

Jul 2014.



LIBRE!

Časopis o slobodnom softveru

broj

27

KALI LINUX

The quieter you become, the more you are able to hear.



22. jul, 2014.

Objavljena je nova verzija *Kali Linuxa*



27. jul, 2014.

Tuluz uštedio milion evra prelaskom na *LibreOffice*.



Creative Commons Autorstvo-Nekomercijalno-Deliti pod istim uslovima



Časopis ili blog? Ponovo?!

Ovu dilemu smo rešili već u prvom broju časopisa. Zašto se opet vraćamo na ovu temu? Da vas odmah razuverimo, uopšte nemamo dilemu da li će i dalje LiBRE! biti časopis. LiBRE! časopis, makar dok je ova ekipa na čelu projekta, zadržaće formu časopisa. Postoji sada druga dilema, da li članci koji su primereni nekom blogu, mogu biti objavljeni u časopisu?

Časopis ima striktna pravila po pitanju forme i ozbiljnosti članaka koje objavljuje. To podrazumeva pisanje u trećem licu jednine i u prvom licu množine, zatim podrazumeva proveru objavljenih informacija. One moraju da budu tačne i da budu očišćene od subjektivnih utisaka. Zamka ovakve forme članaka, naročito pri predstavljanju nekog projekta, jeste monotonija i takvi članci mogu da liče na prepisivanje tehničke dokumentacije projekta. Naročito postaju dosadne recenzije velikih distribucija koje se u manje-više sličnoj formi ponavljaju na svakih šest meseci.

Blog je mnogo slobodniji po pitanju forme pisanja. Ima svojih mana u vidu unošenja previše subjektivnih utisaka, informacije ne moraju biti sto posto tačne jer su plod prvog utiska i možda su u kombinaciji sa

nekom greškom koju je bloger napravio pa nije dobio rezultat koji je po dokumentaciji projekta trebalo da dobije. Ako o ukusima ne treba raspravljati (ukus je potpuno individualna stvar) i informacije nisu sto posto tačne, da li je onda takav tekst za časopis?

Rešavanje ove dileme krenuli smo od korisnosti i zanimljivosti blogerskog teksta. Činjenica je da svaki blog pati od doze subjektivizma i dela dezinformacije koje su plod nedovoljnog proveravanja informacija, pa ipak mnogi blogovi su vrlo popularni baš zato što nisu suvo-parni. Da li su i korisni? Mislimo da jesu. Objektivne informacije o projektu čitalac, koji ih traži, može da nađe na više mesta (naročito u dokumentaciji projekta), a subjektivne utiske i eventualne probleme može da pročita samo u nečijem blogu. Problem možda postoji, a možda je i proizvod greške blogera. Bez obzira da li je greška u projektu, ili je greška blogera, velika je šansa da se ponovi i nekom drugom. Dobar bloger će dati i rešenje tog problema, tako da korist za čitaoca svakako postoji.

Ovakav pristup otvara zeleno svetlo blogerskim tekstovima u časopisu. Ipak LiBRE! ne sme da podleigne i postane teren za isključivo bloger-



ske tekstove. Ozbiljnost i proverena informacije mora da ostane imperativ našeg časopisa. Zato ćemo samo odškrinuti vrata za blogerske tekstove ekskluzivno u podrubrici „U potrazi za idealnom distribucijom”.

U ovom broju u podrubrici „U potrazi za idealnom distribucijom” objavljujemo blogerski tekst o *Ubuntu 14.04*. O *Ubuntu* smo za ove dve i po godine već pisali četiri puta, a ovim novim pristupom pokušavamo da ne postanemo dosadni. Osim blogerskog predstavljanja distribucija, zamolićemo blogere da pišu i kako su svoje distribucije prilagodili sopstvenim potrebama, što po našem, skromnom, mišljenju može da bude zanimljivo čitaocima.

Vaše blogerske tekstove, mišljenja, kritike i primedbe i dalje možete slati LiBRE! redakciji na već poznatu adresu elektronske pošte `libre [et] lugons [dot] org`.

Do čitanja

LiBRE! tim

Moć slobodnog
softvera



Broj: 26

Periodika izlaženja: mesečnik

Izvršni urednik: Stefan Nožinić

Glavni lektor: Aleksandar Božinović

Lektura:

Milena Beran

Jelena Munčan

Maja Panajotović

Aleksandra Ristović

Redakcija:

Đejan Čugalj

Aleksandar Todorović

Marko Kažić

Gavrilo Prodanović

Veljko Simić

Aleksandar Brković

Nikola Hardi

Mihajlo Bogdanović

Petar Simović

Vladimir Cicović

Zlatan Vasović

Marko Novaković

Aleksandar Vesić

Saradnici:

Goran Mekić

Sandrina Dimitrijević

Željko Popivoda

Nedeljko Stefanović

Joakim Janjatović

Stefan Stojanović

Jelena Georgijević

Vladimir Popadić

Počasni članovi redakcije:

Aleksandar Stanislavljević

Željko Šarić

Grafička obrada:

Dejan Maglov

Ivan Radeljić

Dizajn:

Mladen Ščekić

Zoran Lojpur

Kontakt:

IRC: #floss-magazin na irc.freenode.net

E-pošta: libre@lugons.org

<http://libre.lugons.org>



LiBRE! vesti str. 6

Vesti



Puls slobode str. 8

Mumble kanal
Linux zajednice Srbije str. 8



NSA vas prati! str. 12

U susret:
BalCCon2k14 - Second Base
(2. deo) str. 14

Predstavljamo str. 17

Kali Linux - Reinkarnacija str. 17



U potrazi za idealnom
distribucijom:
Ubuntu 14.04 str. 22



Kako da...? str. 28

libGDX
„Java game development
framework” (3. deo) str. 28

libGDX

Uvod u programski
jezik C (4. deo) str. 32

Oslobađanje str. 35

Uticaj matematike na
nastanak i temelje
računarstva (3. deo) str. 35

Demokratija zahteva
slobodan softver str. 39



Slobodni profesionalac str. 41

Pure str. 41



Internet, mreže komunikacije str. 44

Enkriptovana elektronska pošta (2. deo) str. 44



Apache Lucene: Korak od Googla str. 48



LIBRE! prijatelji





Objavljen je CentOS 7

7. jul, 2014.



Dugo očekivano izdanje *CentOS 7* konačno je objavljeno. Ova distribucija nastala je kompajliranjem izvornog koda *Red Hat Enterprise Linux 7*.

Koristan link: <http://j.mp/WVFC6m>

Novi Zorin OS 9 je stigao

15. jul, 2014.



Tačka težišta *Zorin OS* tima bile su stabilnost i brušenje širokog spektra njegovih sjajnih performansi. *Zorin OS 9* je baziran na *Ubuntu 14.04 LTS*.

Koristan link: <http://j.mp/1xW1yJu>

Nova verzija FreeBSD 9.3 je dostupna

15. jul, 2014.



Sada je dostupna četvrta dopuna stabilnog devetog izdanja *FreeBSD*-a. Naglasak je na unapređenju stabilnosti verzije 9.2.

Koristan link: <http://j.mp/1lrV97U>

Objavljen Deepin 2014

21. jul, 2014.



Objavljena je nova verzija ove kineske distribucije koja osvaja sve veći broj korisnika svojom jednostavnošću i ugodnim dizajnom.

Koristan link: <http://j.mp/1pyMQX3>

Kali Linux 1.0.8

22. jul, 2014.



Nova verzija *Kali Linux* donosi podršku za *USB EFI boot* što omogućava instalaciju i pokretanje ovog sistema na najnovijem hardveru kao što je

Apple iBook.

Koristan link: <http://j.mp/1mec9tJ>

Talis 1.1

22. jul, 2014.



Talis

Poznata *Linux* distribucija koja štiti privatnost svojih korisnika, *Talis*, objavila je svoju novu 1.1 verziju. Svim korisnicima se preporučuje da što pre

pređu na novu verziju u kojoj su ispravljani brojni sigurnosni propusti, unapređena podrška za *UEFI boot*, zamenjena *Windows XP* kamuflaža sa *Windows 8* kamuflažom itd.

Koristan link: <http://j.mp/1s3mGfk>



GOG.com od sada nudi i igre za Linux
25. jul, 2014.



GOG je najavio da će do kraja godine objaviti sto igara za operativni sistem *Linux* iz svoje ponude.

Koristan link: <http://j.mp/1zMB5Rr>

Tuluza uštedeo milion evra prelaskom na LibreOffice
27. jul, 2014.



Tuluza, četvrti najveći grad u Francuskoj, objavio je rezultate svoga prelaska na *LibreOffice*. Proces tranzicije započeo je u 2011. godini i trajao je sve do aprila ove godine. U njega je uloženo 800 000 evra, a donosi uštedu od milion evra.

Koristan link: <http://j.mp/1pyMSyh>

QEMU 2.1
1. avgust, 2014.



Objavljena je nova verzija *QEMU*-a 2.1.

Koristan link: <http://j.mp/1ky3kju>

GPLv3 dizajn 2D/3D grafičke kartice u Verilogu je sada dostupan
3. avgust, 2014.



open hardware

Iako je dosta ovakvih pokušaja propalo, jedan projekat je još uvek živ i aktivno se razvija.

Koristan link: <http://j.mp/1tMiqoq>

Steam ima više od 600 igrica za Linux
3. avgust, 2014.



Od pre dva meseca, broj igara za *Linux* na platformi *Steam* povećan je za otprilike sto igara.

Koristan link: <http://j.mp/1ky3UxL>

LIBRE! prijatelji

LUTHERUS

Et in Arcadia ego!



ictcasopis.ict.edu.rs



**LOVĆENAC
LINUX USER GROUP**



Grupa korisnika GNU/Linux operativnih sistema u Lovćencu

info i tutorijali na srpskom
lubunturs.wordpress.com





Mumble kanal

Linux zajednice

Srbije

Autori: Marko Pavlović i Ivan Radeljić

Uvod

U današnje vreme teško je zamisliti život (za neke i jedan dan) bez društvenih mreža. Voleli ih ili ne, one sve više čine našu svakodnevnicu. Prateći taj trend, u sklopu društvene mreže *Google+* nastala je zajednica „Linux u Srbiji”, koja okuplja sve zaljubljenike, poznavaoce i potencijalne nove korisnike slobodnih tehnologija (*FLOSS*) sa našeg govornog područja.

Zajednica trenutno broji trista osamdeset i tri člana i javnog je tipa, tako da svako može da pristupi. Članovi zajednice redovno objavljuju razne zanimljivosti i aktuelnosti vezane za *Gnu/Linux* i one su razvrstane po kategorijama. Tako možete pročitati najnovije vesti, zatražiti pomoć, pogledati tutorijal, započeti diskusiju,

izneti sugestiju, ili se pohvaliti slikom svoje *Gnu/Linux* radne površine.

Kako bi dodatno poboljšao komunikaciju među članovima naše zajednice, osnivač Marko Pavlović (*Shiva*) je iznajmio i podesio *Mumble* server (*VoIP* softver za ćaskanje). Njegovu ideju je podržao određen broj članova i ubrzo je u večernjim satima na serveru nastalo pravo druženje.

Teme i redovni sastanci

Teme su u početku bile *Gnu/Linux* distribucije, odnosno sličnosti i razlike među njima. Kasnije se pričalo o detaljnim podešavanjima, razmenjivala su se iskustva i neke od specifičnih situacija sa kojima su se pojedini članovi susretali. Naravno, svako je mogao da zatraži bilo kakvu pomoć vezanu za svoj *Gnu/Linux* OS i svi članovi se zaista trude da pomognu, a



sve to kroz jedan prijateljski razgovor.

Na tim druženjima nikada se nisu unapred definisale teme o kojima će se diskutovati, već je to uvek išlo sponatano, nekada i nevezano za *Gnu/Linux*, pa se tu može čuti i dosta priča kojima je sam život bio režiser.

Međutim, pre nekoliko meseci poseta serveru je blago zatajila. Usled nepostojanja dogovorenog termina, većina članova se mimoilazila na serveru, pa je teško odmah po logovanju aktivno se uključiti u razgovor.

Shvativši to, osnivači su došli na ideju da organizuju redovne sastanke koji će se održavati u unapred određenom terminu. Dogovor je pao, održavaće se

sredom u 20 časova. Kako je vreme odmicalo, ispostavilo se da je to bio pravi pogodak. I pored toga što članovi mogu u svako doba da pristupe serveru, nekako svi smo navikli da to bude u dogovorenom terminu. Ne bismo nikoga posebno izdvojili, ali svako ko je bio makar jednom na sastanku, imao je više nego pozitivno iskustvo.

Na poslednjim sastancima broj *on-line* korisnika je prelazio petnaest. Istakli bismo činjenicu da posete nisu samo iz Srbije, pa smo tako imali i goste iz susedne Hrvatske, kao i naše redovne članove iz zapadne Evrope. Zbog raznih sfera interesovanja, na serveru smo otvorili i privatne kanale koji su vezani za jednu određenu oblast (kanali su uglavnom povezani sa nazivom





Gnu/Linux distribucija). Tu bismo izdvojili **LiBRE!** kanal, na koji slobodno možete svratiti i reći svoje mišljenje u vezi časopisa, priključiti se redakciji, kao i izneti predloge za njegovo poboljšanje.

Mumble podešavanja

Mumble je *open-source* softver koji je odličan za časkanje i za igranje igrica. Komunikacija je uvek enkriptovana, pa je privatnost zagarantovana. Da biste koristili *Mumble* server, potrebno je instalirati klijent koji postoji za *Gnu/Linux*, *Mac* i *Windows*. Kod *Gnu/Linux* operativnih sistema to je najlakše učiniti iz riznica. Jedna od prvih stvari koje bismo spomenuli, jeste registracija na serveru jer tako dobijate određene privilegije na pojedinim kanalima i mogućnost otvaranja kanala nad kojima ste administrator. Nakon registracije trebalo bi da napravite rezervnu kopiju svojih *Mumble* sertifikata i *Mumble* konfiguracionog fajla: `~/config/Mumble/Mumble.conf` Ukoliko ste početnik u korišćenju *Mumble* softvera, može se desiti da imate problema sa podešavanjem *push-to-talk* prečice i podešavanjem mikrofona. U tom slučaju možete se nakačiti na server kada je tu neko od korisnika i oni će vam pomoći da podesite *push-to-talk*, ili možete pokušati sami sledeći ove smernice:

- poželjno je da na sastancima koristite slušalice i imate utišane zvučnike kako ne biste pravili eho drugim korisnicima.
- poželjno je da podesite **configure** >

Settings > **Audio Input** > **Interface System** na *pulseaudio* i opciju **transmission** > **transmit** na istoj strani na *push-to-talk*. Takođe, kada to podesite, dodajte i na kartici *shortcuts* prečicu za *push-to-talk*.

Pošto završite ta sitna podešavanja *Mumble* klijenta, trebalo bi da bude spreman za korišćenje. Ne treba zaboraviti da od sada, kada želite da pričate na kanalu, morate da držite pritisnuto dugme za *push-to-talk* koje ste izabrali u podešavanjima. Koristili smo **Left Ctrl** + **Left Win** kao prečicu (prim.aut.).

To možete testirati prelaskom na bilo koji kanal osim *AFK* i pritiskom na crveno dugme na traci sa alatkama pokrećete snimanje, zatim pritisnite *push-to-talk* prečicu i izgovorite nekoliko reči dok snimate svoj glas i potom lansirate tu datoteku u omiljeni audio *player*. Ukoliko čujete svoj glas, podesili ste dobro *Mumble* klijent.

Za sva dodatna podešavanja i eventualne probleme koje imate sa *Mumble* klijentom, obratite se za pomoć zajednici „*Linux* u Srbiji”, ili još bolje direktno na samom *Mumble* serveru. Na klijentu imate opciju da pišete tekstualne poruke, tako da i kada vam ne radi mikrofona, možete pisati, svakako će se naći neko od iskusnijih korisnika da pomogne u podešavanjima.

Parametri pristupa

Label - Linux zajednica Srbije

Address - mumble-de.cleanvoice.ru



Port - 61030

Username - Vaše korisničko ime (po želji)

Ideje, planovi

Da sastanci ne budu samo prazne priče određenog broja ljudi, članovi zajednice su rešili da neke od ideja sprovedu u delo. Naime, u planu je da se u narednom periodu iskoristi znanje trenutnih članova *Mumble* kanala „Linux zajednice Srbije” i da se organizuju predavanja na teme vezane za slobodan softver. Na sastancima se inače razmenjuje znanje među članovima koji su tada prisutni, ali ništa od toga ne ostaje sačuvano. Predavanja će biti u formi *webinara*, a pošto *Mumble* nije pogodan za taj tip predavanja, za sada se razmatraju alternative koje će u potpunosti ispuniti zahteve predavača. Svi zainteresovani će moći uživo pratiti predavanja koja će kasnije biti dostupna i za preuzimanje.

Za početak imamo nekoliko predavača. Oni odlično poznaju oblasti koje će predavati i svoje znanje će nesebično deliti sa drugima. Zamišljeno je da predavanja traju četrdeset i pet minuta gde će naratora pratiti slajdovi kako bi bila dinamičnija. I dok traju dogovori oko tehničke strane predavanja (koja platforma će biti korišćena za strimovanje, testiranje audio-video kvaliteta i dr.), vi se možete prijaviti kao jedan od narednih predavača. Poželjno bi bilo da već posedujete slično iskustvo, jer bi zajednica „Linux u Srbiji” učestvovala na *FLOSS* konferencijama i prezentovala svoja najbolja predavanja.

S nadom da će ideje brzo realizovati, LiBRE! tim će pisati o svakom predavanju koje zajednica „Linux u Srbiji” objavi.

Korisni linkovi:

- [1] Google+ zajednica: „Linux u Srbiji”
- [2] <http://mumble.sourceforge.net/>





NSA vas prati!

Autor: Aleksandar Todorović

Zanimajte li se za anonimnost na internetu? Čitate li magazin o *Linuxu*? NSA vas prati!

Uvod

Prošlo je više od godinu dana kako je *Snowden* izašao u javnost sa prvim informacijama o tome u kolikoj mjeri nas NSA prati. Podaci koje on iznosi, i u ovo doba su vrlo aktuelni. Međutim, sada su objavljeni novi podaci, a neki od stručnjaka smatraju da ovo prvi put nije djelo *Snowdena*, nego da je u pitanju neki novi, za sada neidentifikovan zviždač [1] [2].

Zanimajte li se za anonimnost na internetu? Prati vas NSA!

Do sada smo saznali mnogo toga o tome ko su tačno mete koje NSA pokušava da napadne – od direktnih pristupa vodećim internet kompanijama kao što su *Google*, *Microsoft*, *Facebook*, *Dropbox* i ostali, preko namjernog oslabljivanja enkripcijskih algoritama, pa do pokušaja invertovanja anonimnosti koje pruža *Tor* (program fokusiran na



anonimnost na internetu).

Međutim, novi javno dostupni podaci nam govore da tu ne staje opseg napada na obične korisnike. Ukoliko ste se nekada zanimali za anonimnost na internetu, prati vas NSA. Ukoliko ste ikada posjetili stranicu *Tor* projekta, koristili *Tails Linux* distribuciju, koristili *TrueCrypt* za enkripciju podataka, ili su vas zanimali neki drugi drugi programi vezani za anonimnost i sigurnost na internetu, od tada ste na listi osoba koje prati NSA (prim. aut.).



Postoje mnogi razlozi za anonimnost na internetu i svima je jasno da većina od tih razloga nema neku malicioznu aktivnost u fokusu. Od onog malog dijela razloga koji imaju za cilj neku malicioznu aktivnost, šanse da tom malicioznom aktivnosti prijetite



sigurnosti SAD-u su toliko niske da nisu vrijedne spomena. Međutim, izgleda da NSA smatra drugačije.

Čitate li poznati *Linux* magazin? Prati vas NSA!

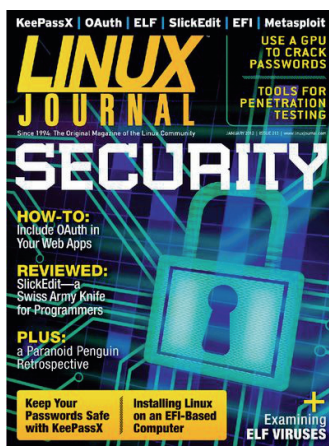
LINUX JOURNAL

Da tu ne staje kontroverza oko novih podataka, govori i podatak kako se među listom domena koje NSA prati, našla i jedna domena koja je potpuno nepovezana sa anonimnosti na internetu. Ta IP adresa pripada jednom od najpoznatijih magazina u svijetu koji se fokusira na *Linux* i *open source* softver. U pitanju je *Linux Journal* magazin. Kao da ni to nije dovoljno, u dijelu izvornog koda koji je postao dostupan javnosti, *Linux Journal* je u komentaru opisan kao forum koji koriste ekstremisti. Šta je ekstremistično u pisanju o *Linuxu*, nije nam poznato.

Zaključak

Već dugo vremena znamo da radnje koje provodi NSA nisu legalne i kako špijuniraju bilo koga, ko im padne na pamet. Dobro je poznato i da je mala vjerovatnoća da postoji osoba na planeti koja nije u poslednjih petnaestak godina bila na meti NSA i čiji dio podataka

nije završio u njihovom centru za smještanje podataka. Međutim, sada je javno poznata nova informacija. NSA u svom sistemu dijeli internet korisnike na dva dijela: na korisnike koji znaju nešto o privatnosti na internetu i korisnike koji se ne raspituju o tome. Svi članovi iz prvog dijela internet korisnika su pod nadzorom i sve što NSA može da skupi o tim osobama, ona skuplja. Međutim, uzimajući u obzir da je *Linux Journal* domena napadnuta, dolazimo do zaključka da vas ne mora zanimati anonimnost na internetu da bi vas NSA pratila. Čak i obični *Linux* korisnici koji čitaju navedeni magazin, pod pratnjom su i njihovi podaci se sakupljaju. Ko zna, možda je naš magazin sljedeći na redu.



Korisni linkovi:

- [1] https://www.schneier.com/blog/archives/2014/07/nsa_targets_pri.html
- [2] http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html
- [3] Izvorni kod: <http://daserste.ndr.de/panorama/xkeyscorerules100.txt>



U susret:



2k14 - Second Base

(2. deo)

Autor: jelena&milobit&BobuS von LUGoNS

U Novom Sadu od 05. do 07. septembra u Muzeju savremene umetnosti Vojvodine održaće se drugi po redu regionalni hakerski kongres *BalCCON2k14 – Second Base*. Prošli se zvao „Prvi kontakt”, a ovaj treba da bude dalji napredak pa je dobio ime „Druga baza”. Da li je to ideja hakera koji se bavi bejzbolom? Kada neko pročita da se održava hakerski kongres, ko zna šta mu iskrsne u mislima? Momci sa pepeljarama koji bulje u ekrane, dredovi i martinke, ili ko zna kakva kombinacija nastala u glavama holivudskih dizajnera? (prim. aut.)

Program kongresa obuhvata brojne prezentacije, radionice kao i predavanja iz oblasti bezbednosti računarskih sistema, sa posebnim osvrtom na društvenopolitičke teme, poput zaštite privatnosti na internetu, slobodnog softvera, programskih jezika, razvoja aplikacija i brojne druge. Predavači su poznati i priznati pripadnici hakerskih zajednica iz

celog sveta.

Organizatori kongresa su novosadsko udruženje *Linux* korisnika *LUGoNS* i *Wau Holland* fondacija iz Hamburga. Osnovni cilj udruženja je rad na boljitku društva, podsticanje korišćenja *GNU/Linux* sistema, kako u preduzećima, tako i kod pojedinaca i entuzijasta. *LUGoNS* je podrška svim *Linux* korisnicima, kako u Novom Sadu, Vojvodini, tako i u Srbiji. Članovi udruženja nastoje takođe da podignu svest o informatičkoj kulturi i promovišu *FLOSS* (eng. *Free/Libre and Open Source Software*).

Zamišljeno je da *BalCCON* postane centar hakerske zajednice u regionu, svima koji finansijski nisu u mogućnosti da posećuju druge kongrese u Evropi i SAD-u. Ovakva manifestacija neophodna je na Balkanu, kako bi postojalo mesto na kome se jednom godišnje razmenjuju novostečena znanja, sastaju mladi puni ideja i stariji puni iskustva i znanja, da se upoznaju, povežu i ohrabre svi koje računari, mreže, sigurnost i nekonvencionalan način razmišljanja zanimaju, a nemaju gde da dobiju željene informacije. Time bi se u samoj hakerskoj zajednici podizao nivo

stručnosti uz vođstvo starijih kolega, a i rešio bi se problem nemogućnosti da se dopre do prostora i vremena da se sopstveni radovi prezentuju. Dovođenje poznatih i priznatih ljudi kao predavača, jeste omogućavanje ljudima iz regiona da te iste predavače sada vide uživo, te da diskutuju sa njima na teme koje ih interesuju. *BalcCon* želi da približi svet studentima koji se interesuju za haktivizam, slobodni kôd i tehničke nauke, te svim mladima kojima su ove i srodne teme interesantne. Na ovaj način, mladi imaju priliku da prezentuju svoje radove ukoliko su interesantni, inovativni i u skladu sa moralnim načelima za koje se zalaže cela zajednica okupljena oko slobodnog kôda. Hajde da vidimo ko su predavači. Hakeri to jesu. Haker je onaj ko svoje znanje o računarima želi da prenese i podeli sa drugima. Ideja da je hacker nešto zlonamerno, nastala je u glavama holivudskih dizajnera. Dođite! Otvorite oči i uši i primite pametne informacije, a da ne dolaze iz TV uređaja ili sa nekog „lajovanog“ (ne nedostaje slovo **k**, prim. aut.) linka.

• *Mitch Atman:*



Haker iz San Franciska, pronalazač. Autor uređaja koji gase sve poznate marke televizora i pušta

vaš um na slobodu. Rešen je da podeli sa vama svoje znanje o elektronici, lemljenju i da zajedno sa njim napravite svoj sopstveni *Arduino* kontroler.

• *Bernd Fix:*



Haker iz Berlina, osnivač *Chaos Computer Cluba* 1986. godine. Tvorac prvog demo virusa u Časopisu. Drži se maksime pravog hakera: „*Dont' mess around with other people's data*“. Možete čuti šta se novo dešava na polju tzv. postkvantum kriptologije. Čemu to služi? Nemamo pojma, ali ćemo doći na predavanje (prim.aut.).

• *Aleksandr Timorin:*



SCADA sistemi - na prvi pogled potpuno van bilo kakvog životno potrebnog znanja (prim.aut.). Ko bi rekao kakvo hakersko znanje se valja iza površine?

• *Anand Buddhdev:*



Znate li ono, kada se pitate koja *IP* adresa, koje ime, *DNS* serveri, gde se to registruje? Anand dolazi iz *RIPE NCC*, a držaće uvod u *Ansible*, ni manje ni više.



- Voja Antonić i Dejan Ristanović:



Da li se neko seća časopisa „Računari u vašoj kući”, pa još prvog broja, sve sa opisom samogradnje računara Galaksija? Upoznajte lično njenog tvorca. Šta još zna? Čujte i ova predavanja! Nije sve zastarelo, nešto je postojalo i pre toga.

- Žarko Živanov:



Ko se seća gore-pomenute Galaksije, Komodora, ZX Spectruma i Amstrad računara, moći će od Žarka da čuje mnogo toga, a što je najbolje, moći će to

uživiti i da proba. Retro kutak, sećanje na sate i sate igre na najboljim mašinama na svetu.

- Moritz Bartl:



Nemački izraz *ZwibelFreunde* znači „prijatelji luka”. Luka? Ako se setimo kako izgleda logo za *Tor*, stvari će postati jasnije. Hoćete li doći?

Šta još reći - dođite, čujte, vidite, probajte! Nije haker ono što piše Holivud.

Lista predavača nije konačna, ali je možete pratiti na:

<https://2k14.balcccon.org/index.php?title=Speakers>

Ukoliko smo vas zainteresovali da prisustvujete kongresu, rezervišite i kupite kartu na sajtu <https://tickets.balcccon.org>.

Takođe, ukoliko imate neka pitanja, možete stupiti u kontakt s nama preko *e-maila* na [orga \[at\] balcccon \[dot\] org](mailto:orga@balcccon.org).

Više o programu i organizaciji na: <https://balcccon.org>

Zvanični *Twitter* nalog: @BalCCon2k14





Reinkarnacija

Autor: Aleksandar Vesić

Backtrackov nasljednik - „Kali Linux 1.0”

Posle pet glavnih izdanja, *BackTrack* više ne postoji. Ipak, ljubitelji te *Linux* distribucije koncipirane za *pentesting* (provala u *IT* sisteme) ne treba da budu tužni jer je sa *Kali Linuxom 1.0* došao dostojni nasljednik koji je ceo projekat prebacio u jedan ozbiljni *Debian* derivat. Prvi put je javnost saznala za ime *Kali Linux 2.2* januara 2013. od *Offensive Securityja*, tima okupljenog oko izraelskog specijaliste za *IT* bezbednost *Mati* („*muts*”) *Aharonija*. Tim *Offensive Securityja* je na svojim blogovima i putem *Twittera* objavio da je *BackTrack* ponovo rođen. Dan izdavanja te *Linux* distribucije specijalizovane za *IT*-bezbednost sa afinitetom za penetracione testove bio je *Black Hat Europe* u Amsterdamu i već 13. marta je

Kali Linux 1.0 bio spreman za preuzimanje.

Broj izdanja 1.0 ne treba nikog da zavarava, jer *Aharonijeva* distribucija potiče od slavni predaka. Od nekadašnjeg *Whoppixa* je nastao *WHAX*, a *WHAX* i *Auditor* su se stopili 2006. godine u *BackTrack* i od *BackTracka* je posle sedam godina i deset zvaničnih izdanja nastao *Kali Linux*. Kod ove distribucije radi se o čistokrvnom *Debianovom* derivatu baziranom na *Wheezyju* i taj 3.7 *kernel* sadrži sve neophodne zakrpe potrebne za iniciranje paketa za napade na bežične mreže.

Kali Linux je moguće preuzeti u različitim varijantama, *ISO* paket postoji za *x86* i *x64* arhitekture. Pored toga, postoji kompletno instalirani *Kali* sistem u formi virtuelne *VMware-x86* mašine. Kao okruženje radne površi koristi se *GNOME*, ali kao alternativa se nudi i minimalistička verzija kompletno bez



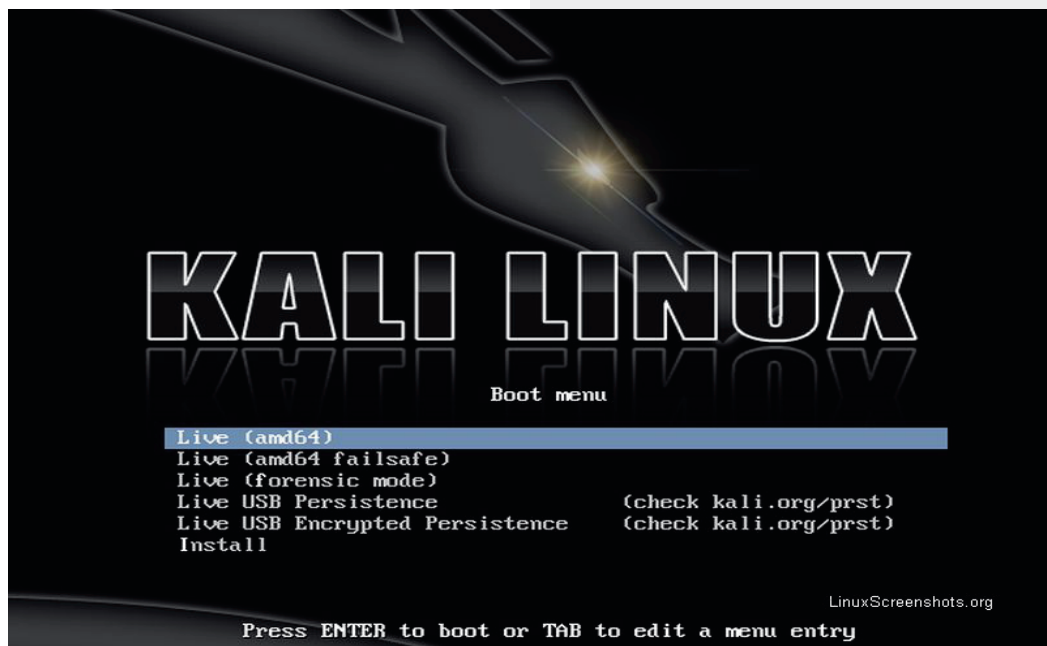
okruženja radne površi. Ukoliko želite drugačije okruženje, kao npr. *KDE*, *LXDE*, *xfce*, *E17* ili *MATE*, to je takođe moguće sasvim jednostavno izvesti. *ISO* varijanta dozvoljava pored *Live-Boota* isto tako direktnu instalaciju kao i forenzički modus. Forenzički modus ostavlja hard disk sistema, koji se istražuje, nedirnutim i sprečava automatsko montiranje svih priključenih memorija, *HD*-a i *USB*-a. Pored ostalog, nije zaboravljena ni instalacija putem mreže *PXE* (*Preboot Execution Environment*) koju je moguće bez komplikacija podesiti.

Funkcionalnost i na malim sistemima

Kali je takođe dostupan i za *ARM* arhitekture *ARMEL* i *ARMHF*. U vreme

izdavanja je testiran na uređajima *Samsung Chromebook*, *SainSmart SS808*, *ODroid-U2* i *Raspberry Pi*. Kao radno okruženje se koristi *xfce*. Sama mogućnost da svako može *Kali Linux* da koristi čak i na minimalističkim računarima koji su jednostavni da se skriveno nose, može biti važno za bezbednost i ne sme se nikako ignorisati.

Kali Linux izgleda na prvi pogled poput *BackTracka*, čak su i inicijalni podaci za *Login* (*root/toor*) zadržani. *GNOME* struktura menija je prerađena, ali se može brzo naviknuti na nju ako već imate radno iskustvo sa *BackTrackom*. Upada u oko i nova „Top-10” lista u kojoj se nalaze najprominentniji alati za *IT* bezbednost koji su linkovani na jednom mestu. Tu su između ostalih *Metasploit Framework*, *Maltego Community*, *Nmap*, *Hydra* i *Aircrack-ng*.



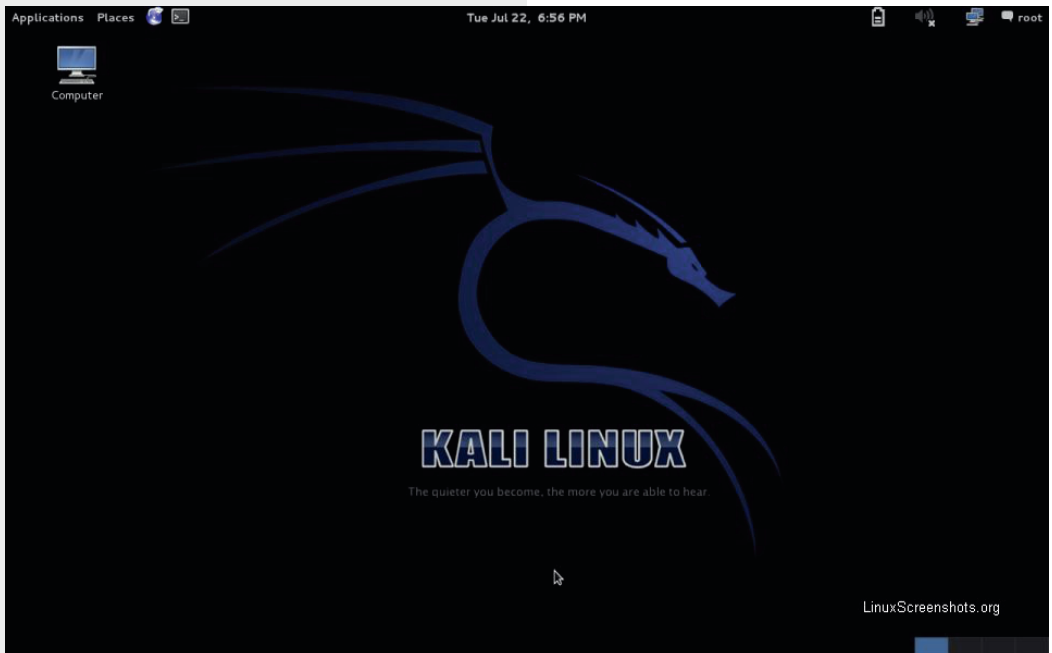


Kali GUI se predstavlja prerađenom strukturom menija, ali nema potrebe očajavati jer se *Kali* pridržava *FHS*-a (eng. *Filesystem Hierarchy Standard*), tako da su aplikacije u „pretraži” funkciji uključene i dostupne svuda. Standardni rečnik poznat kod *BackTracka* koji se koristi za napade na sisteme zaštićene lozinkom, na primer uz pomoć *Hydre*, reduciran je na listu **rockyou.txt** veličine **134MB**. Nju je moguće naći u *gzip* komprimiranoj formi na **/usr/share/wordlists**. Zbog toga svega su se pojavile kontroverzne diskusije na forumima gde se nemilice raspravlja i iznose argumenti „za” i „protiv” nove strukture.

Aharonijeva odluka da od samog početka projekta *Kali* uključi *Debian* specijalistu *Raphaela* („buxy”) *Hertzoga*, pokazala se odličnom. *Hertzog* je izuzetno doprineo

kod tehničkog dela oko infrastrukture vezane za riznice kao i kod mogućnosti koju ima *Kali* da svako može da napravi svoj lični i sebi prilagođen *ISO* uz pomoć *Debianovog live-build scripts*. Detaljno uputstvo kako se to može učiniti, već se nalazi u *Kali* dokumentaciji. Osim toga, njihov tim održava za svakog vidljive otvorene verzije preko *gita* u kojima su autori pobrojani i svi oni moraju pakete da potpišu sa *GPG*.

Community koja aktivno učestvuje u projektu, aktivno je podržana od strane mnogih proizvođača, a od pojedinih neočekivano mnogo. Tako na primer *RAPID7* (*Metasploit*) vodi *Kali Linux* kao zvanični operativni sistem za komercijalnu verziju *Metasploit*-a i samim tim nudi „podršku proizvođača”. Komercijalna varijanta *Web* radne površine od *Metasploita* je tako integri-





sana u *Kali Linux*. Naravno, besplatno je moguće koristiti samo *Community* verziju i to tek nakon što ste se registrovali. Besplatni *Metasploit Framework*, osnova i ideja današnjih *Metasploit* proizvoda oduvek spada u *Aharonijev* standardni repertoar i nudi pojednostavljenu radnu površinu za napade putem *Exploits*.

Proizvođači i njihova uloga

Aharonijev tim je pokušavao još od vremena *BackTracka Metasploit-Framework* da upakuje u paket, koji nije ni predviđen da bude upakovan. *RAPID7* je, kako navodi *Aharoni*, iskoristio *Kali Linux* da napravi jedan pravi *Debian* paket za *Metasploit* i povrh toga obećao je da će o svom trošku da ga aktualizuje svakih sedam dana.

Paterva je svoju *Maltego-Community* verziju *Kali Linux Edition 3.3.0* postavio dostupnom. Uz pomoć *Maltegoa*, moguće je u *IT* bezbednosnom okruženju sakupljati podatke i iste potom dinamički-agregirano predstaviti. Taj proizvođač se oduvek fokusirao na pregledno vizualiziranje kompleksne povezanosti sakupljenih podataka i njihovu međusobnu povezanost. Kao i kod *Metasploita*, u poređenju sa komercijalnom verzijom, *Community* verzija ne nudi sve mogućnosti i za njegovu upotrebu se mora registrovati.

Automatska aktualizacija dolazi

Što se tiče aktuelnosti oruđa koje stoji na raspolaganju povezano sa *Debian* paketom, postoje planovi za bližu



budućnost. *Aharoni* je otkrio da njegov tim radi na ideji da uz pomoć automatizovanog centralnog sistema, određene eksterne *git* i *svn repositories* u realnom vremenu nadgleda i da kod novih verzija automatski generiše u nove *Kali* pakete. Na osnovu izjave razvojnog tima da su izvršili veliku akciju čišćenja integrisanih alata, u *Kali Linuxu* se nalazi više od trista poznatih alata, od onih za napad i analizu do onih za *Reverse engineering* i digitalnu forenziku kao npr. *TSK* sa *Autopsy*. Pored standardne podrške za mnogobrojne *WLAN* čipove, u bežičnom okruženju su takođe zastupljeni i *Bluetooth*, *RFID*, *NFC* kao i *ZigBee*.

Popularni *Frontend* za *Metasploit Framework* pod imenom *Armitage* koji je u trenutku izdavanja verzije 1.0 nedostajao, moguće je jednostavno uz pomoć **apt-get install armitage** naknadno instalirati. Naravno, ukoliko *Armitage* nedostaje, moguće ga je takođe uz pomoć **apt-get dist-upgrade** automatski instalirati.

Inače *Kali Linux* se ponaša jako tiho u mreži. Pojedini servisi koji omogućavaju spoljnu identifikaciju, kod startovanja sistema su deaktivirani i moraju se po potrebi startovati. To važi podjednako i za *Metasploit* ili *Armitage* pre čije upotrebe je potrebno koristiti komande **service postgresql start** za baze podataka i **service metasploit start** za *RPC* i *Web-Service*. Ukoliko želite to da automatizujete prilikom podizanja sistema, možete koristiti **update-rc.d <service> enable**.

OpenVAS & Co. traže ranjivosti

U oblasti analize ranjivih tačaka *Kali Linux* integriše pored raznih *Fuzzera* i *Scannera* takođe i *OpenVAS*, jedne varijante skenera ranjivosti *Nessus*. Kome je *Nessus* draži, može da skine *Debianov* paket sa internet stranice proizvođača i putem **dpkg -i <Package>** kao i **/etc/init.d/nessusd start** instalira i pokrene. Ranjivosti kod *Web* aplikacija moguće je istražiti uz pomoć raznih skenera, između ostalog i sa *Burp Suite Free Edition 1.5*.

Zaključak

Kada su *Aharonija* pitali za značenje naziva *Kali*, odgovorio je da je *Kali* jedno lepo ime i da ima mnogo značenja u različitim jezicima, kao i da oni nisu ništa specifično time hteli da kažu.

Sama distribucija ostavlja jedan jako pozitivan utisak. Ne viđa se često da jedan *Community* projekat tako detaljno obnovi i oživi distribuciju koje više nema. Zadivljujuće je da mali tim od petoro ljudi ostvari takve rezultate i pored toga definiše de fakto standard za sve distribucije koje se fokusiraju na *IT* bezbednost. Mi im želimo mnogo sreće i uspeha u daljem razvoju kvalitetne *Kali Linux* distribucije.

Izvori:

- [1] <http://www.kali.org/downloads/>
- [2] <http://www.kali.org/official-documentation/>
- [3] <http://www.kali.org/community/>



U potrazi za idealnom distribucijom:



ubuntu^o

14.04

Autor: Aleksandar Todorović

Canonical je objavio novu verziju najpoznatije *Linux* distribucije 17. aprila. Ovo je *LTS* verzija (skr. *LTS* - *long term support*), što znači da ima podršku sljedećih pet godina. Nosi kodni naziv *Trusty Tahr*, a broj nove verzije je 14.04. Čekajući novu verziju moje najdraže distribucije (*elementary OS*), odlučih se da isprobam novu verziju *Ubuntu*a.

Da napomenem, ovo mi nije samo prvi put da koristim novu verziju *Ubuntu*a, nego mi je prvi put da koristim *Ubuntu* uopšte. Nikad ga prije nisam koristio i nisam siguran šta treba da očekujem. Ovo je sasvim subjektivno opisan moj put kroz *Ubuntu*.

Na laptopu sam imao instaliran samo jedan sistem - *Windows 8.1*. Pored njega je stajala gomila praznog prostora na hard disku predviđenog za neku *Linux* distribuciju i jedna odvojena enkriptovana particija (koristeći *TrueCrypt*) za podatke koje koristim i na *Linuxu* i na *Windowsu* (o nedavnoj kontroverzi *TrueCrypt*a sam pisao u prošlom broju). Na laptopu postoji podrška za *UEFI*,

međutim ta podrška je podrazumevano bila isključena još prije godinu i po dana kada sam kupio laptop. Ništa ne bi trebalo da spriječi da se *Ubuntu* instalira.

Ubacujem *USB* sa novom verzijom *Ubuntu*a i pokrećem *live* verziju *Ubuntu*a. Nikad nisam doživio da je potrebno duže od minute od klika za pokretanje *live* verzije do stvarnog pokretanja *live* verzije. Ostao sam začuđen. Međutim, shvatio sam da *Ubuntu* sa svojim *Unity* korisničkim interfejsom ne nosi bez razloga titulu jednog od najzahtjevnijih operativnih sistema koji su bazirani na *Linuxovom* kernelu.

Na prvi pogled, *Ubuntu* je lijepo dizajniran. Prate svoj dizajn iz verzije u verziju i to mi se sviđa. Odlučih da ga instaliram na slobodan prostor koji imam. Pokrećem instalaciju, od praznog prostora pravim tri particije: *swap*, *boot* i *root* particiju. Označim da mi se *GRUB* instalira na *boot* particiju, ostali dio sistema na *root* particiju. Uključujem opciju da mi se prilikom instalacije sistema instaliraju i vlasnički kodeci, a isključujem opciju da instaliram i svaki



trenutno dostupni *update* prilikom instalacije da bih ubrzao proces instalacije.

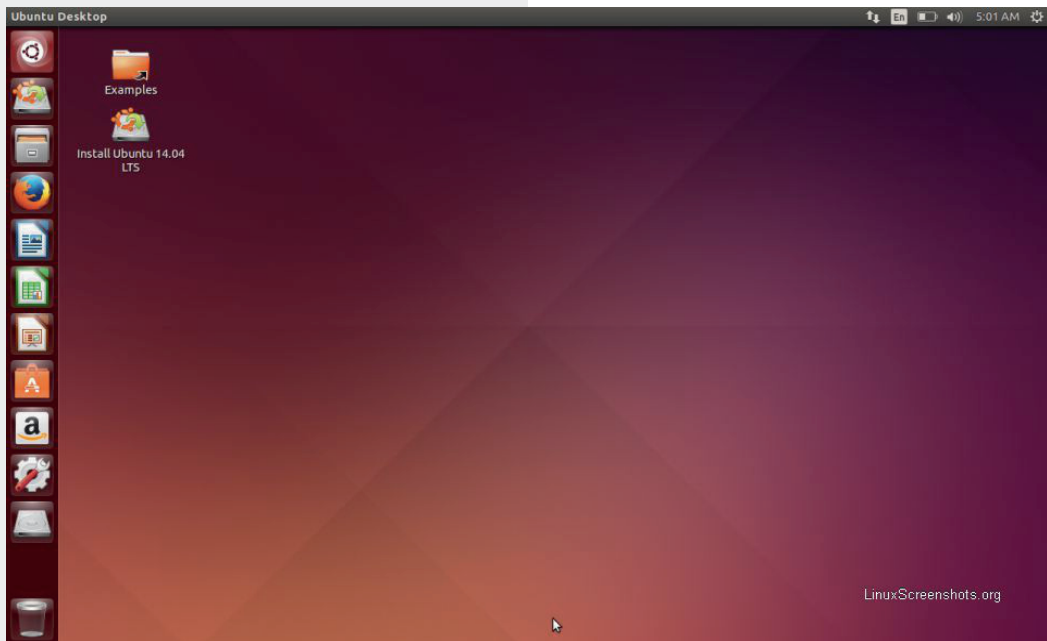
Moja želja da time ubrzam proces instalacije nije uspjela. Instalacija je trajala dobrih dvadesetak minuta, što je duže od bilo koje distribucije koje sam pokušao da instaliram (a pokušao sam mnogo). Gledajući u terminal prilikom instalacije, primjetio sam da se neke linije više puta ponavljaju. To je ostalo nerazjašnjeno u mojoj glavi. Završila se instalacija i sistem je tražio da ga restartujem, što sam i uradio.

Sistem se restartovao i *bootovao* u *Windows*!? Sad mi tek ništa nije bilo jasno. Tokom instalacije sam vidio komande za instalaciju *GRUB*-a, za njegov *update* i za prepoznavanje drugih sistema, međutim, *GRUB* se nije pokrenuo. *Boot* je izgledao potpuno

jednako kao i prije nego što sam instalirao *Ubuntu*. Tu sam već bio spreman da odustanem od svog istraživanja po *Ubuntu*.

Dan poslije sam se našao u situaciji da više ne mogu da podnesem izgled novog *Windows* sistema. Odlučio sam da malo istražim problem sa *Ubuntu*om samo da bih se riješio *Windowsa*. Jedan od prvih linkova na *Googlu* me je odveo na dio *Ubuntu* dokumentacije koji mi preporučuje da probam *boot-repair* paket koristeći *live* sliku. Kao i sve do sada što sam pokušao koristeći *Ubuntu*, i za izvršavanje *boot-repair* opcije mi je trebalo duže, nego što sam mislio da hoće. Nakon što se proces završio, *GRUB* je napokon radio i prikazivao mi je ispravno oba sistema.

Nakon mučenja sa instalacijom, za koje nisam mislio da će biti potrebno

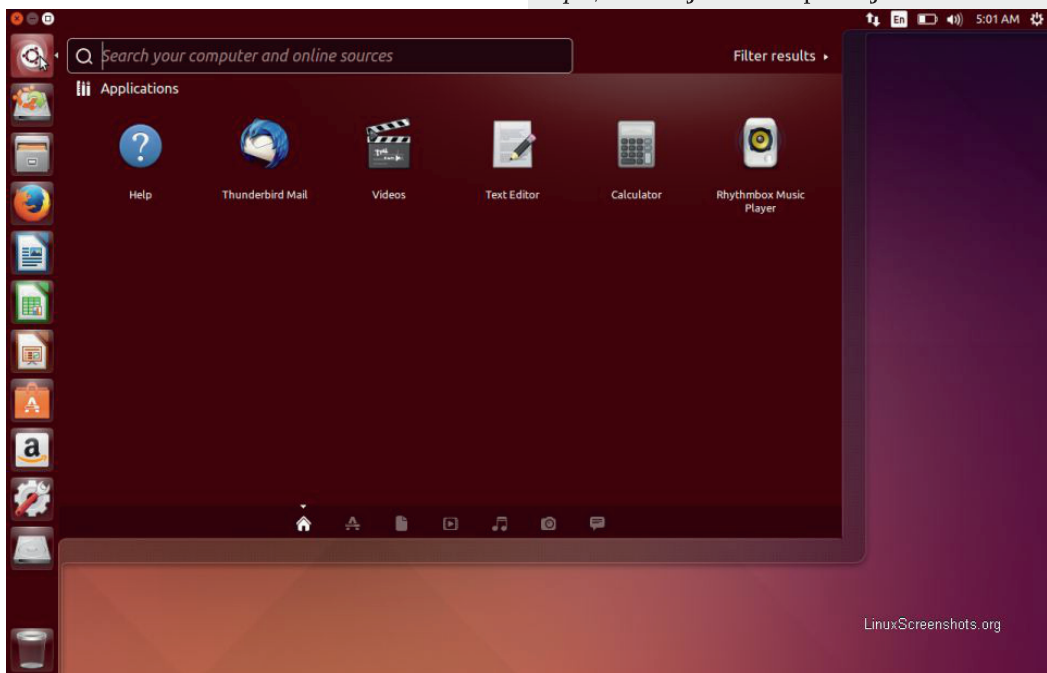




uzimajući u obzir da koristim najpoznatiju *Linuxovu* distribuciju, pokrećem *Ubuntu* sa svog hard diska. Sada je došlo na red istraživanje o tome kako sistem funkcioniše. Isprobavam *Unity* koji je doživio toliko negativnog publiciteta. Čini se brz za sada, međutim laptop ima problema sa pregrijavanjem. Nakon manje od minute istraživanja kako *Unity* radi, iskočio mi je prozor koji mi kaže da je dostupan *update* za neke od instaliranih paketa. Uzimajući u obzir da je prošlo manje od tri mjeseca kako je nova verzija *Ubuntu*a postala dostupna za javnost, pomislio sam da količina paketa za koje je dostupan *update* neće biti velika. Međutim, prevario sam se. Preuzimalo se preko *200MB* i instaliralo se pedesetak ažuriranih paketa. Proces je ponovo trajao nekih dvadesetak minuta i u tom

trenutku sam bio zahvalan što nisam uključio tu opciju prilikom instalacije sistema.

Prilikom samog ažuriranja sam postao svjestan da ova avantura uz ovakve probleme sa pregrijavanjem laptopa neće dobro da se završi. Da napomenem da laptop nema nikakvih problema sa pregrijavanjem koristeći novi *Windows*, a koristeći druge distribucije problemi postoje samo kada je sistem previše opterećen. Instalirao sam *tlp* i nakon njegovog pokretanja situacija se uveliko popravila. Imam običaj da isključim laptop sa punjača na nekoliko sekundi, samo da provjerim koliko bi laptop izdržao pod takvim opterećenjem na bateriji. Prije instaliranja *tlsa*, *Ubuntu* mi je pokazivao da bi baterija izdržala četrdeset minuta. Nakon pokretanja *tlsa*, to vrijeme se poboljšalo na sat i



LinuxScreenshots.org



deset minuta. To i dalje nije impresivno upoređujući sa dva i po sata koristeći *Windows* i dva sata koristeći *Arch Linux* sa *KDE* okruženjem, međutim može da prođe.

Što se tiče novih funkcija *Unity* okruženja, sada je moguće birati da li želite da aplikacijske kontrole prikazete u gornjem panelu ili u naslovnom panelu od aplikacije, moguće je smanjiti veličinu ikona na *launcheru*, softver centar se sada automatski prilagođava ukoliko proširite njegov prozor, a tu su i novi *wallpaperi* između kojih možete birati. Iako nove funkcije nisu drastične, sada korisnik ima više opcija za prilagođavanje *Unitya*, što svakako čini korištenje *Unity* okruženja prijatnijim. Ja moram da priznam da se nisam tako osjećao. Osjećao sam se kao da se borim sa sistemom da bih dobio ono što hoću: jednostavan i dobro dizajniran korisnički interfejs preko kojeg ću brzo i efikasno instalirati i koristiti druge programe.

Nakon što sam nekoliko dana dao priliku *Unity* interfejsu, shvatio sam da on jednostavno nije za mene. Iako mu ne mogu naći mnogo mana, mogu reći da sistem nije dobro „ispoliran” i da se javljaju neke greške (primjer: poruka o dostupnim *updatima* je u prozoru imala mogućnost da prikaže nazive paketa koji se ažuriraju, međutim nisu svi nazivi paketa bili vidljivi).

Pored klasičnog *Ubuntu*a sa *Unity* grafičkim interfejsom, stigle su nam i nove verzije službeno podržanih *Ubuntu*ovih derivata sa drugačijim korisničkim interfejsom:

- *Kubuntu - Ubuntu* sa *KDE* korisničkim interfejsom: <http://www.kubuntu.org/getkubuntu>
- *Ubuntu GNOME - Ubuntu* sa *GNOME* korisničkim interfejsom: <http://wiki.ubuntu.com/UbuntuGNOME/GetUbuntuGNOME>
- *Xubuntu - Ubuntu* sa *Xfce* korisničkim interfejsom: <http://xubuntu.org/getxubuntu>
- *Lubuntu - Ubuntu* sa *LXDE* korisničkim interfejsom: <http://help.ubuntu.com/community/Lubuntu/GetLubuntu>

Bilo mi je drago što sam napokon našao vremena da isprobam najpoznatiju *Linuxovu* distribuciju. Daleko od toga da me je oduševila i daleko od toga da ću je redovno koristiti. Moja potraga za distribucijom koju ću koristiti dok ne izađe nova verzija moje najdraže *Linuxove* distribucije se nastavlja.

Dodatni izvori

Autor: Željko Popivoda

Napomena: *LTS* izdanje ima podršku u trajanju od pet godina za *Ubuntu* i *Kubuntu*, odnosno tri godine za *Ubuntu GNOME*, *Xubuntu* i *Lubuntu*.

Ubuntu

Ubuntu kao podrazumevano okruženje radne površi koristi *Unity*.

Preporučujem da pogledate snimke ekrana: <http://www.linuxscreenshots.org/?release=Ubuntu%2014.04> i video pregled <http://youtu.be/YbXWljOxA9U>.



Predstavljamo

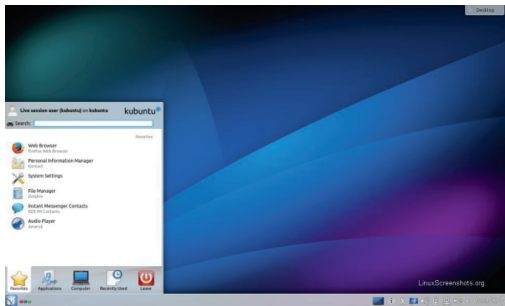


Ubuntu možete preuzeti sa:
<http://www.ubuntu.com/download>

Korisni linkovi:

1. <http://fridge.ubuntu.com/2014/04/17/ubuntu-14-04-trusty-tahr-released/>
2. <https://wiki.ubuntu.com/TrustyTahr/ReleaseNotes>

Kubuntu



Kubuntu - *Ubuntu* sa *KDE* okruženjem radne površi.

Preporučujem da pogledate snimke ekrana: <http://www.linuxscreenshots.org/?release=Kubuntu%2014.04> i video pregled <http://youtu.be/VNzZr4aFPVY>.

Kubuntu možete preuzeti sa:
<http://www.kubuntu.org/getkubuntu>

Korisni linkovi:

1. <http://www.kubuntu.org/news/kubuntu-14.04>
2. <https://wiki.ubuntu.com/TrustyTahr/ReleaseNotes/Kubuntu>

Ubuntu GNOME



Ubuntu GNOME - *Ubuntu* sa *GNOME* okruženjem radne površi.

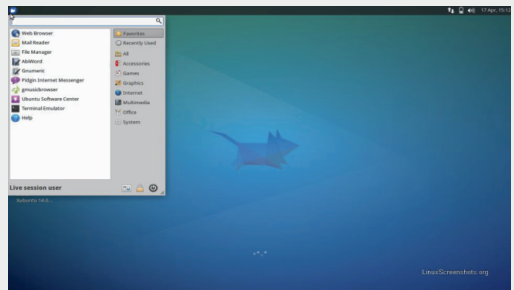
Preporučujem da pogledate snimke ekrana <http://www.linuxscreenshots.org/?release=Ubuntu%20GNOME%2014.04> i video pregled <http://youtu.be/dTNmAorlQBY>.

Ubuntu GNOME možete preuzeti sa:
<http://wiki.ubuntu.com/UbuntuGNOME/GnetUbuntuGNOME>.

Korisni linkovi:

1. <http://ubuntugnome.org/ubuntu-gnome-14-04-lts-is-released/>
2. <https://wiki.ubuntu.com/TrustyTahr/ReleaseNotes/UbuntuGNOME>

Xubuntu



Xubuntu - *Ubuntu* sa *Xfce* okruženjem radne površi.



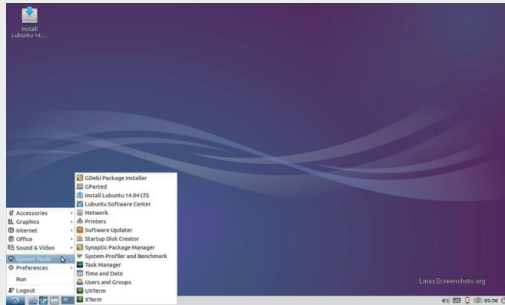
Preporučujem da pogledate snimke ekrana <http://www.linuxscreenshots.org/?release=Xubuntu%2014.04> i video pregled http://youtu.be/Dv26_2bjyY .

Xubuntu možete preuzeti sa: <http://xubuntu.org/getxubuntu> .

Korisni linkovi:

1. <http://xubuntu.org/news/14-04-release/>
2. <https://wiki.ubuntu.com/TrustyTahr/ReleaseNotes/Xubuntu>

Lubuntu



Lubuntu - *Ubuntu* sa *LXDE* okruženjem radne površi.

Preporučujem da pogledate snimke ekrana <http://www.linuxscreenshots.org/?release=Lubuntu%2014.04> i video pregled <http://youtu.be/fiwKz8zV240> .

Lubuntu možete preuzeti sa: <http://help.ubuntu.com/community/Lubuntu/GetLubuntu> .

Korisni linkovi:

1. <http://lubuntu.net/blog/lubuntu-1404-trusty-tahr-released>
2. <https://wiki.ubuntu.com/TrustyTahr/ReleaseNotes/Lubuntu>

Pregled popularnosti GNU/Linux /BSD distribucija za mesec jul

Distrowatch

1	Mint	2041<
2	Ubuntu	1685>
3	Debian	1483<
4	CentOS	1343>
5	Mageia	1162=
6	Zorin	1102>
7	openSUSE	1017=
8	Fedora	1001<
9	Arch	959>
10	Kali	776=
11	LXLE	729=
12	Deepin	724>
13	elementary	721<
14	Lubuntu	677>
15	Puppy	651<
16	Manjaro	650>
17	Tails	620>
18	HandyLinux	588>
19	Ultimate	566<
20	FreeBSD	552<
21	Salix	542>
22	Scientific	539>
23	Android-x86	513>
24	Bodhi	502>
25	SparkyLinux	495<

Pad <

Porast >

Isti rejting =

(Korišćeni podaci sa *Distrowatcha*)



libGDX

„Java game development framework”

(3. deo)





Autor: Gavriilo Prodanović

Svako bi od *frameworka* za razvoj Sigrica na više platformi očekivao dobru apstrakciju po pitanju ulaznih uređaja da bi ubrzao svoj proces razvijanja, a *LibGDX* se sa time može pohvaliti. Naš *framework* posjeduje dva osnovna načina za obradu ulaza: prvi je *pooling* gdje pozivanjem metode utvrđujemo stanje ulaznog uređaja (npr. da li je tipka na tastaturi spuštena ili čitanje pozicija miša), a drugi je hvatanje događaja (eng. *event handling*).

Preko *poolinga* možemo pristupiti uređajima uz pomoć nekoliko osnovnih metoda. Da li je *touch screen* dodirnut, možemo provjeriti pomoću `isTouched()` koja vraća `true` ako postoji dodir i `false` u suprotnom. Za *multitouch* možemo pozvati `isTouched(int index)`, gdje *index* označava koji prst želimo provjeriti. Da bismo dobili koordinate dodira, postoje `getX()` i `getY()` metode, a za *multitouch* u argument prosljedimo indeks našeg prsta/pokazivača. Na *desktopu* za manipulaciju mišem možemo koristiti gore prethodno navedene metode, a u tom slučaju ulaz sa miša će se tretirati kao *single-touch screen*. Za miš takođe postoje dodatne metode kao što su

`isButtonPressed(int button)`, `setCursorPosition(int x, int y)` i `setCursorCatched(boolean)` koja hvata kursor na sredinu ekrana i čini ga nevidljivim; i na kraju `setCursorImage` kojom možemo promijeniti dosadnu bijelu strelicu u nešto ljepše. Sve ove metode, osim `isButtonPressed`, dostupne su samo na *desktopu*, dok ova na mobilnim platformama dodir ekrana

registruje kao klik lijevog tastera miša. Tipke sa tastature i posebnu dugmad na mobilnim platformama možemo *poolingom* da hvatamo uz pomoć `isKeyPressed(int key)` metode, a *key* kodovi se nalaze u statičkoj klasi *Keys*.

Pooling može biti zgodan u nekim situacijama, ali mnogo praktičnije je koristiti hvatanje događaja. U *LibGDX*-u ćemo događaje hvatati tako što implementiramo interfejs *InputProcessor*, a onda instancu implementiranog interfejsa postavimo tako što ga prosljedimo

`Gdx.input.setInputProcessor(InputProcessor)` metodi. *InputProcessor* deklarira sledeće metode za implementaciju: - *touchDown*, *touchUp* i *touchDragged* - pomoću njih možemo registrovati kada je prst spušten ili dignut, ili da li ga pomjeramo po ekranu. - *keyDown*, *keyUp* i *keyTyped* - prve dvije metode prosljeđuju *keycode*, a *keyTyped* će se pozvati samo kada se generiše *unicode* printabilni karakter. - *mouseMoved* i *scrolled* se pozivaju samo na *desktop* platformi. Prva prosljeđuje *x* i *y* koordinate, dok druga prosljeđuje `-1` ili `1` u zavisnosti od smjera točkića na mišu kada se okrene.

Koristeći *touch* kao glavni ulazni uređaj za kontrolu igre, prirodan način pristupa je korišćenje nekih osnovnih gestova (eng. *gesture*) jednim prstom ili pomoću više njih. Kao primjer uzećemo uvećavanje pomoću dva prsta. Unutar *LibGDX*-a postoji klasa *GestureDetector* koja implementira *InputProcessor* interfejs i može da prepozna osam osnovnih gestova koji su definisani u *GestureListener* interfejsu. Za gestove

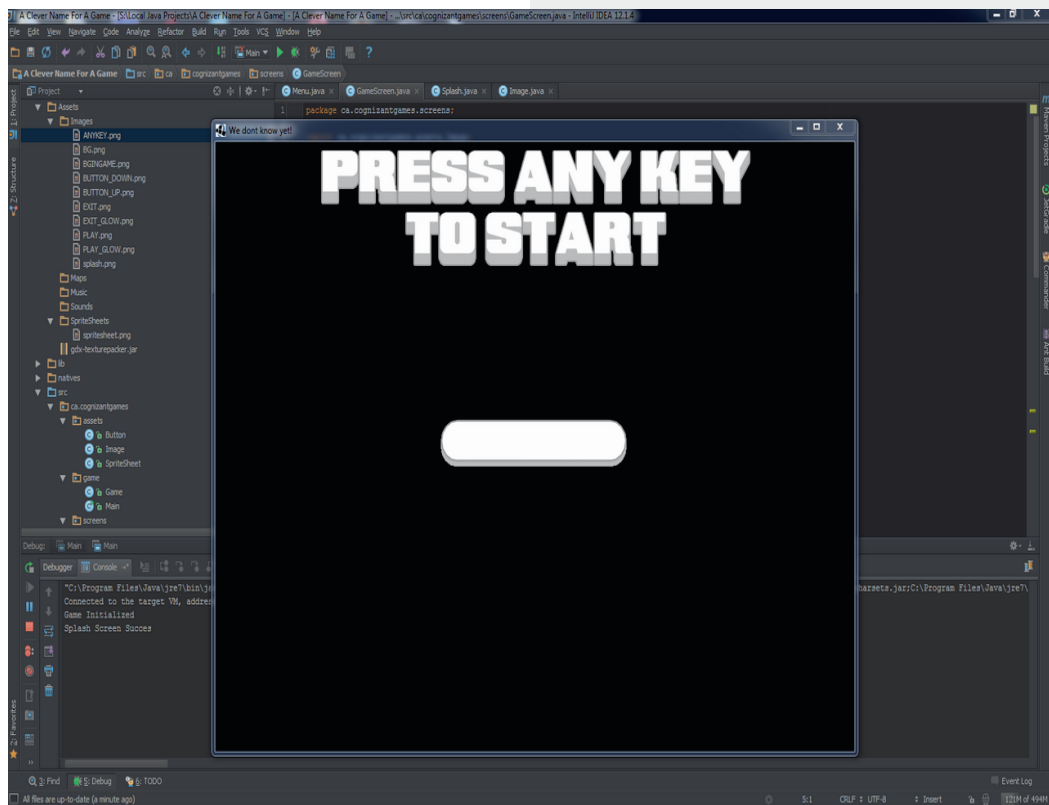


koji se mogu izvesti jednim prstom/pokazivačem na *desktop* platformi, *GestureDetector* će za ulaz da *wrapuje* miš.

Na mobilnim uređajima uglavnom su prisutni akcelerometar i kompas, a čitanje njihovih vrijednosti je moguće preko *poolinga* u našem *frameworku*. Jedini problem je što se sensorima može pristupiti samo preko *poolinga* i ne postoje *helper* klase koje bi nam pomogle u implementaciji kontrole na ovaj način. Uz akcelerometar i kompas možemo na mobilnim uređajima koristiti i vibracije da bismo prenijeli što bolji utisak igraču. Da bismo aktivirali

vibraciju, možemo metodi **Gdx.input.vibrate** proslijediti trajanje vibracije u milisekundama, ako želimo izvesti složenu vibraciju, možemo proslijediti cjelobrojni niz u kojem svaki neparni element označava dužinu trajanja vibracije u milisekundama, a svaki parni mirovanje u milisekundama. Drugi argument označava element od koga počinje ponavljanje u petlji ili **-1** ako želimo da se vibracija zaustavi na kraju niza. U slučaju da trenutnu vibraciju želimo prekinuti prije završetka, u tome će nam pomoći **cancelVibrate()**.

Ukoliko od igrača trebate zatražiti neki unos kao što su nadimak ili lozinka za





server, u tome vam može pomoći *TextInputListener* i metoda **Gdx.input.getTextInput** koja će izbaciti dijalog i pitati korisnika za unos. Izgled dijaloga zavisi od platforme, pa će na *Androidu* da bude uobičajen *Android* dijalog, a za *desktop* - *Swing* dijalog. Ukoliko odlučite pisati svoje kontrole za unos sa tastature, na *desktopu*, *iOS*-u i na *Android* uređajima sa fizičkom tastaturom će to biti lako izvodljivo. Za *Androide* koji nemaju fizičku tastaturu, može se koristiti *onScreen* tastatura, ali postoje bagovi koji neće htjeti prikazati tastaturu uopšte, ili određeni virtualni tasteri neće funkcionisati. Od tastatura poznato je da *stock android* ili *Googlova* tastatura odlično radi. Od bagovitih tastatura mogu se spomenuti *HTC* i *Samsungove* i mnoge još druge. Ovaj problem je prisutan i zna da zada glavobolju, ali da ne bude kao potpuno obeshrabljenje, reći ćemo da nije fatalan i postoje načini da se zaobiđe, kao što je na primjer dodatan *Activity* u *Android* projektu koji služi za skupljanje uobičajenih podataka.

Možda biste željeli na *desktopu* koristiti mogućnosti koje postoje na mobilnoj platformi kao što su *multitouch*, akcelerometar i kompas, da li zbog bržeg testiranja ili da biste stvorili neku vrstu hibridne platforme. U tome će vam pomoći klase *RemoteSender* i *RemoteInput*. *RemoteInput* implementira interfejs *Input* tako da sve gore što smo do sad naveli, jeste podržano. *RemoteInput* je

taj koji otvara ulaznu konekciju i čeka da se poveže neki *RemoteSender* koji implementira interfejs *InputProcessor* i u konstruktoru uzima *IP* adresu i port na koji treba da se poveže. Na *Play Storu* postoji *Gdx Remote* aplikacija koja vam može uštedjeti vrijeme.

Gejmeri imaju još jedan vid ulaza za računar, a to su džojstici ili *gamepadovi*. U *LibGDX*-u oni su podržani preko ekstenzije *gdx-controllers*. Može se koristiti *poolovanje*, ili se mogu registrovati *event listeneri*. Pošto ne postoji standard po pitanju mapiranja dugmadi na ovim uređajima, biće potrebno da korisnika provedete kroz konfiguraciju džojstika. Trenutno jedini mapirani kontroler je *Ouya* za koji ne morati provesti igrača kroz konfiguraciju. Ova ekstenzija može da se koristi i na *Android* uređajima koji pokreću najmanje 3.1 verziju ovog sistema.

Na kraju da rezimiramo ukratko: *LibGDX* posjeduje dobru apstrakciju i bogatu podršku za različite ulazne uređaje. Osim boga sa nekim *onScreen* tastaturama, možemo reći da smo u potpunosti zadovoljni kako je ulaz odrađen u ovom *frameworku*.





Uvod u programski jezik C

(4. deo)

Autor: Veljko Simić

Nizovi i matrice

U prošlom broju smo pričali o uslovnom grananju i kontroli toka programa. Naučili smo rad sa petljama, pa bismo ovaj tekst, u kome će biti reči o nizovima, počeli jednim pitanjem: kako ćemo napisati program koji računa prosečnu vrednost za deset vrednosti koje se unose? Pretpostavljamo da bi vaše rešenje imalo neku petlju koja bi se izvršavala deset puta i u njoj biste unosili vrednosti u neku promenljivu, nazovimo je zbir, sabirali biste te vrednosti i na kraju biste tu promenljivu podelili sa 10. Dobro, hajde da malo otežamo zadatak. Posle računanja proseka ispisati sve vrednosti koje su veće od njega! Tu nastaje problem: mi te vrednosti nismo zapamtili, već samo njihov zbir. Kada bismo pokušali da zadatak rešimo sa deset različitih promenljivih, zadatak bi bio poprilično ograničen i veoma teško bismo ga uopštili za, na primer, šesnaest vrednosti. Za ovakve, a i mnoge druge situacije, koriste se nizovi.

Niz je određen broj memorijskih lokacija koje imaju isti naziv. Pojedinačnim vrednostima se pristupa



pomoću njihovog indeksa (njihovog rednog broja u nizu) i sve vrednosti u nizu moraju biti istog tipa. Indeks niza u programskom jeziku C se piše u uglastim zagradama i, pošto sve počinje od 0, to važi i za numeraciju članova niza.

Opšta deklaracija niza izgleda ovako:

```
tip ime_niza[broj_članova];
```

Npr. ako nam treba niz koji ćemo nazvati Pera, od deset članova tipa *int*, deklarisaćemo ga ovako:

```
int pera[10];
```




Kad želite da peti član tog niza ima vrednost 42:

```
pera[4]=42;
```

Kao što vidite, sve počinje od 0, pa peti član niza ima indeks 4. Jedan od uobičajenih početničkih lapsusa jeste pristupanje članu koji ne postoji. U ovom slučaju bi bio član sa indeksom 10 – dakle `pera[10]` ne postoji, a ova greška se naziva *off by one*.

Možda mislite da određivanje broja članova niza pri deklaraciji ograničava nizove, ali, kao što smo rekli na početku, niz je skup memorijskih lokacija i računar mora znati koliko memorije treba da rezerviše. Postoji način dinamičkog dodeljivanja memorije nizu. To ćemo opisati u nekom od narednih tekstova. Ne moraju svi članovi niza biti iskorišćeni. Tako da, ako ste rezervisali deset mesta, možete da iskoristite deset, jedno, ali i nijedno.

U programskom jeziku C vrednosti elemenata niza nisu unapred deklarirane – dakle, u tim elementima se nalazi vrednost koja se nalazila na toj memorijskoj lokaciji, osim u slučaju kada je niz definisan kao globalna promenljiva. Tada svi članovi niza imaju vrednost 0.

Sada kada možemo reći da imate neko teorijsko znanje o nizovima, možemo uraditi zadatak s početka teksta.

```
#include <stdio.h> int main()
{
    int n, niz[100], zbir=0, i;
    //definišemo niz od 100
```



```
elemenata
    float prosek;
    printf ("Unesite duzinu
niza manju od 100");
    scanf ("%d",&n);
    for (i=0;i<n;i++)
// ovo je uobičajan način
unošenja niza
    scanf ("%d",&niz[i]);

    for (i=0;i<n;i++)
    zbir=zbir+niz[i];

    prosek=zbir/n;

    for (i=0;i<n;i++)
// pronalaženje i ispisivanje
svih elemenata niza većih od
proseka
    if (niz[i]>prosek)
        printf ("%d ",niz[i]);

    return 0;
}
```

Nizovi takođe mogu da budu više-dimenzionalni. Dvodimenzionalni nizovi se nazivaju matrice. Matrice imaju veliku ulogu pre svega u čuvanju i obradi tabelarnih podataka. Da biste dobro vladali matricama, potrebno je da imate iskustva sa višestrukim *for* petljama. Prolazak kroz matricu je šablonski postupak i svodi se na upotrebu dve ugnježdene petlje *for*, od kojih je spoljna za redove, a unutrašnja za kolone. Tako prolazimo kroz matricu red po red. Matrica se definiše slično kao niz, samo što ima dve uglaste zagrade koje označavanju indekse reda i kolone. Ako želimo da definišemo matricu 10×10 tipa *int*, to bi izgledalo ovako:



```
int matrica[10][10];
```

Sledi primer učitavanja i ispisa matrice:

```
#include <stdio.h> int main()
{
    int matrica[20][20],m,n,i,j;

    printf ("Unesite dimenzije
matrice manje od 20!");
    scanf ("%d%d",&m,&n);

    for (i=0;i<m;i++)
//unošenje matrice
        for (j=0;j<n;j++)
            scanf
("%d",&matrica[i][j]);
```

```
for (i=0;i<m;i++){ //ispis
matrice
    for (j=0;j<n;j++)
        printf ("%d
",matrica[i][j]);
        printf ("\n");
    }

    return 0;
}
```

Ovo je bio kratak uvod u diskusiju o nizovima i matricama. U sledećem broju ćemo pokazati neke nove tehnike sa ovim strukturama i neke nove stvari u C jeziku.





Uticaj matematike na nastank i temelje računarstva (3. deo)

Ograničenja, problemi i njihov značaj za kriptografiju

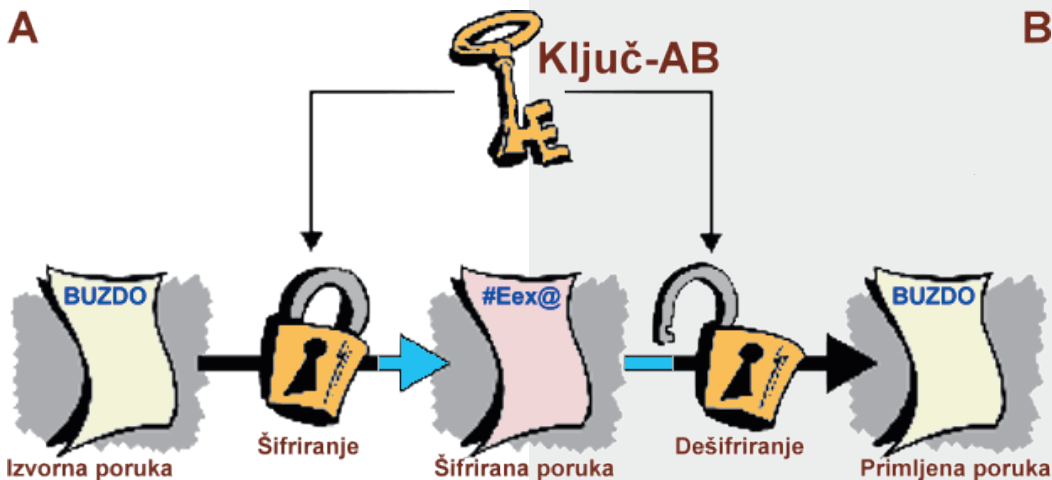
Autor: Nedeljko Stefanović

Među prve rezultate spadaju i rezultati o nemogućnosti rešavanja nekih problema algoritmom. Jedan od takvih rezultata je i problem zaustavljanja koji se sastoji u tome da za dati program na ulazu, koji sam ne zahteva nikakav ulaz, odredimo da li bi se taj program jednom pušten u rad završio u konačnom broju koraka.

Drugi srodan rezultat je da nije moguće napraviti programski jezik koji bi obuhvatio sve algoritme i čiji bi se svi programi zaustavljali u konačnom broju koraka. Da bi neki programski jezik obuhvatio sve algoritme (zaustavljive postupke), on mora da dopušta i konstrukcije kao što su beskonačne petlje, tj. konstrukcije koje mogu da rade, a da se nikada ne zaustave. Najveći broj programskih jezika je baš takav, a ima i sistema kod kojih se žrtvuje obuhvatanje svih algoritama zarad univerzalne zaustavljivosti. Primer je pomoćnik u dokazivanju teorema *Agda*.

Osim dokazivanja da neki problemi nisu algoritamski rešivi, izučava se i algoritamska složenost problema koji se mogu algoritamski rešiti. Složenost određenog algoritma za rešavanje nekog problema su resursi (vremenski ili memorijski ili i jedni i drugi) za njegovo izvršavanje, dok je složenost problema zapravo složenost najefikasnijeg mogućeg algoritma za njegovo rešavanje. Ponekad možemo znati da za neki zadatak imamo optimalan algoritam, ali to najčešće nije slučaj jer je to jako teško dokazati.

Ponekad je dobro što su neki problemi algoritamski jako teški jer ne želimo da budu rešeni. Takvi su problemi razbijanja kriptografskih primitiva čije bi rešavanje dovelo do zloupotreba. Bilo bi jako dobro da imamo kriptografske primitive za koje imamo dokaze da se ne mogu razbiti bez određenih izračunatih resursa koji prevazilaze snagu bilo kakvog hardvera koji se može proizvesti. Međutim, to nije slučaj, a isključivi razlog je što još uvek nije dostignut potreban stepen razvoja matematike. Za



sada se kriptografska bezbednost proverava empirijski, tako što se algoritmi objavljuju u naučnim časopisima, pa ako se za određen broj godina niko nije javio sa postupkom razbijanja, onda se algoritam smatra bezbednim. Svakako bi bolje bilo imati dokaz bezbednosti.

Kriptografske primitive treba svakako da budu efikasne za upotrebu na predviđen način, a što teže za razbijanje. Obično se kao zahtev za efikasnom upotrebom uzima da broj koraka bude ograničen polinomom po složenosti ulaza (ovde je to veličina ključa). Za takve probleme se kaže da pripadaju klasi složenosti P . Kao zahtev za teško rešavanje se obično uzima da broj koraka raste eksponencijalno u odnosu na složenost ulaza.

Sve primitive se mogu razbiti u polinomijalnom vremenu na mašinama sa neograničenim paralelizmom (npr. beskonačnim brojem procesora koji mogu paralelno da rade). Ako tražimo privatni ključ od 100 bitova kada je dat

javni ključ, mi zapravo treba da proverimo sve moguće nizove od 100 bitova, koji od njih čini privatni ključ koji se slaže sa datim javnim. Prvo možemo problem podeliti na dva slučaja – one kod kojih je prvi bit jednak 0 i one kod kojih je prvi bit jednak 1. Te slučajeve mogu da obrađuju dva procesora paralelno. Zatim, svaki od ta dva slučaja podelimo na dva podslučaja – kada je drugi bit jednak 0 i kada je drugi bit jednak 1. Te podslučajeve mogu paralelno da obrađuju četiri procesora. Tako ćemo u sto koraka cepanja svakog od podslučajeva na dva podslučaja u sto koraka uposliti procesore od kojih svaki obrađuje jedan niz od 100 bitova i svi rade paralelno. To omogućava da se na takvim mašinama taj problem reši efikasno. Slična ideja se može primeniti i na razbijanje simetričnih ključeva i kriptografskih heš (eng. *hash*) funkcija.

Za takve probleme se kaže da pripadaju klasi NP , koja iz navedenih razloga čini teorijski maksimum kriptografske



bezbednosti.

Za klase P i NP se još uvek ne zna da li su iste ili različite. Za rešenje tog problema je čak ponuđena nagrada od milion američkih dolara i on svakako predstavlja centralni nerešeni problem teorijskog računarstva. Ako su te klase jednake, s obzirom na to da problemi razbijanja uvek pripadaju klasi NP , oni u tom slučaju pripadaju i klasi P , što znači da je efikasno razbijanje moguće, pa bi primena kriptografije bila znatno ograničena i otežana. U suprotnom ostaje mogućnost da postoji problem koji je primenljiv na kriptografiju i ima potrebne osobine. Stoga je u svakom slučaju neophodno rešiti taj problem da bi se stiglo do primena u kriptografiji.

Mada je mašine sa neograničenim

paralelizmom nemoguće napraviti, one nužno učestvuju u formulacijama stavova relevantnih istraživanja, koja se sprovode jer je priroda problema takva. Drugačije nije moguće doći do rezultata jer je preduslov za neosporan dokaz nekog stava da stav po svojoj formulaciji bude tačan.

Čak i kada se to uspe, ostaje još jedan problem. Fizičari su otkrili drugačiji pristup izračunavanju tzv. kvantnim računarima, koji mada mogu da rešavaju potpuno iste probleme kao klasični (tj. ne dovode u pitanje Čerč-Tjuringovu tezu), neke probleme mogu da rešavaju i efikasnije, gde spadaju i problemi razbijanja nekih (ne svih) kriptografskih algoritama. Stoga treba dokazati otpornost i na napade kvantnim računarima (tzv. problem





postkvantne kriptografije), što je još teži zadatak.

Još jedna primena

Za kraj, pomenimo jedan pravac istraživanja koji objedinjuje formalizaciju matematike i formalizaciju pojma algoritma.

Programi se obično testiraju na konačnom broju primera. Mada se primeri pažljivo biraju tako da verovatnoća neispoljavanja greške ako postoji bude što manja, obično nešto promakne. Drugi put je formalna provera softvera, gde se željene osobine nekog programskog koda dokazuju kao teoreme. Međutim, pošto su ljudi podložni greškama, dokaze treba da proveri mašina.

U tom pogledu, najpre imamo proveravače dokaza kojima mora celokupan dokaz biti dat na ulazu. S obzirom na to da je ljudima naporno da unose baš svaki korak dokaza, drugi pristup su dokazivači teorema koji automatski dokazuju zadatu teoremu. Međutim, pošto se ispostavilo da je taj cilj za većinu matematičkih teorija čak nedostižan, zlatna sredina su pomoćnici u dokazivanju koji takođe zahtevaju dokaz na ulazu, ali ne svaki korak, jer imaju „ograničenu pamet“, tako da čovek ne mora da unosi baš svaki korak, već samo ono za šta mašina kaže da joj je ostalo „nejasno“.

Vodeći takvi programi su *Isabelle*, *Coq* i *Agda*, pri čemu su svi oni akademski projekti dostupni kao slobodan softver otvorenog koda. To je u ovom slučaju čak neophodno, jer je provera isprav-

nosti programa koji proverava dokaz, sastavni deo naučne provere dokaza koje ti programi proveravaju. Stoga je taj model uobičajen za akademske projekte, jer u suprotnom ne bi bilo moguće naučno pozivanje na rezultate koji se njima dobijaju.



Loša vest je da takav pristup, mada eliminiše greške u izvornom kodu u celini (a pristup je primenljiv i na druge softverske komponente, kao i na hardver), zahteva mnogo kvalifikovaniju radnu snagu od klasične i samim tim je daleko skuplji, pa se za sada primenjuje samo za namene visokog rizika, gde može doći do gubitka ljudskih života, narušavanja ljudskog zdravlja ili velike materijalne štete.

Ipak, verujemo da taj pristup ima širu budućnost (mada ne tako skoro). Svaki programski jezik omogućava izradu softvera do neke složenosti, kada ljudi počinju da prave više novih grešaka, nego što ispravljaju stare. Sa ovim pristupom nema granica u složenosti, tako da postepeno mogu da budu pravljenе složene komponente koje će da koriste i ostali koji razvijaju softver.

Demokratija zahteva slobodan softver

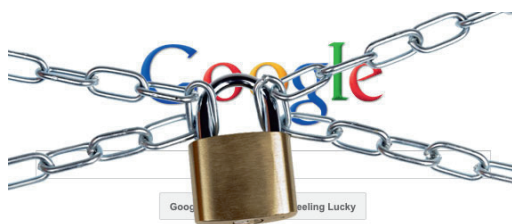
Autor: Matijas Kiršner

Preveo i adaptirao: Dejan Maglov

Tehnologija je kroz istoriju uticala na društvo. Čitanje, pisanje, aritmetika, poljoprivreda, štampa i radio su primeri izuma koji su promenili naš način shvatanja trgovine, umetnosti i nauke. Softver je sa kulturološkog stajališta najvažnija tehnologija 21. veka. *Free Software Foundation Europe* (FSF Europe) obavezala se da obezbedi ljudima u našem društvu pravo da oblikuju ovu tehnologiju po svojim potrebama.

Danas je nemoguće zamisliti svakodnevni život bez softvera. Većina nas ne može da provede nijedan dan bez korišćenja softvera. Ljudi koriste softver na radnom mestu (radna stanica), na laptopu i na mobilnim telefonima. Softver se takođe nalazi i na manje očiglednim mestima kao što su vozovi, automobili, televizori, veš-mašine, frižideri, i mnogi drugi uređaji. Većina od ovih uređaja ne može da funkcioniše bez softvera. Bez softvera ne bismo mogli pisati pisma, telefonirati, ići u kupovinu ili putovati kao što smo navikli. Softver je centralni instrument našeg društva. Kada drugi kontrolišu alat tako važan za nas kao što je softver,

oni mogu da izvrše veliki uticaj na naše akcije. Ko kontrolišu pretraživač, koji mi koristimo, određuje šta ćemo pronaći. Onaj ko kontrolišu našu elektronsku poštu, ima priliku da nas cenzuriše. Jednostavno rečeno, kontrola komunikacionog servisa podrazumeva sposobnost odlučivanja ko može da razmenjuje, šta i sa kim. Slično, onaj koji odlučuje kako softver funkcioniše, ima veliki uticaj na to kako živimo i šta radimo.



U modernim demokratijama moć je odvojena. Mi delimo vlast na zakonodavnu, izvršnu i sudsku vlast i svaka ima svoju posebnu instituciju. Osim toga mi delimo odgovornost na nekoliko nivoa nadležnosti, odnosno na centralnu vladu, regionalne vlade i lokalne samouprave. Ključna funkcija slobode štampe je da nas štiti od formiranja informativnog monopola, gde bi previše moći bilo koncentrisano u rukama manjine. Ključna korist efikasne demo-



kratije je da možete dati bilo kakvu funkciju unutar demokratskog sistema i vašem najvećem političkom protivniku. (Poslednja rečenica je ključna za shvatanje savremene demokratije. Ovo je ideal koji su dostigle sve najveće kapitalističke demokratije. Ideal je stvoriti privid demokratije kod kojeg izgleda da narod bira svoju vlast, a u stvari, ko god je na vlasti, ništa se ne menja, barem ništa ključno. To nije problem ako postoji konsenzus oko nacionalnih interesa koje niko ne sme da ugrozi, ali u svim ostalim slučajevima ovakva demokratija može da stvori samo problem. - prim. prev.)

Veoma je opasno za demokratiju da softver, kritični društveni instrument, bude pod kontrolom male grupe moćnika. (Ovde je ključ softver, ali to isto važi i za energiju, ključne sirovine, hranu i lekove. To su ključni centri moći u današnjoj demokratiji a ne političari. - prim. prev.) Ne samo da naša komunikacija zavisi od softvera, već zavisi i veliki deo infrastrukture društva. *FSF Europe* želi da zastupa interese korisnika računara, a da se izbori da u budućnosti kontrolu nad softverom imaju svi. Društvo ne sme sebi da priušti da bude zavisno od privatnih interesa kada je u pitanju alat tako važan kao što je softver.

Naše društvo mora da obezbedi da svako ima priliku da oblikuje softver po svojoj meri. To pretpostavlja da imamo slobodu da koristimo softver za bilo koju svrhu, da proučavamo kako softver radi, da ga delimo sa drugima, i sami poboljšavamo.

- **Pravo na korišćenje:** Predstavlja slobodu upotrebe softvera za bilo koju svrhu bez ograničenja (na primer zabrane korišćenja u komercijalne ili poslovne svrhe). To obezbeđuje mogućnost pojedincu da doprinosi zajednici.
- **Pravo na proučavanje:** To je pravo na slobodu proučavanja kako softver funkcioniše, odnosno izvorni kod, što predstavlja srž za razumevanje rada računara.
- **Pravo na deljenje:** Sloboda deljenja softvera omogućuje da možemo pomoći drugima tako što bismo najbolji softver delili sa njima.
- **Pravo na unapređenje:** Na kraju, društvo mora imati slobodu da modifikuje softver, menja ga u svrhu unapređenja i prilagođavanja ličnim potrebama.

Softver koji poštuje ove četiri slobode, jeste slobodan softver.

Demokratskom društvu su potrebni čvrsti temelji. Jedna od tih fundamenata je slobodan softver.

Literatura:

<https://fsfe.org/freesoftware/society/demo-cracry.en.html>





Pure



Autor: Zlatan Vasović

CSS je uvek bio interesantan jezik za *framework*, jer *web* dizajnerima treba nekakav set stilova koji će im olakšati posao pri izradi *web* sajtova. U moru CSS *frameworka*, na vrh su se istakli *Bootstrap* [1] i *Foundation* [2]. Ipak, *framework* su uglavnom veliki, sa previše elemenata. Iz tog razloga se pojavila nova ideja — minimalistički *framework*.

Yahoo web development tim je rešio da

napravi *framework* i za svoje, i za potrebe drugih, koji sadrži samo osnovne elemente. Rezultat toga je *Pure* [3], sada već popularni minimalistički *framework*.

Osvrt

Pure sadrži samo osnovne elemente — tipografiju, *grid*, forme, dugmiće (engl. *buttons*), tabele i menije.

Kompresovan i „gzipovan“, *Pure* „teži“ samo 4.4kB.

The screenshot shows the Pure CSS website interface. On the left is a dark navigation menu with items: PURE, Get Started, Layouts, Base, Grids, Forms, Buttons, Tables, Menus, Tools, Customize, Extend, Blog, Releases, Skin Builder, and YUI Library. The main content area features the 'Pure' logo, the text 'A set of small, responsive CSS modules that you can use in every web project.', a code snippet for linking the stylesheet, two buttons ('Get Started' and 'View on GitHub'), and a horizontal bar listing modules and their sizes: Base (1.2KB), Grids (0.8KB), Forms (1.4KB), Buttons (0.8KB), Tables (0.5KB), and Menus (1.2KB). At the bottom, it says 'CSS with a minimal footprint.'



Upotreba

Pure se može direktno učitati sa *weba* preko brzog *YUI API*-ja. Potrebno je dodati sledeći kod u `<head>` *HTML* stranice:

```
<link rel="stylesheet"
href="http://yui.yahooapis.com/
pure/0.5.0/pure-min.css">
```

Zbog male veličine datoteke, ne bi trebalo da utiče na učitavanje stranice.

Može se i direktno preuzeti sa linka [4].

Uređivanje

Framework je osmišljen tako da se lako može urediti, kako od strane dizajnera, tako i od strane programera. Za dizajnere tu je „*Skin Builder*” [5], a za programere izvorni kod u *GitHub* repozitorijumu [6].

Skin Builderom možete menjati boju pozadine, teksta, radijus i slično, kako biste prilagodili *Pure* svojim potrebama.

Ako vam je potrebna bilo kakva dodatna pomoć, pročitajte <http://purecss.io/start/>.

Skin Builder An App for Generating Custom Skin CSS Documentation File an issue

Style Schemes Items Code Preview color palette details

Edit Master Color... Edit Page Color...

Horiz. padding: 100% Reset Vert. padding: 100% Reset

Border-radius: 100% Reset

Text Contrast: 150 Reset

Sample

Forms - Checkboxes and Radios

Checkbox option

Radio button choice

Radio other choice

Default Inline Form

Legend

Email Password Opt in Sign in

Aligned Form

Username

Username

Password

Password

Email Address

Email Address

Disabled

Disabled input here...

Check me out

Submit

Form - Stacked

Legend

Full Name

Block help text

E-Mail

Required State

AL

I've read the terms and conditions

Submit

Form - Grouped Inputs

Username

Password

Email

Another Group

More Stuff

Sign in

Rounded Form

Search

Buttons

Start

Tables - Default

#	Make	Model	Year
1	Dodge	Ram 1500	2010
2	Honda	Accord	2000

Skin Preview

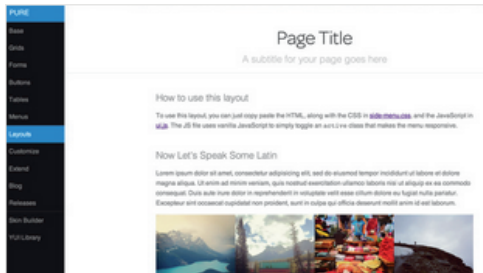
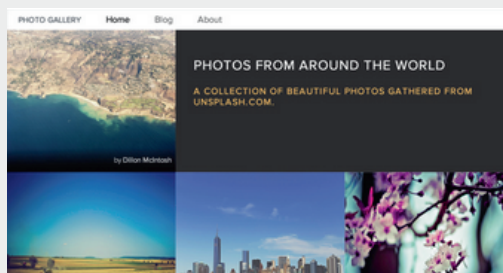
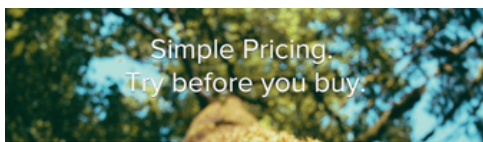
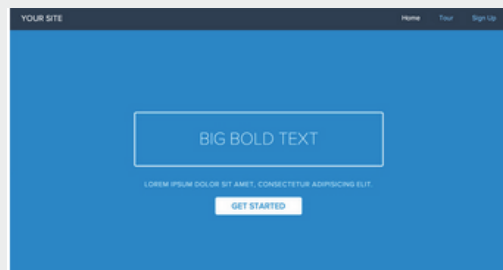
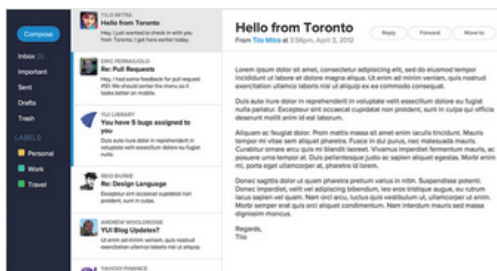
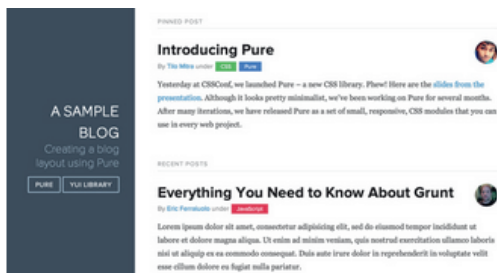


Zaključak

Pure je veoma koristan framework za one koji počinju da rade sa CSS-om, ali i za one koji ne žele da troše vreme na pravljenje celog frameworka od nule. Zasluzuje našu preporuku (prim.aut.).

Linkovi

- [1] <http://getbootstrap.com>
- [2] <http://foundation.zurb.com>
- [3] <http://purecss.io>
- [4] <http://yui.yahooapis.com/pure/0.5.0/pure-min.css>
- [5] <http://yui.github.io/skinbuilder/?mode=pure>
- [6] <https://github.com/yui/pure/>





Enkriptovana elektronska pošta

(2. deo)

Autor: Petar Simović

Pošto smo se u prošlom delu ukratko upoznali sa ovakvim vidom enkripcije, sada ćemo malo detaljnije proći kroz proces instalacije i korišćenja enkripcije za šifrovanje i sigurnosnu razmenu elektronske pošte. Pre nego što nastavimo, napomenućemo nekoliko stvari. Prva stvar je verovatno banalna čitaocima prethodnog dela, a odnosi se na generisanje ključeva. Naime, pre nekoliko nedelja objavljen je tekst (<http://goo.gl/7yxTfa>) u kome *Snowden* govori kako enkripcija funkcioniše i kako doskočiti Američkoj bezbednosnoj agenciji šifrujući svoju elektronsku poštu koristeći *PGP*, što je u redu, ali se takođe sugeriše da se koristi besplatni *on-line* program (*iGolder*: <http://goo.gl/SvQivp>) za generisanje ključeva (i privatnog i javnog), što gospodin *Snowden* nikada nije naveo. Naravno, ovo nije prvi put da se situacija globalnog nadzora, neupućenost korisnika i izjave *Snowdena* koriste za navođenje korisnika na pogrešan put, pa ovom prilikom skrećemo pažnju da se ključevi moraju generisati na vašoj

mašini i da se mora čuvati privatni ključ. Druga stvar je da se ne oslanjate previše na *on-line* usluge kada su u pitanju privatnost i sigurnost podataka. Tako se, na primer, sajt jedne od novijih *on-line* aplikacija (*Intactmail*: <http://goo.gl/Z4n8pW>) za šifrovanje elektronske pošte već gasi, iako nije prošlo ni pola godine otkako se o njoj počelo pisati (<http://goo.gl/YKXo7l>), tako da je najsigurniji štreberski način „sve preko terminala”, ili za početnike preko nekih dodataka za *desktop* aplikacije poput *Thunderbirda*.

Sada možemo da pređemo na instalaciju. Biće vam potrebni sledeći programi:

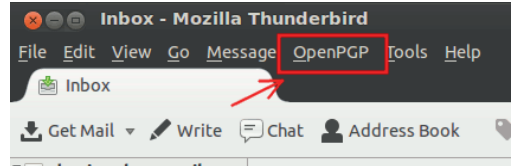
- *GnuPG*, koji je na većini današnjih *Linux* distribucija već uključen u samu instalaciju operativnog sistema tako da je velika verovatnoća da ga već imate instaliranog, što možete proveriti u terminalu sledećom komandom:

```
gpg --version
```

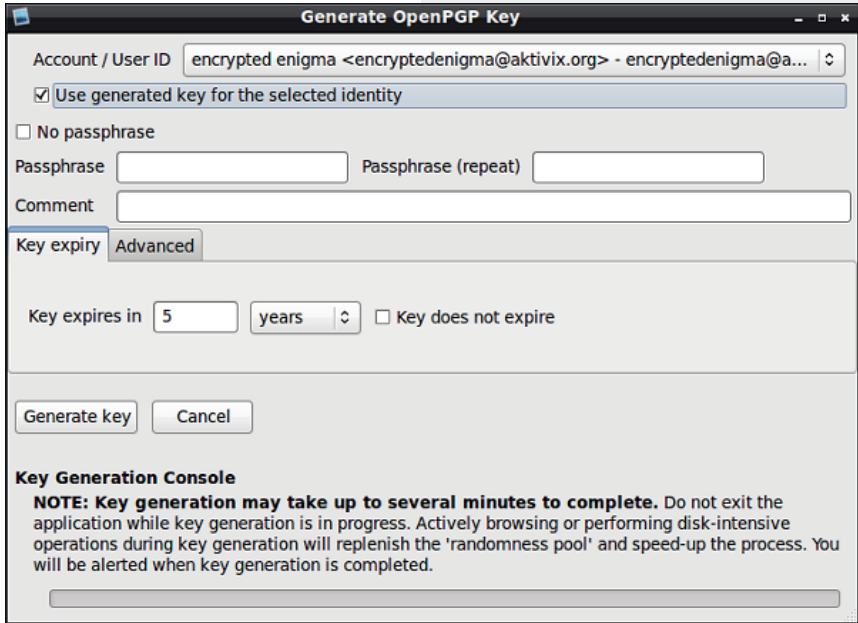
- *Thunderbird* (<http://goo.gl/RLdzIR>) – nije obavezno da to bude ovaj program, pa tako možete koristiti *Claws Mail* koji redovno ide uz *Tails* ili *Icedove*, ili neki drugi *open-source* program. Prethodno proverite koje sigurnosne dodatke za enkripciju podržava.
- *Enigmail* (<http://goo.gl/J3sztY>) ekstenzija za *Thunderbird* ali i za druge programe poput *Icedova*, koju možete instalirati iz *Thunderbirda* (*Tools* » *Add-ons*», pa tražiti „*Enigmail*”).

Nakon što ste instalirali potrebne aplikacije, napravite nalog elektronske pošte, ili unesite već postojeći (*Create new account* » *Email*), i nakon što popunite tražena polja o adresi elektronske pošte i šifru koja joj odgovara, možete pritisnuti *Read messages*. Biće učitana sva vaša pošta sa servera tog naloga elektronske pošte. Potom je potrebno da napravite par ključeva koji ćete koristiti za šifrovanje uz taj nalog. Ukoliko koristite više naloga, za svaki će vam biti potrebni posebni ključevi, ali polako: kada napravite prvi i počnete da ga koristite, dodavanje novih naloga i generisanje ključeva za isti neće biti problem.

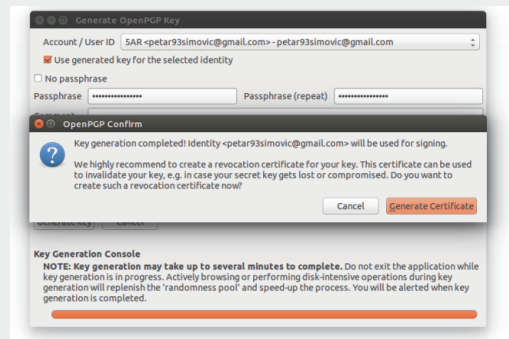
Sada je potrebno da generišete prvi par ključeva što ćete uraditi iz *Thunderbirda*, gde bi trebalo da imate opciju *OpenPGP*. U njenom padajućem meniju odaberite *Key Management*. Otvoriće vam se novi prozor i u njegovim opcijama u vrhu prozora potražite opciju *Generate*, pa onda *New Key Pair*.



Pre nego što pritisnete *Generate*, morate popuniti polja za sigurnosnu frazu (*Passphrase*), koja predstavlja lozinku za pristup vašem privatnom ključu za određeni nalog elektronske pošte, i proveriti da li je prikazani nalog elektronske pošte onaj za koji generišete ključeve (polje *Account* » *User ID*). Sigurnosnu frazu treba da negde sačuvate ili zapišete jer će vam često biti potrebna. Takođe, svaki nalog će imati svoju nezavisnu frazu kao i enkripcione ključeve. Ukoliko sada pritisnete *Generate*, računar će početi da generiše 2048-bitne *RSA* ključeve, što je zadovoljavajuća dužina ključeva koji će isteći za pet godina. Najbolje je da ove opcije sve ostavite kakve su podrazumevane, ukoliko ste početnik, dok naprednije korisnike ohrabrujemo da povećaju dužinu ključeva na 4096-bitova i da vreme isteka smanje na dve godine. Još samo jedna napomena pre nego što pritisnete *Generate* dugme i računar sve uradi za vas: pročitajte belešku masnim slovima ispod *Generate* dugmeta i pripremite se da aktivno surfujete netom, otvarajte sve aplikacije koje vam padnu na pamet, pustite neki video i muziku, kako bi računar imao visok stepen entropije o kojoj smo pričali u prošlom delu i pripremite neku eksternu memoriju za skladištenje poverljivih podataka nakon generisanja ključeva, u vidu *USB* memorije ili *CD-a*.



Po završetku kreiranja ključeva pokažeće vam se poruka koja preporučuje da kreirate i sertifikat u slučaju da izgubite ključeve, ili ih neko sazna. Obavezno prihvatite i sačuvajte sertifikat! Pošto već ima dosta fajlova koje treba da čuvate u vezi sa enkripcijom vaše pošte, predlažemo vam da ih uredno sačuvate u neki prazan direktorijum posebno za ove namene koji ćete posle presnimiti na *USB* ili *CD* (za dodatne mere opreza možete direktorijum šifrovati, pa ga tek onda presnimiti).



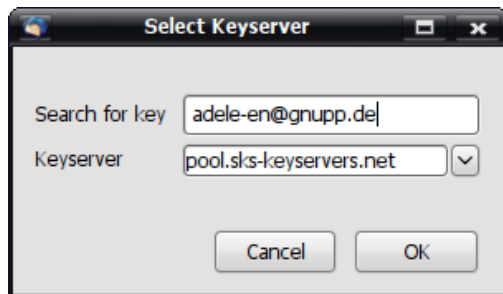
Sada bi u otvorenom prozoru *OpenPGP Key Managementa* trebalo da vam se pojavi novi podatak sa vašim mejlom, što je ustvari vaš par ključeva. Možete primetiti da on ima i svoj *Key ID* koga bi trebalo, takođe, da zapišete ili sačuvate negde. Nemojte zatvarati ovaj prozor jer vam treba za sledeći korak. Sledeća stvar je takođe važna i odnosi se na objavljivanje vašeg javnog ključa na

jedan od servera javnih ključeva. Ovo je veoma korisno jer ne morate porukama razmenjivati ključeve ako ste ih oboje objavili na server javnih ključeva, nego je potrebno da samo pretražite server o podacima za imejl čiji javni ključ želite. Ovo možete uraditi tako što ćete u otvorenom prozoru *OpenPGP KEY MANAGEMENT* pritisnuti desni klik miša na ključeve koje ste upravo kreirali i odabrati opciju *UPLOAD PUBLIC KEYS TO KEYSERVER*. Ostavite *keyserver* da bude podrazumevani „*pool.sks-keyservers.net*” i pritisnite *OK*!



Pred kraj, da biste se uverili da ovo zaista radi, možete poslati enkriptovanu ili digitalno potpisanu poruku automatskom *OpenPGP* robotu *Adele*, koji će odmah na nju odgovoriti. Prvo izaberite iz *Thunderbirda* opciju *OpenPGP*, pa *Key Management*, pa onda iz njegovih opcija *Keyserver*, zatim *Search for Keys* i tu unesite imejl adresu *Adele* robota: *adele-en@gnupp.de* na serveru javnih ključeva. Vaš javni ključ možete poslati primaocu i kao *Attachment* (*OPENPGP* » *KEY MANAGEMENT* » desni klik na vaš mejl sa koga šaljete » *SEND PUBLIC KEYS BY EMAIL*) što će otvoriti novu poruku i uključiti u

Attachment vaš javni ključ. Ukoliko ste već svoj ključ objavili na server javnih ključeva, nije potrebno da ga šaljete porukom, već samo recite primaocu da ga potraži na serveru.



Nakon toga će njena adresa biti u meniju *Key Managementa* iz koga treba da desnim dugmetom miša kliknete na njenu adresu i da izaberete opciju *Sign key*, podesite nivo poverenja i unesete vašu sigurnosnu frazu koju ste, nadamo se, sačuvali. Ukoliko niste sačuvali sigurnosnu frazu, moraćete da pravite nove ključeve i stare da obrišete, pa sve iz početka.

Ovo je osnova koja vam je potrebna da biste svoju elektronsku poštu osigurali šifrovanjem. Naravno, pošto je ovo elektronska pošta i potrebno je dvoje da bi funkcionisala, morate poštovati slobodu onoga sa druge strane ako ne želi da šifruje svoju poštu, i zato je potrebno da se najpre probudi svest među ljudima o kriptografiji, pa će je početi češće koristiti.



Korak do Googla (6. deo)

Autor: Dejan Čugalj

Toliko toga je rečeno, urađeno, napisano, i na kraju objašnjeno u *Lucene* serijalu. Za kraj ostaje famozni **Indeks** koji je srž *Lucene*.

Taj **Indeks**, koji nije običan *Index*, sve više sagledavajući *Lucene*, vidimo da je to ono što čini *FLOSS* zajednicu (prim.aut.). **Indeks** nam daje opštu predstavu da *Google* nije jedini i univerzalni šablon po kom bi trebalo da se vodimo. Kao primer moramo navesti incident koji se desio u *Kini* i koji bi trebalo da predstavi klasično izbegavanje monopolizma, kako u ekonomskim naukama, tako i u *IT* sferi.

krucijalnog dela internet korišćenja, a to je pretraga (prim.aut.). Rezultat ovog monopolističkog ponašanja *Googla* je izrodio *Baidu*, jedinstveni pretraživač korišćen samo u *Kini*, a nama daje za primer upotrebu *Lucene* familije jedinstvenog principa, algoritama, koji smo do sada ukratko, koliko je to moguće, „pretrčali” u *Java* programskom jeziku.

Iako bi ovde trebalo da široko razmatramo **Indeks**, taj pojam o kom govorimo skoro sedam meseci, pokušaćemo da ga svedemo na neko teorijsko razmatranje opšte-zatečenog stanja globalnog *IT*-a. Zašto spominjemo ovo, zašto je to toliko bitno u ovako „razrađenom” i „usklađenom”, skoro pa bismo rekli i standardizovanom svetu internet tehnologija? Ono što čini internet, upravo je ta **sloboda**, *FLOSS* zajednica, deljenje opšte stečenog znanja i težnja ka poboljšanju, okosnica mladih naučnika koji streme ostvarivanju cilja naukom, a u svrhu poboljšanja sveopšteg. Tako je i rođen *GNU/Linux*(prim.aut.).



Jednostavnom odlukom tako moćne kompanije kao što je *Google*, skoro trećina čovečanstva je ostala bez



Neverovatno zalaganje, samopožrtvovanje *Richarda Matthew Stallmana*, ostavilo je *open-source* licencu - GNU General Public License kao zaveštanje pionirskog koraka kojim smo se približili upravo tim *Lucene* **Indeksom**. Kako bismo objasnili taj isti **Indeks**, moramo da se vratimo na početak serijala i da opet spomenemo da je *Lucene* upravo proizišao iz *Googla*, tj. jednog od „radnika” koji je radio u *Googlovom* razvojnom timu.



Nekako ostajemo zatečeni činjenicom da se sve svodi na pojedince, individue, da su najveća otkrića vezana usko, široko, za te briljantne umove, koji sklapajući sve kockice u celinu, daju nama, običnim ljudima, mogućnost da se nekako odvojimo od globalističko-monopolističke osnove i da počnemo da razmišljamo svojom glavom (prim.aut.).

Ono što čini taj famozni *Lucene* **Indeks** specijalnim, nije više u sferi programiranja, algoritma, već predstavlja okosnicu, prvu liniju fronta borbe kojom bi trebalo svi da se vodimo, ali kako naši čitaoci prate **LiBRE!** časopis, i samim tim što čitaju kraj serijala o *Lucene*, mislimo da smo korak bliže pobeđi (prim.aut.).

LiBRE! prijatelji

LUTHERUS

Et in Arcadia ego!



ICT časopis

ictcasopis.ict.edu.rs



LOVĆENAC
LINUX USER GROUP



Grupa korisnika GNU/Linux operativnih sistema u Lovćencu

info i tutorijali na srpskom
lubunturs.wordpress.com





BalCCon (<https://balccon.org>) organizuje zajednica i svaka pomoć nam je dobrodošla.

Kongres ne bi bilo moguće organizovati bez ljudi koji će volontirati na njemu i pomoći nam da se BalCCon održi.

BalCCon se oslanja na vašu pomoć. Molimo vas da razmislite o volontiranju na BalCCon2k14 - Second Base! Možete se prijaviti slanjem e-maila, na [jelena \[at\] balccon \[dot\] org](mailto:jelena@balccon.org).

E-mail naslov: Volonter BalCCon2k14

Pošaljite:

Ime i prezime (nadimak):

Zemlja:

E-mail:

Broj mobilnog:

Veličina majce:

Nešto o sebi: (do 1000 reči)

Bitno je samo da volonteri žele da nešto novo nauče i da pomognu. Sve potrebne informacije volonteri će dobiti na licu mesta, a u toku kongresa će imati podršku koordinатора volontera.

Rok za prijavu je 25.08.2014.

Hvala vam što ste odlučili da se prijavite za volontiranje na BalCCon2k14.