knjiga, Zagreb, 1996.

Tijek izvođenja nastave-nastavni rad

Uvodni dio

Nakon pripreme za rad, dijalogom s uvodim učenike u novo gradivo: obrada s odvajanjem čestica. Gdje su se već susretali s operacijskim sustavima, koja je njihova uloga, koje vrste operacijskih sustava poznaju. Zapisati naslov „Operacijski sustavi na ploču“ na ploču.

Glavni dio

Obrada novog sadržaja

Na početku definiram računalni sustav. Računalni sustav čini jedan ili više glavnih procesora, radna memorija, diskovi, pisači, tipkovnica, monitor, mrežne kartice i druge vrste ulazno-izlaznih uređaja. Pisanje učinkovitih programa za takav sustav je vrlo složen i težak posao. Zbog toga se računala nadograđuju softverskim slojem koji zovemo operacijski sustav Zadatak operacijskog sustava a je povezivanje svih dijelova računalnog sustava i pružanje korisničkim programima jednostavno sučelje za rad sa hardverom.

Zatim pomoću Power Point prezentacije objašnjavam povijesni razvoj računala. Svaku generaciju računala zapišem na ploči, te uz pomoć prezentacije navodim njihova glavna svojstva i slikovno ih prikazujem.

1. generacija. (1945-55) Elektronske cijevi i prekidači

Osobitost ove generacije je izostanak potrebe za sistemskim softverom zbog neučinkovitosti računala.

2. generacija. (1955-65) Tranzistori i serijska obrada

Dolazi do pojave snažnijih računala sa mogućnošću specijalizirane obrade u znanstvene svrhe sa dobro podržanim matematičkim operacijama (IBM 7094) i komercijalne obrade sa podržanim radom sa ulazno-izlaznim uređajima (IBM 1401). Obrada se izvodila serijski, program za programom (batch obrada). Računalo IBM 1401 korišteno je za prijenos programa sa čitača bušenih kartica na magnetnu traku. Magnetna traka je zatim prenesena na računalo IBM 7094 gdje se izvodila konkretna obrada i zapis rezultata na izlaznu traku. Zadatak OS-a, odnosno sistemskog softvera je učitavanje programa sa ulazne trake, zatim učitavanje programa za izvođenje učitanog programa korisnika sa sistemske trake, izvođenje programa

korisnika i na kraju zapis rezultata na izlaznu traku. Postupak se ponavljao sve dok nisu izvedeni svi programi sa ulazne trake. Na kraju se izlazna traka prenijela na računalo IBM 1401 kako bi se ispisali izlazni rezultati na pisač.

3. generacija. (1965-1980) Integrirani krugovi i multiprogramiranje

Dolazi do smanjenje razlika između računala i razvoja OS za širu upotrebu računala OS/360. Također se uvode novi koncepti: multiprogramiranje, spooling i timesharing. Multiprogramiranjem se ostvaruje izvođenje više programa na jednom računalu što se ostvaruje dijeljenjem memorije na dijelove (particije) i učitavanjem programa u jednu particiju. Objašnjavam Spooling. To je tehnika koja se zasniva na učitavanju programa u oslobođenu particiju odmah nakon završetka izvođenja ranije učitanog programa. Govorim o projektu Projekt MULTICS, razvijan je u suradnji sa vodećim informatičkim tvrtkama toga vremena, ali nije u potpunosti ispunio očekivanja jer je zadovoljenje zahtjeva jedne grupe korisnika uzrokovalo degradaciju kvaliteta usluga za druge korisnike. Istraživača tvrtke Bell Labs, Ken Thompson je razvio verziju MULTICS-a za osobno (preteču današnjih PC-a) računalo tipa PDP-1, što je označilo početak razvoja operativnog sustava UNIX. UNIX je napisan u programskom jeziku C i prenosiv je na različite hardverske konfiguracije. Programski kod UNIX-a u počecima je bio dostupan omogućujući nadogradnju sustava prema vlastitim potrebama. To je rezultiralo velikim brojem nekompatibilnih verzija UNIX-a pa je definiran standard POSIX sa skupom osnovnih funkcija koje moraju biti podržane. Kasnije verzije UNIX-a su komercijalizirane što je programski kod učinilo nedostupnim. Za potrebe edukacije studenata stvoren je po uzoru na UNIX, operativni sustav MINIX sa jednostavnijom strukturom i mogućnošću nadogradnje i testiranja sustava. Namjena MINIX-a je edukacija studenata pa njegovi tvorci nisu pokazali interes za nadogradnjom MINIX-a. Student Linus Torvards izradio je napredniju verziju MINIX-a i nastavio njen razvoj što je rezultiralo operativnim sustavom Linux. Linux je OS razvijen od velikog broja programera širom svijeta, uvjetujući malu komercijalnu cijenu sustava i relativno skromne hardverske zahtjeve u odnosu na OS-e sličnih osobina.

4. generacija (1980-sadašnjost) Osobna računala

Razvoj osobnih računala uvjetovao je i razvoj OS-a za osobna računala te prilagodbu postojećih OS-a. Pojavljuju se prvi OS-i za osobna računala CP/M (Control Program for Microcomputers), DOS (Disk Operating System), zatim MS-DOS, WINDOWS 3.1, WINDOWS 3.11, WINDOWS 95, WINDOWS 98, WINDOWS Millenium. Osobitost

WINDOWS sustava je povezanost sa operativnim sustavom MS-DOS. Paralelno sa razvojem navedenih WINDOWS OS-a razvijaju se i WINDOWS NT (New Technology) operativni sustavi namijenjeni profesionalnoj upotrebi. WINDOWS NT su 32-bitni OS neovisan o OS MS-DOS-u. Značajnije verzije WINDOWS NT OS-a su WINDOWS NT 4.0, WINDOWS 2000, te WINDOWS XP. Za Apple računala razvijen je poseban operacijski sustav – Macintosh operativni sustav. Povezivanjem računala javila se potreba za nadogradnjom OS osobnih računala za mrežnu komponentu. Pouzdani mrežnim OS-i su UNIX, LINUX i WINDOWS NT. Najnoviji trend je razvoj OS-a za distribuiranu obradu. Mrežni operativni sustavi su proširenje OS-a osobnih računala za mogućnost kontrole pristupa podacima drugog računala i prijenos podataka između računala, dok distribuirani operativni sustavi omogućuju izvođenje obrade na više računala što znatno povećava kompleksnost OS-a. Razvoj OS-a i dalje će biti uvjetovan razvojem računalne tehnologije (hardvera i tehnoloških inovacija u prijenosu podataka) i prilagođavati će se zahtjevima krajnjih korisnika.

Na ploču ispisujem vrste operacijskih sustava:

- Mainframe OS
- Multiprocesorski OS
- Real-time OS
- Embeded OS
- Smart card OS

Svaki od njih posebno opisujem.

Mainframe operacijski sustavi su OS za centralizirana računala koje opslužuje veliki broj terminalima spojenih korisnika. Mainframe OS-i bili su dominantni prije pojave osobnih računala PC-a. Primjeri su OS/360 i OS/390.
Server operacijski sustavi su OS koji velikom broju klijent računala pružaju usluge korištenje hardverskih i softverskih resursa server računala. Primjeri su WINDOWS NT, UNIX i LINUX.

Multiprocesorski operacijski sustavi podržavaju rad dva ili više centralno procesorskih jedinica CPU-a. U pravilu su to modificirani server operacijski sustavi
sa posebnim osobinama za komunikaciju i spajanje.

Operativni sustavi za osobna računala – omogućuju prikladno radno okruženje za

jednog korisnika. Primjeri su WINDOWS 98, WINDOWS Millenium, WINDOWS 2000, LINUX, Macintosh OS itd.

Real-time operacijski sustavi su sustavi koji moraju generirati rezultat obrade (odgovor, response) na ulazne podatke u realnom vremenu (u pravilu za manje od 1s). Ukoliko je kašnjenje reakcije pogubno za sigurnost sustava govorimo o hard time sustavu, a ako se kašnjenje može tolerirati govorimo o soft-time sustavu.

Embeded operacijski sustavi su OS za male konzole (elektronički adresari, memorijske pločice itd.) sa smanjenim opsegom funkcija.

Smart card operacijski sustavi su OS namijenjeni korištenju različitih elektroničkih kartica (bankovne kartice, telefonske kartice, parkirne kartice itd.). Zatim učenicima prikazujem pojedinačno Windows operacijski sustav, zatim Linux, te objašnjavam razliku među njima.

Objašnjavam pojam procesa. To su aktivnosti koje nastaju pri izvođenju programa korisnika. Dajem primjer procesa.
Objašnjavam pojam zastoja. To su nepoželjne situacije koje dovode do blokiranja izvođenja dva ili više procesa. Dajem primjer zastoja.

Završni dio

Evaluacija obrađenog nastavnog gradiva

Na kraju sata učenicima dajem listiće s pitanjima kako bi provjerio usvojenost gradiva:

Kako definiramo operacijski sustav?

Navedite generacije računala?

Navedite vrste operacijskih sustava?

Definirajte proces.

Definirajte zastoj.

Od učenika očekujem cjelovite odgovore vlastitim riječima i ocjenu će dobiti naknadno, nakon što pregledam sve, a ocijeniti će se prema slijedećem kriteriju:

učenik je točno odgovorio na sva postavljena pitanja.…..... izvrstan (5)

učeniku je jedan odgovor netočan.....vrlo dobar (4)

učenik je odgovorio na većinu pitanja točnim odgovorima.....……dobar (3)

učenik je odgovorio na većinu pitanja netočno .....dovoljan (2)

učenik nije znao niti jedno postavljeno pitanje .....nedovoljan (1)

Nakon što su ispunili listiće i predali ih, najavljujem slijedeći sat koji će biti vježbe na računalima te im dajem kratke upute o ponašanju u računalnoj učionici

Izgled ploče

OPERACIJSKI SUSTAVI

1. GEN. (1945-55) ELEKTRONSKE CIJEVI I PREKIDAČI

2. GEN. (1955-65) TRANZISTORI I SERIJSKA OBRADA

3. GEN. (1965-1980) INTEGRIRANI KRUGOVI I MULTIPROGRAMIRANJE

4. GEN. (1980-sadašnjost) OSOBNA RAČUNALA

VRSTE OS-A

- Mainframe OS
- Multiprocesorski OS
- Real-time OS
- Embeded OS
- Smart card OS

Procesi - aktivnosti koje nastaju pri izvođenju programa korisnika
Zastoj - nepoželjne situacije koje dovode do blokiranja izvođenja dva ili više procesa

Domagoj Bobovec

*Pregledao:_____ *Datum:_____

Osvrt na izvođenje:

(Sažet kritički osvrt na sadržajnu, stručno – teorijsku, organizacijsko – tehničku i subjektivnu komponentu vođenja nastavnog procesa.)

*Ocjena:_____ _____ _____

(Potpis ocjenjivača) (Datum)

_____

7. ZAKLJUČAK

U današnjem svijetu problem sigurnosti operacijskih sustava nije zanemariv. Postoje nebrojeni načini na koje netko sa zlom namjerom može nanjeti štetu našem računalu ili našoj imovini putem njega. Kao reakcija na to razvijeni su brojni alati sa svrhom spriječavanja zlonamjernog napada.

U ovome radu sam se detaljno usmjerio na zaštitu emaila. Ukoliko je taj medij ugrožen netko zlonamjeran može njegov sadržaj upotrebljavati u svoju korist ili nama na štetu. Jedan od načina na koji ga je moguće zaštititi je GNU Pivacy Guard. Radi se o aplikaciji koja štiti mail kriptacijom. Na taj način će email moći čitati samo osoba za koju to i želimo, odnosno ona s kojom smo podijelili ključ koji dekriptira zaštićenu poruku.

Softver te vrste će se i dalje razvijati i napedovati i postajati u svojoj funkciji sve bolji. Razlog tome je i djelom to što osobe koje izvršavaju napade također pronalaze nove načine na koje mogu napraviti štetu.

GNU Privacy Guard je dio GNU softvera i kao takav potpuno besplatan. Trenutni trendovi navode na zaključak da će u budućnosti besplatan postati još zastupljeniji i dostupniji krajnjem korisniku.

8. POPIS LITERATURE

[1] Borislav Đorević, Dragan Pleskonjić, Nemanja Maček: Operativni sistemi: UNIX i Linux, Viša elektrotehnička škola Beograd, 2004.

[2] https://upload.wikimedia.org/wikipedia/commons/a/af/Tux.png

[3] http://distrowatch.com/dwres.php?resource=major

[4] http://www.linuxzasve.com/kako-je-nastao-linux

[5] https://www.dailytut.com/wp-content/uploads/2011/10/24-560x490.png

[6] https://wiki.open.hr/wiki/Linusovo_pismo

[7] https://wiki.open.hr/w/images/5/5a/Stallman_i_linus.png

[8] Raphaël Hertzog, Roland Mas: The Debian Administrator's Handbook, 2015.

[9] Martin F Krafft: The Debian System Concepts and Techniques, Open Source Press GmbH, 2005.

[10] https://www.debian.org/releases/index.hr.html

[11 http://www.riteh.uniri.hr/zav_katd_sluz/zr/nastava/uur/download/predavanja/2010-2011/UUR4_2010.pdf

[12] Božidar Kovačić, Operacijski sustavi skripta, Rijeka 2008

[13] http://vpnexpress.net/wp-content/uploads/2014/03/GnuPG.jpg

[14] https://www.digitalocean.com/community/tutorials/how-to-use-gpg-to-encrypt-and-sign-messages-on-an-ubuntu-12-04-vps

[15] http://public.mzos.hr/lgs.axd?t=16&id=18552

[16]http://www.asoo.hr/UserDocsImages/Kurikulumi/SZ_Tehnicar%20za%20racunalstvo_za%20odobrenje_2013_02.pdf