Јул 2014.

ЛиБРЕ!

Часопис о слободном софтверу

број 27

22. јул, 2014.

Објављена је нова верзија *Kali Linux*-а

27. јул, 2014.

Тулуз уштедео милион евра преласком на *LibreOffice* .

Реч уредника

Часопис или блог? Поново?!

Ову дилему смо решили већ у првом броју часописа. Зашто се опет враћамо на ову тему? Да вас одмах разуверимо, уопште немамо дилему да ли ће и даље ЛиБРЕ! бити часопис. ЛиБРЕ! часопис, макар док је ова екипа на челу пројекта, задржаће форму часописа. Постоји сада друга дилема, да ли чланци који су примерени неком блогу, могу бити објављени у часопису?

Часопис има стриктна правила по питању форме и озбиљности чланака које објављује. То подразумева писање у трећем лицу једнине и у првом лицу множине, затим подразумева проверу објављених информација. Оне морају да буду тачне и да буду очишћене од субјективних утисака. Замка овакве форме чланака, нарочито при представљању неког пројекта, јесте монотонија и такви чланци могу да личе на преписивање техничке документације пројекта. Нарочито постају досадне рецензије великих дистрибуција које се у мање-више сличној форми понављају на сваких шест месеци.

Блог је много слободнији по питању форме писања. Има својих мана у виду уношења превише субјективних утисака, информације не морају бити сто посто тачне јер су плод првог утиска и можда су у комбинацији са неком грешком коју је блогер направио па није добио резултат који је по документацији пројекта требало да добије. Ако о укусима не треба расправљати (укус је потпуно индивидуална ствар) и информације нису сто посто тачне, да ли је онда такав текст за часопис?

Решавање ове дилеме кренули смо од корисности и занимљивости блогерског текста. Чињеница је да сваки блог пати од дозе субјективизма и дела дезинформације које су плод недовољног проверавања информација, па ипак многи блогови су врло популарни баш зато што нису сувопарни. Да ли су и корисни? Мислимо да јесу. Објективне информације о пројекту читалац, који их тражи, може да нађе на више места (нарочито у документацији пројекта), а субјективне утиске и евентуалне проблеме може да прочита само у нечијем блогу. Проблем можда постоји, а можда је и производ грешке блогера. Без обзира да ли је грешка у пројекту, или је грешка блогера, велика је шанса да се понови и неком другом. Добар блогер ће дати и решење тог проблема, тако да корист за читаоца свакако постоји.

Овакав приступ отвара зелено светло блогерским текстовима у часопису. Ипак ЛиБРЕ! не сме да подлегне и постане терен за искључиво блог-

ерске текстове. Озбиљност и проверена информације мора да остане императив нашег часописа. Зато ћемо само одшкринути врата за блогерске текстове ексклузивно у подрубрици „У потрази за идеалном дистрибуцијом”.

У овом броју у подрубрици „У потрази за идеалном дистрибуцијом” објављујемо блогерски текст о *Ubuntu 14.04*. О *Ubuntu*-у смо за ове две и по године већ писали четири пута, а овим новим приступом покушавамо да не постанемо досадни. Осим блогерског представљања дистрибуција, замолићемо блогере да пишу и како су своје дистрибуције прилагодили сопственим потребама, што по нашем, скромном, мишљењу може да буде занимљиво читаоцима.

Ваше блогерске текстове, мишљења, критике и примедбе и даље можете слати ЛиБРЕ! редакцији на већ познату адресу електронске поште libre [et] lugons [dot] org.

До читања

ЛиБРЕ! тим

Моћ слободног софтвера

Број: 27
Периодика излажења: месечник

Извршни уредник: Стефан Ножинић

Главни лектор: Александар Божиновић

Лектура:
Милена Беран
Јелена Мунћан
Маја Панајотовић
Александра Ристовић

Редакција:
Дејан Чугаљ, Александар Тодоровић
Марко Кажић, Гаврило Продановић
Вељко Симић, Александар Брковић
Никола Харди, Михајло Богдановић
Петар Симовић, Владимир Цицовић
Златан Васовић, Марко Новаковић
Александар Весић

Сарадници:
Горан Мекић, Сандрина Димитријевић
Жељко Попивода, Недељко Стефановић
Јоаким Јањатовић, Стефан Стојановић
Јелена Георгијевић, Владимир Попадић

Почасни чланови редакције:
Александар Станисављевић
Жељко Шарић

Графичка обрада:
Дејан Маглов, Иван Радељић

Дизајн:
Младен Шћекић, Зоран Лојпур

Контакт:
IRC: #floss-magazin на irc.freenode.net
Е-пошта: libre@lugons.org

http://libre.lugons.org

ЛиБРЕ! пријатељи

ubuntu SRBIJA

Slackware Srbija

webserveri.info
info@webserveri:~$ Sve o serverima i programiranju

ubuntu LoCo Montenegro

ЈУгоНС
УДРУЖЕЊЕ ЛИНУКС КОРИСНИКА НОВОГ САДА

ЛИНог
Линукс блог | вести и мишљења

linux zasve
REGIONALNI LINUX PORTAL
linuxzasve.com

archlinux.rs

Објављен је CentOS 7
7. јул, 2014.

Дуго очекивано издање *CentOS 7* коначно је објављено. Ова дистрибуција настала је компајлирањем изворног кода *Red Hat Enterprise Linux 7*.

Користан линк: http://j.mp/WVFC6m

Нови Zorin OS 9 је стигао
15. јул, 2014.

Тачка тежишта *Zorin OS* тима биле су стабилност и брушење широког спектра његових сјајних перформанси. *Zorin OS 9* је базиран на *Ubuntu 14.04 LTS*.

Користан линк: http://j.mp/1xW1yJu

Нова верзија FreeBSD 9.3 је доступна
15. јул, 2014.

Сада је доступна четврта допуна стабилног деветог издања *FreeBSD*-а. Нагласак је на унапређењу стабилности верзије 9.2.

Користан линк: http://j.mp/1lrv97U

Објављен Deepin 2014
21. јул, 2014.

Објављена је нова верзија ове кинеске дистрибуције која осваја све већи број корисника својом једноставношћу и угодним дизајном.

Користан линк: http://j.mp/1pyMQX3

Kali Linux 1.0.8
22. јул, 2014.

Нова верзија *Kali Linux*-а доноси подршку за *USB EFI boot* што омогућава инсталацију и покретање овог система на најновијем хардверу као што је *Apple iBook*.

Користан линк: http://j.mp/1mec9tJ

Talis 1.1
22. јул, 2014.

Позната *Linux* дистрибуција која штити приватност својих корисника, *Talis*, објавила је своју нову 1.1 верзију. Свим корисницима се препоручује да што пре пређу на нову верзију у којој су исправљани бројни сигурносни пропусти, унапређена подршка за *UEFI boot*, замењена *Windows XP* камуфлажа са *Windows 8* камуфлажом итд.

Користан линк: http://j.mp/1s3mGfk

GOG.com од сада нуди и игре за Linux
25. јул, 2014.

GOG је најавио да ће до краја године објавити сто игара за оперативни систем *Linux* из своје понуде.

Користан линк: http://j.mp/1zMB5Rr

Тулуза уштедео милион евра преласком на LibreOffice
27. јул, 2014.

Тулуза, четврти највећи град у Француској, објавио је резултате свога преласка на *LibreOffice*. Процес транзиције започео је у 2011. години и трајао је све до априла ове године. У њега је уложено 800 000 евра, а доноси уштеду од милион евра.

Користан линк: http://j.mp/1pyMSyh

QEMU 2.1
1. август, 2014.

Објављена је нова верзија *QEMU*-а 2.1.

Користан линк: http://j.mp/1ky3kju

GPLv3 дизајн 2D/3D графичке картице у Verilog-у је сада доступан
3. август, 2014.

Иако је доста оваквих покушаја пропало, један пројекат је још увек жив и активно се развија.

Користан линк: http://j.mp/1tMiqoq

Steam има више од 600 игрица за Linux
3. август, 2014.

Од пре два месеца, број игара за *Linux* на платформи *Steam* повећан је за отприлике сто игара.

Користан линк: http://j.mp/1ky3UxL

Аутори: Марко Павловић и Иван Радељић

Увод

У данашње време тешко је замислити живот (за неке и један дан) без друштвених мрежа. Волели их или не, оне све више чине нашу свакодневницу. Пратећи тај тренд, у склопу друштвене мреже *Google+* настала је заједница „*Linux* у Србији”, која окупља све заљубљенике, познаваоце и потенцијалне нове кориснике слободних технологија (*FLOSS*) са нашег говорног подручја.

Заједница тренутно броји триста осамдесет и три члана и јавног је типа, тако да свако може да приступи. Чланови заједнице редовно објављују разне занимљивости и актуелности везане за *Gnu/Linux* и оне су разврстане по категоријама. Тако можете прочитати најновије вести, затражити помоћ, погледати туторијал, започети дискусију, изнети сугестију, или се похвалити сликом своје *Gnu/Linux* радне површине.

Како би додатно побољшао комуникацију међу члановима наше заједнице, оснивач Марко Павловић (*Shiva*) је изнајмио и подесио *Mumble* сервер (*VoIP* софтвер за ћаскање). Његову идеју је подржао одређен број чланова и убрзо је у вечерњим сатима на серверу настало право дружење.

Теме и редовни састанци

Теме су у почетку биле *Gnu/Linux* дистрибуције, односно сличности и разлике међу њима. Касније се причало о детаљним подешавањима, размењивала су се искуства и неке од специфичних ситуација са којима су се поједини чланови сусретали. Наравно, свако је могао да затражи било какву помоћ везану за свој *Gnu/Linux OS* и сви

чланови се заиста труде да помогну, а све то кроз један пријатељски разговор.

На тим дружењима никада се нису унапред дефинисале теме о којима ће се дискутовати, већ је то увек ишло спонтано, некада и невезано за *Gnu/Linux*, па се ту може чути и доста прича којима је сам живот био режисер.

Међутим, пре неколико месеци посета серверу је благо затајила. Услед непостојања договореног термина, већина чланова се мимоилазила на серверу, па је тешко одмах по логовању активно се укључити у разговор.

Схвативши то, оснивачи су дошли на идеју да организују редовне састанке који ће се одржавати у унапред одређеном термину. Договор је пао, одржаваће се средом у 20 часова. Како је време одмицало, испоставило се да је то био прави погодак. И поред тога што чланови могу у свако доба да приступе серверу, некако сви смо навикли да то буде у договореном термину. Не бисмо никога посебно издвојили, али свако ко је био макар једном на састанку, имао је више него позитивно искуство.

На последњим састанцима број *on-line* корисника је прелазио петнаест. Истакли бисмо чињеницу да посете нису само из Србије, па смо тако имали и госте из суседне Хрватске, као и наше редовне чланове из западне Европе. Због разних сфера интересовања, на серверу смо отворили и приватне канале који су везани за једну одређену област (канали

су углавном повезани са називом *Gnu/Linux* дистрибуција). Ту бисмо издвојили ЛиБРЕ! канал, на који слободно можете свратити и рећи своје мишљење у вези часописа, прикључити се редакцији, као и изнети предлоге за његово побољшање.

Mumble подешавања

Mumble је *open-source* софтвер који је одличан за ћаскање и за играње игрица. Комуникација је увек енкриптована, па је приватност загарантована. Да бисте користили *Mumble* сервер, потребно је инсталирати клијент који постоји за *Gnu/Linux*, *Mac* и *Windows*. Код *Gnu/Linux* оперативних система то је најлакше учинити из ризница. Једна од првих ствари које бисмо споменули, јесте регистрација на серверу јер тако добијате одређене привилегије на појединим каналима и могућност отварања канала над којима сте администратор. Након регистрације требало би да направите резервну копију својих *Mumble* сертификата и *Mumble* конфигурационог фајла:
~/.config/Mumble/Mumble.confУколико сте почетник у коришћењу *Mumble* софтвера, може се десити да имате проблема са подешавањем *push-to-talk* пречице и подешавањем микрофона. У том случају можете се накачити на сервер када је ту неко од корисника и они ће вам помоћи да подесите *push-to-talk*, или можете покушати сами следећи ове смернице:

- пожељно је да на састанцима користите слушалице и имате утишане звучнике како не бисте правили ехо другим корисницима.
- пожељно је да подесите **configure** > **Settings** > **Audio Input** > **Interface System** на *pulseaudio* и опцију **transmission** > **transmit** на истој страни на *push-to-talk*. Такође, када то подесите, додајте и на картици *shortcuts* пречицу за *push-to-talk*.

Пошто завршите та ситна подешавања *Mumble* клијента, требало би да буде спреман за коришћење. Не треба заборавити да од сада, када желите да причате на каналу, морате да држите притиснуто дугме за *push-to-talk* које сте изабрали у подешавањима. Користили смо **Left Ctrl + Left Win** као пречицу (прим.аут.).

То можете тестирати преласком на било који канал осим *AFK* и притиском на црвено дугме на траци са алаткама покрећете снимање, затим притисните *push-to-talk* пречицу и изговорите неколико речи док снимате свој глас и потом лансирате ту датотеку у омиљени аудио *player*. Уколико чујете свој глас, подесили сте добро *Mumble* клијент.

За сва додатна подешавања и евентуалне проблеме које имате са *Mumble* клијентом, обратите се за помоћ заједници „*Linux* у Србији", или још боље директно на самом *Mumble* серверу. На клијенту имате опцију да пишете текстуалне поруке, тако да и када вам не ради микрофон, можете писати, свакако ће се наћи неко од искуснијих корисника да помогне у подешавањима.

Параметри приступа

Label - Linux заједница Србије
Address - mumble-de.cleanvoice.ru
Port - 61030
Username - Ваше корисничко име (по жељи)

Идеје, планови

Да састанци не буду само празне приче одређеног броја људи, чланови заједнице су решили да неке од идеја спроведу у дело. Наиме, у плану је да се у наредном периоду искористи знање тренутних чланова *Mumble* канала „*Linux* заједнице Србије" и да се организују предавања на теме везане за слободан софтвер. На састанцима се иначе размењује знање међу члановима који су тада присутни, али ништа од тога не остаје сачувано. Предавања ће бити у форми *webinar*-а, а пошто *Mumble* није погодан за тај тип предавања, за сада се разматрају алтернативе које ће у потпуности испунити захтеве предавача. Сви заинтересовани ће моћи уживо пратити предавања која ће касније бити доступна и за преузимање.

За почетак имамо неколико предавача. Они одлично познају области које ће предавати и своје знање ће несебично делити са другима. Замишљено је да предавања трају четрдесет и пет минута где ће наратора пратити слајдови како би била динамичнија. И док трају договори око техничке стране предавања (која платформа ће бити коришћена за стримовање, тестирање аудио-видео квалитета и др.), ви се можете пријавити као један од наредних предавача. Пожељно би било да већ поседујете слично искуство, јер би заједница „*Linux* у Србији" учествовала на *FLOSS* конференцијама и презентовала своја најбоља предавања.

С надом да ће идеје брзо реализовати, ЛиБРЕ! тим ће писати о сваком предавању које заједница „*Linux* у Србији" објави.

Корисни линкови:
[1] Google+ заједница: „Linux у Србији"
[2] http://mumble.sourceforge.net/

NSA вас прати!

Аутор: Александар Тодоровић

Занимате ли се за анонимност на интернету? Читате ли магазин о *Linux*-у? *NSA* вас прати!

Увод

Прошло је више од годину дана како је *Snowden* изашао у јавност са првим информацијама о томе у коликој мјери нас *NSA* прати. Подаци које он износи, и у ово доба су врло актуелни. Међутим, сада су објављени нови подаци, а неки од стручњака сматрају да ово први пут није дјело *Snowden*-а, него да је у питању неки нови, за сада неидентификован звиждач [1] [2].

Занимате ли се за анонимност на интернету? Прати вас *NSA*!

До сада смо сазнали много тога о томе ко су тачно мете које *NSA* покушава да нападне – од директних приступа водећим интернет компанијама као што су *Google*, *Microsoft*, *Facebook*, *Dropbox* и остали, преко намјерног ослабљивања енкрипцијских алгоритама, па до покушаја инвертовања анонимности које пружа *Tor* (програм фокусиран на анонимност на интернету).

Међутим, нови јавно доступни подаци нам говоре да ту не стаје опсег напада на обичне кориснике. Уколико сте се некада занимали за анонимност на интернету, прати вас *NSA*. Уколико сте икада посјетили страницу *Tor* пројекта, користили *Tails Linux* дистрибуцију, користили *TrueCrypt* за енкрипцију података, или су вас занимали неки други други програми везани за анонимност и сигурност на интернету, од тада сте на листи особа које прати *NSA* (прим. аут.).

Постоје многи разлози за анонимност на интернету и свима је јасно да већина од тих разлога нема неку малициозну активност у фокусу. Од оног малог дијела разлога који имају за циљ неку малициозну активност, шансе да том малициозном активности пријетите

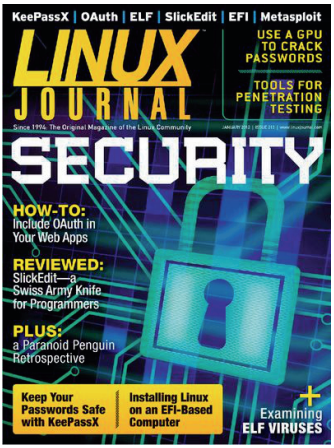
сигурности САД-у су толико ниске да нису вриједне спомена. Међутим, изгледа да *NSA* сматра другачије.

Читате ли познати *Linux* магазин? Прати вас *NSA*!

Да ту не стаје контроверза око нових података, говори и податак како се међу листом домена које *NSA* прати, нашла и једна домена која је потпуно неповезана са анонимности на интернету. Та *IP* адреса припада једном од најпознатијих магазина у свијету који се фокусира на *Linux* и *open source* софтвер. У питању је *Linux Journal* магазин. Као да ни то није довољно, у дијелу изворног кода који је постао доступан јавности, *Linux Journal* је у коментару описан као форум који користе екстремисти. Шта је екстремистично у писању о *Linux*-у, није нам познато.

Закључак

Већ дуго времена знамо да радње које проводи *NSA* нису легалне и како шпијунирају било кога, ко им падне на памет. Добро је познато и да је мала вјероватноћа да постоји особа на планети која није у последњих петнаестак година била на мети *NSA* и чији дио података није завршио у њиховом центру за смјештање података. Међутим, сада је јавно позната нова информација. *NSA* у свом систему дијели интернет кориснике на два дијела: на кориснике који знају нешто о приватности на интернету и кориснике који се не распитују о томе. Сви чланови из првог дијела интернет корисника су под надзором и све што *NSA* може да скупи о тим особама, она скупља. Међутим, узимајући у обзир да је *Linux Journal* домена нападнута, долазимо до закључка да вас не мора занимати анонимност на интернету да би вас *NSA* пратила. Чак и обични *Linux* корисници који читају наведени магазин, под пратњом су и њихови подаци се сакупљају. Ко зна, можда је наш магазин сљедећи на реду.



Корисни линкови:

[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

У сусрет:

2k14 - Second Base

Аутор: jelena&milobit&BobuS von LUGoNS

У Новом Саду од 05. до 07. септембра у Музеју савремене уметности Војводине одржаће се други по реду регионални хакерски конгрес *BalCCon2k14 – Second Base*. Прошли се звао „Први контакт”, а овај треба да буде даљи напредак па је добио име „Друга база”. Да ли је то идеја хакера који се бави бејзболом? Када неко прочита да се одржава хакерски конгрес, ко зна шта му искрсне у мислима? Момци са пепељарама који буље у екране, дредови и мартинке, или ко зна каква комбинација настала у главама холивудских дизајнера? (прим. аут.)

Програм конгреса обухвата бројне презентације, радионице као и предавања из области безбедности рачунарских система, са посебним осврtом на друштвено-политичке теме, попут заштите приватности на интернету, слободног софтвера, програмских језика, развоја апликација и бројне друге. Предавачи су познати и признати припадници хакерских заједница из целог света.

Организатори конгреса су новосадско удружење *Linux* корисника *LUGoNS* и *Wau Holland* фондација из Хамбурга. Основни циљ удружења је рад на бољитку друштва, подстицање коришћења *GNU/Linux* система, како у предузећима, тако и код појединаца и ентузијаста. *LUGoNS* је подршка свим *Linux* корисницима, како у Новом Саду, Војводини, тако и у Србији. Чланови удружења настоје такође да подигну свест о информатичкој култури и промовишу *FLOSS* (енг. *Free/Libre and Open Source Software*).

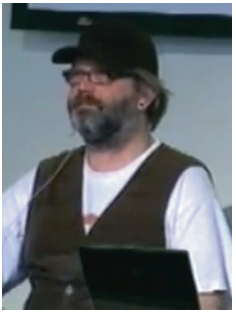
Замишљено је да *BalCCon* постане центар хакерске заједнице у региону, свима који финансијски нису у могућности да посећују друге конгресе у Европи и САД-у. Оваква манифестација неопходна је на Балкану, како би постојало место на коме се једном годишње размењују новостечена знања, састају млади пуни идеја и старији пуни искуства и знања, да се упознају, повежу и охрабре сви које рачунари, мреже, сигурност и неконвенционалан начин размишљања занимају, а немају где да добију жељене информације. Тиме би се у самој хакерској заједници подизао ниво стручности уз вођство старијих колега, а и решио би се проблем немогућности да се допре до простора и времена да се сопствени

радови презентују. Довођење познатих и признатих људи као предавача, јесте омогућавање људима из региона да те исте предаваче сада виде уживо, те да дискутују са њима на теме које их интересују. *BalCCon* жели да приближи свет студентима који се интересују за хактивизам, слободни кôд и техничке науке, те свим младима којима су ове и сродне теме интересантне. На овај начин, млади имају прилику да презентују своје радове уколико су интересантни, иновативни и у складу са моралним начелима за које се залаже цела заједница окупљена око слободног кôда. Хајде да видимо ко су предавачи. Хакери то јесу. Хакер је онај ко своје знање о рачунарима жели да пренесе и подели са другима. Идеја да је хакер нешто злонамерно, настала је у главама холивудских дизајнера. Дођите! Отворите очи и уши и примите паметне информације, а да не долазе из ТВ уређаја или са неког „лајованог" (не недостаје слово **к**, прим. аут.) линка.

• *Mitch Atlman*:

Хакер из Сан Франциска, проналазач. Аутор уређаја који гасе све познате марке телевизора и пушта ваш ум на слободу. Решен је да подели са вама своје знање о електроници, лемљењу и да заједно са њим направите свој сопствени *Arduino* контролер.

• *Bernd Fix*:



Хакер из Берлина, оснивач *Chaos Computer Club*-а 1986. године. Творац првог демо вируса у Часопису. Држи се максиме правог хакера: „*Dont' mess around with other people's data*". Можете чути шта се ново дешава на пољу тзв. пост-квантум криптологије. Чему то служи? Немамо појма, али ћемо доћи на предавање (прим.аут.).

• *Александр Тиморин*:

SCADA системи - на први поглед потпуно ван било каквог животно потребног знања (прим.аут.). Ко би рекао какво хакерско знање се ваља иза површине?

• *Anand Buddhdev*:

Знате ли оно, када се питате која *IP* адреса, које име, *DNS* сервери, где се то региструје? Ананд долази из *RIPE NCC*, а држаће увод у *Ansible*, ни мање ни више.

• Воја Антонић и Дејан Ристановић:

Да ли се неко сећа часописа „Рачунари у вашој кући”, па још првог броја, све са описом самоградње рачунара Галаксија? Упознајте лично њеног творца. Шта још зна? Чујте и ова предавања! Није све застарело, нешто је постојало и пре тога.

• Жарко Живанов:

Ко се сећа горепоменуте Галаксије, Комодора, *ZX Spectruma* и *Amstrad* рачунара, моћи ће од Жарка да чује много тога, а што је најлепше, моћи ће то уживо и да проба. Ретро кутак, сећање на сате и сате игре на најбољим машинама на свету.

• *Moritz Bartl*:

Немачки израз *ZwibelFreunde* значи „пријатељи лука”. Лука? Ако се сетимо како изгледа лого за *Tor*, ствари ће постати јасније. Хоћете ли доћи?

Шта још рећи - дођите, чујте, видите, пробајте! Није хакер оно што пише Холивуд.

Листа предавача није коначна, али је можете пратити на: https://2k14.balccon.org/index.php?title=Speakers

Уколико смо вас заинтересовали да присуствујете конгресу, резервишите и купите карту на сајту https://tickets.balccon.org . Такође, уколико имате нека питања, можете ступити у контакт с нама преко *e-mail*-а на *orga [at] balccon [dot] org*.

Више о програму и организацији на: https://balccon.org

Званични *Twitter* налог: @BalCCon2k14

Реинкарнација

Аутор: Александар Весић

Backtrack-ов наследник - „*Kali Linux 1.0*"

После пет главних издања, *BackTrack* више не постоји. Ипак, љубитељи те *Linux* дистрибуције конципиране за *pentesting* (провала у *IT* системе) не треба да буду тужни јер је са *Kali Linux 1.0*-ом дошао достојни наследник који је цео пројекат пребацио у један озбиљни *Debian* дериват. Први пут је јавност сазнала за име *Kali Linux* 22. јануара 2013. од *Offensive Security*-ја, тима окупљеног око израелског специјалисте за *IT* безбедност *Mati („muts") Aharoni*-ја. Тим *Offensive Security*-ја је на својим блоговима и путем *Twitter*-а објавио да је *BackTrack* поново рођен. Дан издавања те *Linux* дистрибуције специјализоване за *IT*-безбедност са афинитетом за пенетрационе тестове био је *Black Hat Europe* у Амстердаму и већ 13. марта је *Kali Linux 1.0* био спреман за преузимање.

Број издања 1.0 не треба никог да заварава, јер *Aharoni*-јева дистрибуција потиче од славних предака. Од некадашњег *Whoppix*-а је настао *WHAX*, а *WHAX* и *Auditor* су се стопили 2006. године у *BackTrack* и од *BackTrack*-а је после седам година и десет званичних издања настао *Kali Linux*. Код ове дистрибуције ради се о чистокрвном *Debian*-овом деривату базираном на *Wheezy*-ју и тај *3.7 kernel* садржи све неопходне закрпе потребне за иницирање пакета за нападе на бежичне мреже.

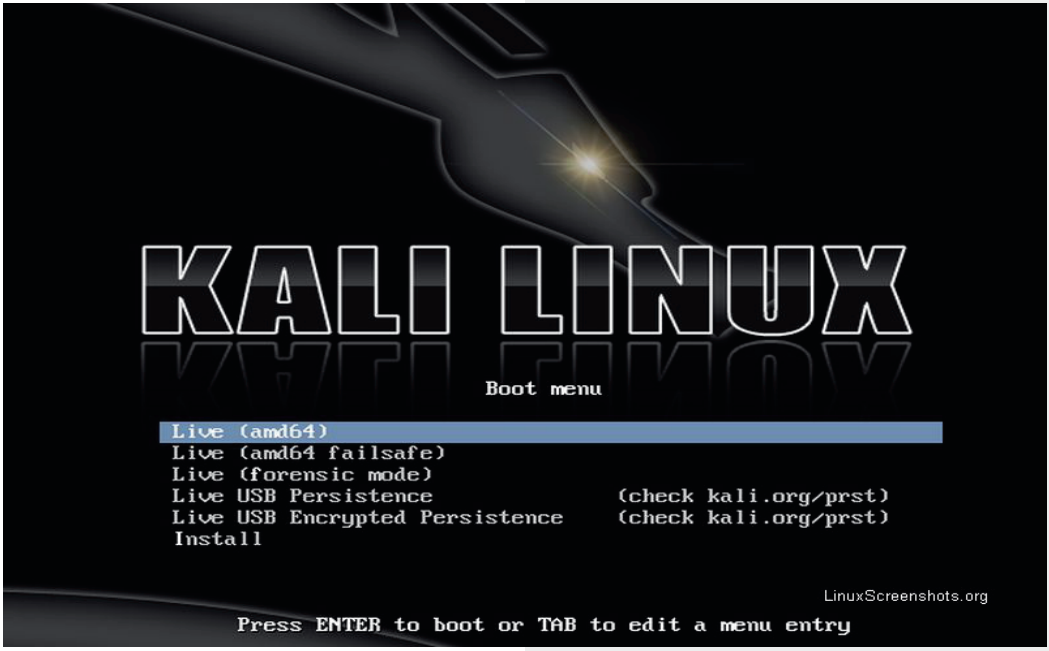
Kali Linux је могуће преузети у различитим варијантама, *ISO* пакет постоји за *x86* и *x64* архитектуре. Поред тога, постоји комплетно инсталирани *Kali* систем у форми виртуелне *VMware-x86* машине. Као окружење радне површи користи се *GNOME*, али као алтернатива се нуди и минималистичка верзија комплетно без окружења радне површи.

Уколико желите другачије окружење, као нпр. *KDE*, *LXDE*, *xfce*, *E17* или *MATE*, то је такође могуће сасвим једноставно извести. *ISO* варијанта дозвољава поред *Live-Boot*-а исто тако директну инсталацију као и форензички модус. Форензички модус оставља хард диск система, који се истражује, недирнутим и спречава аутоматско монтирање свих прикључених меморија, *hd*-а и *usb*-а. Поред осталог, није заборављена ни инсталација путем мреже *PXE* (*Preboot Execution Environment*) коју је могуће без компликација подесити.

Функционалност и на малим системима

Kali је такође доступан и за *ARM* архитектуре *ARMEL* и *ARMHF*. У време издавања је тестиран на уређајима *Samsung Chromebook*, *SainSmart SS808*, *ODroid-U2* и *Raspberry Pi*. Као радно окружење се користи *xfce*. Сама могућност да свако може *Kali Linux* да користи чак и на минималистичким рачунарима који су једноставни да се скривено носе, може бити важно за безбедност и не сме се никако игнорисати.

Kali Linux изгледа на први поглед попут *BackTrack*-а, чак су и иницијални подаци за *Login* (*root/toor*) задржани. *GNOME* структура менија је прерађена, али се може брзо навикнути на њу ако већ имате радно искуство са *BackTrack*-ом. Упада у око и нова „Топ-10" листа у којој се налазе најпроминентнији алати за *IT* безбедност који су линковани на једном месту. Ту су између осталих *Metasploit Framework*, *Maltego Community*, *Nmap*, *Hydra* и *Aircrack-ng*.



Kali GUI се представља прерађеном структуром менија, али нема потребе очајавати јер се *Kali* придржава *FHS*-а (енг. *Filesystem Hierarchy Standard*), тако да су апликације у „претражи" функцији укључене и доступне свуда. Стандардни речник познат код *BackTrack*-а који се користи за нападе на системе заштићене лозинком, на пример уз помоћ *Hydra*-е, редуциран је на листу **rockyou.txt** величине *134MB*. Њу је могуће наћи у *gzip* компримираној форми на **/usr/share/wordlists**. Због тога свега су се појавиле контроверзне дискусије на форумима где се немилице расправља и износе аргументи „за" и „против" нове структуре.

Aharoni-јева одлука да од самог почетка пројекта *Kali* укључи *Debian* специјалисту *Raphael*-а *(„buxy") Hertzog*-а, показала се одличном. *Hertzog* је изузетно допринео код техничког дела око инфраструктуре везане за ризнице као и код могућности коју има *Kali* да свако може да направи свој лични и себи прилагођен *ISO* уз помоћ *Debian*-овог *live-build scripts*. Детаљно упутство како се то може учинити, већ се налази у *Kali* документацији. Осим тога, њихов тим одржава за сваког видљиве отворене верзије преко *git*-а у којима су аутори побројани и сви они морају пакете да потпишу са *GPG*.

Community која активно учествује у пројекту, активно је подржана од стране многих произвођача, а од појединих неочекивано много. Тако на пример *RAPID7* (*Metasploit*) води *Kali Linux* као званични оперативни систем за комерцијалну верзију *Metasploit*–а и самим тим нуди „подршку произвођача". Комерцијална варијанта *Web* радне површине од *Metasploit*-а је тако интегрисана у *Kali*

Linux. Наравно, бесплатно је могуће користити само *Community* верзију и то тек након што сте се регистровали. Бесплатни *Metasploit Framework*, основа и идеја данашњих *Metasploit* производа одувек спада у *Aharoni*-јев стандардни репертоар и нуди поједностављену радну површину за нападе путем *Exploits*.

Произвођачи и њихова улога

Aharoni-јев тим је покушавао још од времена *BackTrack*-а *Metasploit-Framework* да упакује у пакет, који није ни предвиђен да буде упакован. *RAPID7* је, како наводи *Aharoni*, искористио *Kali Linux* да направи један прави *Debian* пакет за *Metasploit* и поврх тога обећао је да ће о свом трошку да га актуализује сваких седам дана.

Paterva је своју *Maltego-Community* верзију *Kali Linux Edition 3.3.0* поставио доступном. Уз помоћ *Maltego*-а, могуће је у *IT* безбедносном окружењу сакупљати податке и исте потом динамички-агрегирано представити. Тај произвођач се одувек фокусирао на прегледно визуализирање комплексне повезаности сакупљених података и њихову међусобну повезаност. Као и код *Metasploit*-а, у поређењу са комерцијалном верзијом, *Community* верзија не нуди све могућности и за његову употребу се мора регистровати.

Аутоматска актуализација долази

Што се тиче актуелности оруђа које стоји на располагању повезано са *Debian* пакетом, постоје планови за ближу

будућност. *Aharoni* је открио да његов тим ради на идеји да уз помоћ аутоматизованог централног система, одређене екстерне *git* и *svn repositories* у реалном времену надгледа и да код нових верзија аутоматски генерише у нове *Kali* пакете. На основу изјаве развојног тима да су извршили велику акцију чишћења интегрисаних алата, у *Kali Linux*-у се налази више од триста познатих алата, од оних за напад и анализу до оних за *Reverse engineering* и дигиталну форензику као нпр. *TSK* са *Autopsy*. Поред стандардне подршке за многобројне *WLAN* чипове, у бежичном окружењу су такође заступљени и *Bluetooth*, *RFID*, *NFC* као и *ZigBee*.

Популарни *Frontend* за *Metasploit Framework* под именом *Armitage* који је у тренутку издавања верзије 1.0 недостајао, могуће је једноставно уз помоћ **apt-get install armitage** накнадно инсталирати. Наравно, уколико *Armitage* недостаје, могуће га је такође уз помоћ **apt-get dist-upgrade** аутоматски инсталирати.

Иначе *Kali Linux* се понаша јако тихо у мрежи. Поједини сервиси који омогућавају спољну идентификацију, код стартовања система су деактивирани и морају се по потреби стартовати. То важи подједнако и за *Metasploit* или *Armitage* пре чије употребе је потребно користити команде **service postgresql start** за базе података и **service metasploit start** за *RPC* и *Web-Service*. Уколико желите то да аутоматизујете приликом подизања система, можете користити **update-rc.d <service> enable**.

OpenVAS & Co. траже рањивости

У области анализе рањивих тачака *Kali Linux* интегрише поред разних *Fuzzer*-а и *Scanner*-а такође и *OpenVAS*, једне варијанте скенера рањивости *Nessus*. Коме је *Nessus* драги, може да скине *Debian*-ов пакет са интернет странице произвођача и путем **dpkg –i <Package>** као и **/etc/init.d/nessusd start** исти инсталира и покрене. Рањивости код *Web* апликација могуће је истражити уз помоћ разних скенера, између осталог и са *Burp Suite Free Edition 1.5*.

Закључак

Када су *Aharoni*-ја питали за значење назива *Kali*, одговорио је да је *Kali* једно лепо име и да има много значења у различитим језицима, као и да они нису ништа специфично тиме хтели да кажу.

Сама дистрибуција оставља један јако позитиван утисак. Не виђа се често да један *Community* пројекат тако детаљно обнови и оживи дистрибуцију које више нема. Задивљујуће је да мали тим од петоро људи оствари такве резултате и поред тога дефинише де факто стандард за све дистрибуције које се фокусирају на *IT* безбедност. Ми им желимо много среће и успеха у даљем развоју квалитетне *Kali Linux* дистрибуције.

Извори:

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

У потрази за идеалном дистрибуцијом:

ubuntu 14.04

Аутор: Александар Тодоровић

Canonical је објавио нову верзију најпознатије *Linux* дистрибуције 17. априла. Ово је *LTS* верзија (скр. *LTS - long term support*), што значи да има подршку сљедећих пет година. Носи кодни назив *Trusty Tahr*, а број нове верзије је 14.04. Чекајући нову верзију моје најдраже дистрибуције (*elementary OS*), одлучих се да испробам нову верзију *Ubuntu*-а.

Да напоменем, ово ми није само први пут да користим нову верзију *Ubuntu*-а, него ми је први пут да користим *Ubuntu* уопште. Никад га прије нисам користио и нисам сигуран шта треба да очекујем. Ово је сасвим субјективно описан мој пут кроз *Ubuntu*.

На лаптопу сам имао инсталиран само један систем - *Windows 8.1*. Поред њега је стајала гомила празног простора на хард диску предвиђеног за неку *Linux* дистрибуцију и једна одвојена енкриптована партиција (користећи *TrueCrypt*) за податке које користим и на *Linux*-у и на *Windows*-у (о недавној контроверзи *TrueCrypt*-а сам писао у прошлом броју). На лаптопу постоји подршка за *UEFI*, међутим та подршка је подразумевано била искључена још прије годину и по дана када сам купио лаптоп. Ништа не би требало да спријечи да се *Ubuntu* инсталира.

Убацујем *USB* са новом верзијом *Ubuntu*-а и покрећем *live* верзију *Ubuntu*-а. Никад нисам доживио да је потребно дуже од минуте од клика за покретање *live* верзије до стварног покретања *live* верзије. Остао сам зачуђен. Међутим, схватио сам да *Ubuntu* са својим *Unity* корисничким интерфејсом не носи без разлога титулу једног од најзахтјевнијих оперативних система који су базирани на *Linux*-овом кернелу.

На први поглед, *Ubuntu* је лијепо дизајниран. Прате свој дизајн из верзије у верзију и то ми се свиђа. Одлучих да га инсталирам на слободан простор који имам. Покрећем инсталацију, од празног простора правим три партиције: *swap*, *boot* и *root* партицију. Означим да ми се *GRUB* инсталира на *boot* партицију, остали дио система на *root* партицију. Укључујем опцију да ми се приликом инсталације система инсталирају и власнички кодеци, а искључујем опцију

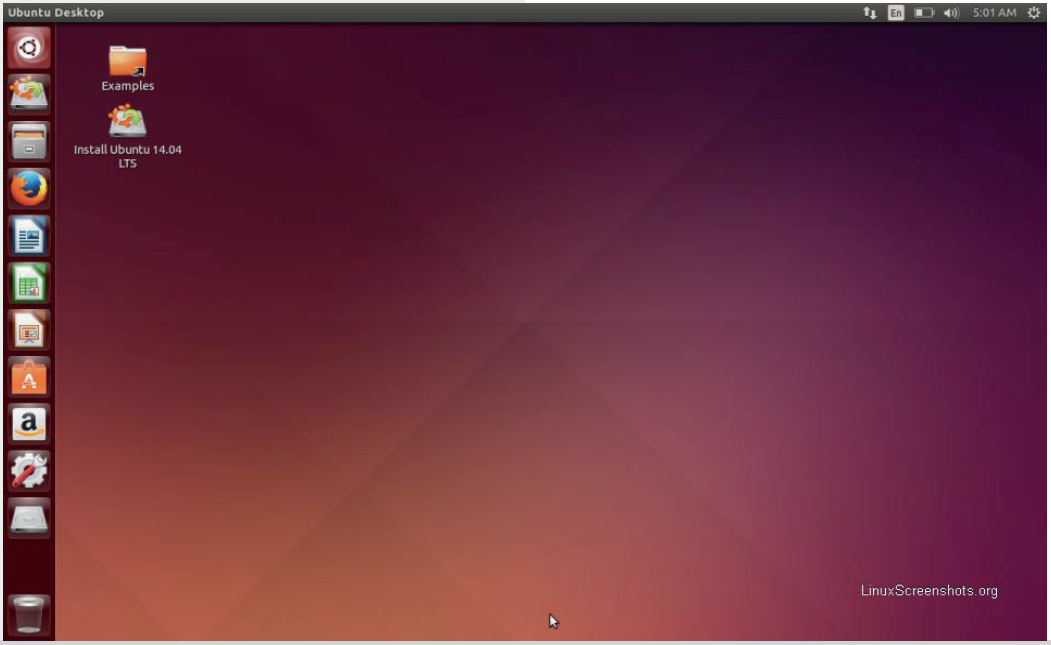
да инсталирам и сваки тренутно доступни *update* приликом инсталације да бих убрзао процес инсталације.

Моја жеља да тиме убрзам процес инсталације није успјела. Инсталација је трајала добрих двадесетак минута, што је дуже од било које дистрибуције које сам покушао да инсталирам (а покушао сам много). Гледајући у терминал приликом инсталације, примјетио сам да се неке линије више пута понављају. То је остало неразјашњено у мојој глави. Завршила се инсталација и систем је тражио да га рестартујем, што сам и урадио.

Систем се рестартовао и *boot*-овао у *Windows*!? Сад ми тек ништа није било јасно. Током инсталације сам видио команде за инсталацију *GRUB*-а, за његов *update* и за препознавање других система, међутим, *GRUB* се није покренуо. *Boot* је изгледао потпуно једнако као и прије него што сам инсталирао *Ubuntu*. Ту сам већ био спреман да одустанем од свог истраживања по *Ubuntu*-у.

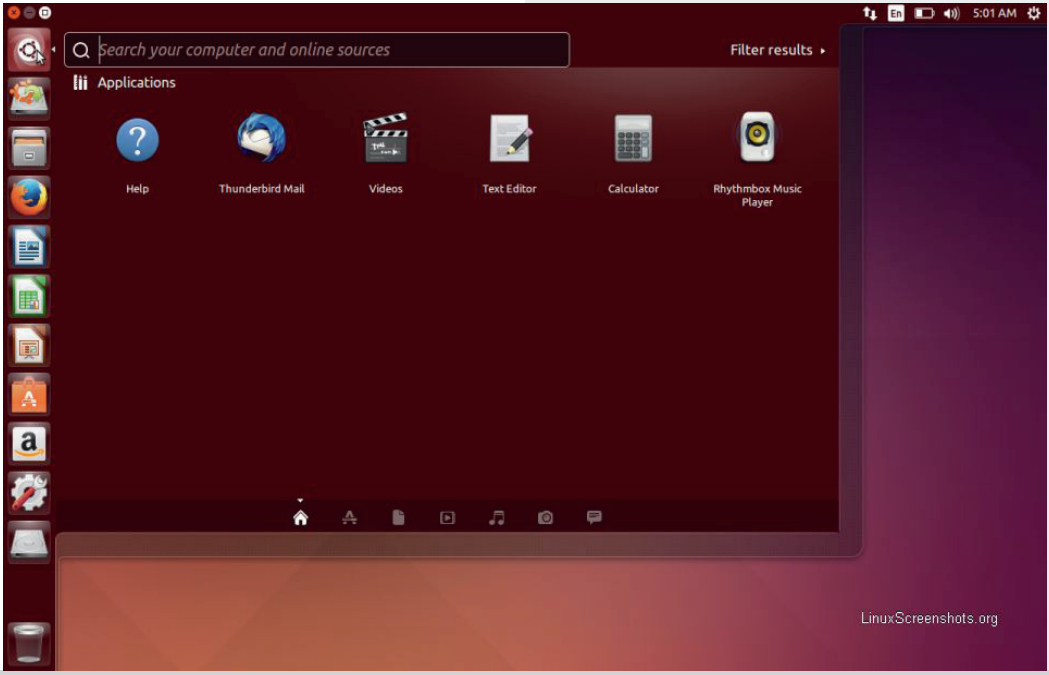
Дан послије сам се нашао у ситуацији да више не могу да поднесем изглед новог *Windows* система. Одлучио сам да мало истражим проблем са *Ubuntu*-ом само да бих се ријешио *Windows*-а. Један од првих линкова на *Google*-у ме је одвео на дио *Ubuntu* документације који ми препоручује да пробам *boot-repair* пакет користећи *live* слику. Као и све до сада што сам покушао користећи *Ubuntu*, и за извршавање *boot-repair* опције ми је требало дуже, него што сам мислио да хоће. Након што се процес завршио, *GRUB* је напокон радио и приказивао ми је исправно оба система.

Након мучења са инсталацијом, за које нисам мислио да ће бити потребно узимајући у обзир да користим



најпознатију *Linux*-ову дистрибуцију, покрећем *Ubuntu* са свог хард диска. Сада је дошло на ред истраживање о томе како систем функционише. Испробавам *Unity* који је доживио толико негативног публицитета. Чини се брз за сада, међутим лаптоп има проблема са прегријавањем. Након мање од минуте истраживања како *Unity* ради, искочио ми је прозор који ми каже да је доступан *update* за неке од инсталираних пакета. Узимајући у обзир да је прошло мање од три мјесеца како је нова верзија *Ubuntu*-а постала доступна за јавност, помислио сам да количина пакета за које је доступан *update* неће бити велика. Међутим, преварио сам се. Преузимало се преко *200MB* и инсталирало се педесетак ажурираних пакета. Процес је поново трајао неких двадесетак минута и у том тренутку сам био захвалан што нисам укључио ту опцију приликом инсталације система.

Приликом самог ажурирања сам постао свјестан да ова авантура уз овакве проблеме са прегријавањем лаптопа неће добро да се заврши. Да напоменем да лаптоп нема никаквих проблема са прегријавањем користећи нови *Windows*, а користећи друге дистрибуције проблеми постоје само када је систем превише оптерећен. Инсталирао сам *tlp* и након његовог покретања ситуација се увелико поправила. Имам обичај да искључим лаптоп са пуњача на неколико секунди, само да провјерим колико би лаптоп издржао под таквим оптерећењем на батерији. Прије инсталирања *tlp*-а, *Ubuntu* ми је показивао да би батерија издржала четрдесет минута. Након покретања *tlp*-а, то вријеме се побољшало на сат и десет минута. То и



даље није импресивно упоређујући са два и по сата користећи *Windows* и два сата користећи *Arch Linux* са *KDE* окружењем, међутим може да прође.

Што се тиче нових функција *Unity* окружења, сада је могуће бирати да ли желите да апликацијске контроле прикажете у горњем панелу или у насловном панелу од апликације, могуће је смањити величину икона на *launcher*-у, софтвер центар се сада аутоматски прилагођава уколико проширите његов прозор, а ту су и нови *wallpaper*-и између којих можете бирати. Иако нове функције нису драстичне, сада корисник има више опција за прилагођавање *Unity*-а, што свакако чини коришћење *Unity* окружења пријатнијим. Ја морам да признам да се нисам тако осјећао. Осјећао сам се као да се борим са системом да бих добио оно што хоћу: једноставан и добро дизајниран кориснички интерфејс преко којег ћу брзо и ефикасно инсталирати и користити друге програме.

Након што сам неколико дана дао прилику *Unity* интерфејсу, схватио сам да он једноставно није за мене. Иако му не могу наћи много мана, могу рећи да систем није добро „исполиран" и да се јављају неке грешке (примјер: порука о доступним *update*-има је у прозору имала могућност да прикаже називе пакета који се ажурирају, међутим нису сви називи пакета били видљиви).

Поред класичног *Ubuntu*-а са *Unity* графичким интерфејсом, стигле су нам и нове верзије службено подржаних *Ubuntu*-ових деривата са другачијим корисничким интерфејсом:

- *Kubuntu* - *Ubuntu* са *KDE* корисничким интерфејсом: http://www.kubuntu.org/getkubuntu
- *Ubuntu GNOME* - *Ubuntu* са *GNOME* корисничким интерфејсом: http://wiki.ubuntu.com/UbuntuGNOME/GetUbuntuGNOME
- *Xubuntu* - *Ubuntu* са *Xfce* корисничким интерфејсом: http://xubuntu.org/getxubuntu
- *Lubuntu* - *Ubuntu* са *LXDE* корисничким интерфејсом: http://help.ubuntu.com/community/Lubuntu/GetLubuntu

Било ми је драго што сам напокон нашао времена да испробам најпознатију *Linux*-ову дистрибуцију. Далеко од тога да ме је одушевила и далеко од тога да ћу је редовно користити. Моја потрага за дистрибуцијом коју ћу користити док не изађе нова верзија моје најдраже *Linux*-ове дистрибуције се наставља.

Додатни извори

Аутор: Жељко Попивода

Напомена: *LTS* издање има подршку у трајању од пет година за *Ubuntu* и *Kubuntu*, односно три године за *Ubuntu GNOME*, *Xubuntu* и *Lubuntu*.

Ubuntu

Ubuntu као подразумевано окружење радне површи користи *Unity*.

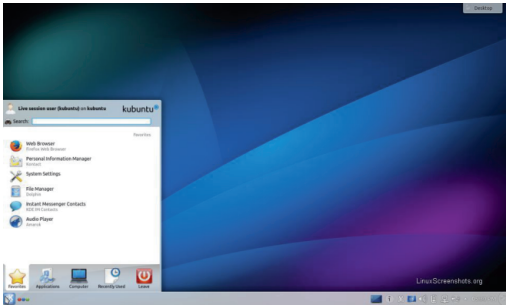
Препоручујем да погледате снимке екрана: http://www.linuxscreenshots.org/

?release=Ubuntu%2014.04 и видео преглед http://youtu.be/YbXWljOxA9U .

Ubuntu можете преузети са: http://www.ubuntu.com/download

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

Kubuntu



Кубунту - *Ubuntu* са *KDE* окружењем радне површи.

Препоручујем да погледате снимке екрана: http://www.linuxscreenshots.org/?release=Kubuntu%2014.04 и видео преглед http://youtu.be/VNzZr4aFPVY .

Kubuntu можете преузети са http://www.kubuntu.org/getkubuntu .

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

Ubuntu GNOME

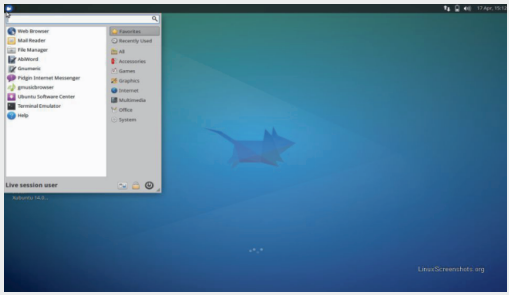
Ubuntu GNOME - *Ubuntu* са *GNOME* окружењем радне површи.

Препоручујем да погледате снимке екрана http://www.linuxscreenshots.org/?release=Ubuntu%20GNOME%2014.04 и видео преглед http://youtu.be/dTNmAorlQBY .

Ubuntu GNOME можете преузети са: http://wiki.ubuntu.com/UbuntuGNOME/GetUbuntuGNOME .

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

Xubuntu



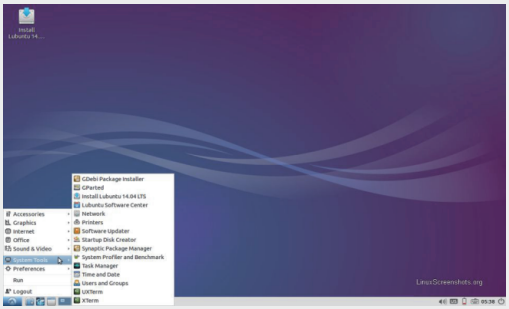
Xubuntu - *Ubuntu* са *Xfce* окружењем радне површи.

Препоручујем да погледате снимке екрана http://www.linuxscreenshots.org/?release=Xubuntu%2014.04 и видео преглед http://youtu.be/Dv26_2bjyhY .

Xubuntu можете преузети са: http://xubuntu.org/getxubuntu .

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

Lubuntu



Lubuntu - *Ubuntu* са *LXDE* окружењем радне површи.

Препоручујем да погледате снимке екрана http://www.linuxscreenshots.org/?release=Lubuntu%2014.04 и видео преглед http://youtu.be/fiwKz8zV240 .

Lubuntu можете преузети са: http://help.ubuntu.com/community/Lubuntu/GetLubuntu .

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

Преглед популарности *GNU/Linux /BSD* дистрибуција за месец јул

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<

Пад <
Пораст >
Исти рејтинг =
(Коришћени подаци са *Distrowatch*-а)

libGDX

„Java game development framework”

(3. део)

Аутор: Гаврило Продановић

Свако би од *framework*-а за развој игрица на више платформи очекивао добру апстракцију по питању улазних уређаја да би убрзао свој процес развијања, а *LibGDX* се са тиме може похвалити. Наш *framework* посједује два основна начина за обраду улаза: први је *pooling* гдје позивањем методе утврђујемо стање улазног уређаја (нпр. да ли је типка на тастатури спуштена или читање позиција миша), а други је хватање догађаја (енг. *event handling*).

Преко *pooling*-а можемо приступити уређајима уз помоћ неколико основних метода. Да ли је *touch screen* додирнут, можемо провјерити помоћу **isTouched()** која враћа **true** ако постоји додир и **false** у супротном. За *multitouch* можемо позвати **isTouched(int index)**, гдје *index* означава који прст желимо провјерити. Да бисмо добили координате додира, постоје *getX()* и **getY()** методе, а за *multitouch* у аргумент прослиједимо индекс нашег прста/показивача. На *desktop*-у за манипулацију мишем можемо користити горе претходно наведене методе, а у том случају улаз са миша ће се третирати као *single-touch screen*. За миш такође постоје додатне методе као што су **isButtonPressed(int button)**, **setCursorPosition(int x, int y)** и **setCursorCatched(boolean)** која хвата курсор на средину екрана и чини га невидљивим; и на крају *setCursorImage* којом можемо промијенити досадну бијелу стрелицу у нешто љепше. Све ове методе, осим *isButtonPressed*, доступне су само на *desktop*-у, док ова на мобилним платформама додир екрана региструје као клик лијевог тастера миша. Типке са тастатуре и посебну дугмад на мобилним платформама можемо *pooling*-ом да хватамо уз помоћ **isKeyPressed(int key)** методе, а *key* кодови се налазе у статичкој класи *Keys*.

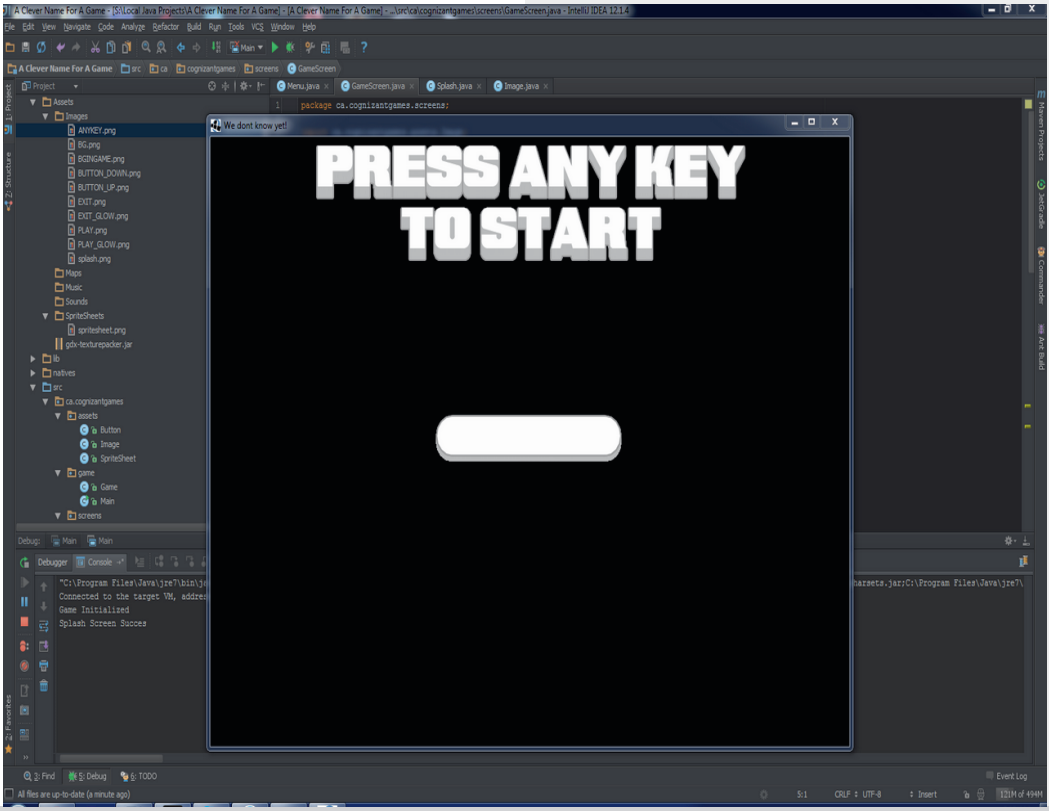
Pooling може бити згодан у неким ситуацијама, али много практичније је користити хватање догађаја. У *LibGDX*-у ћемо догађаје хватати тако што имплементирамо интерфејс *Input Processor*, а онда инстанцу имплементираног интерфејса поставимо тако што га прослиједимо **Gdx.input.setInputProcessor (InputProcessor)** методи. *InputProcessor* декларише следеће методе за имплементацију: - *touchDown*, *touchUp* и *touch Dragged* - помоћу њих можемо регистровати када је прст спуштен или дигнут, или да ли га помјерамо по екрану. - *keyDown*, *keyUp* и *keyTyped* - прве двије методе прослиједују *keycode*, а *keyTyped* ће се позвати само када се генерише *unicode* принтабилни карактер. - *mouse Moved* и *scrolled* се позивају само на *desktop* платформи. Прва прослиједује **x** и **y** координате, док друга прослиједује **-1** или **1** у зависности од смјера точкића на мишу када се окрене.

Користећи *touch* као главни улазни уређај за контролу игре, природан начин приступа је коришћење неких основних гестова (енг. *gesture*) једним прстом или помоћу више њих. Као примјер узећемо увећавање помоћу два прста. Унутар *LibGDX*-а постоји класа *GestureDetector* која имплементира *InputProcessor* интерфејс и може да препозна осам основних гестова који су дефинисани у *Gesture Listener* интерфејсу. За гестове који се могу извести једним прстом/показивачем на *desktop* платформи, *GestureDetector*

ће за улаз да *wrap*-ује миш.

На мобилним уређајима углавном су присутни акцелерометар и компас, а читање њихових вриједности је могуће преко *pooling*-а у нашем *framework*-у. Једини проблем је што се сензорима може приступити само преко *pooling*-а и не постоје *helper* класе које би нам помогле у имплементацији контроле на овај начин. Уз акцелерометар и компас можемо на мобилним уређајима користити и вибрације да бисмо пренијели што бољи утисак играчу. Да бисмо активирали вибрацију, можемо методи **Gdx.input.vibrate** прослиједити трајање вибрације у милисекундама, ако желимо извести сложену вибрацију, можемо прослиједити цјелобројни низ у којем сваки непарни елемент означава дужину трајања вибрације у милисекундама, а сваки парни мировање у милисекундама. Други аргумент означава елемент од кога почиње понављање у петљи или **-1** ако желимо да се вибрација заустави на крају низа. У случају да тренутну вибрацију желимо прекинути прије завршетка, у томе ће нам помоћи **cancelVibrate**().

Уколико од играча требате затражити неки унос као што су надимак или лозинка за сервер, у томе вам може помоћи *TextInputListener* и метода **Gdx.input.getTextInput** која ће



избацити дијалог и питати корисника за унос. Изглед дијалога зависи од платформе, па ће на *Android*-у да буде уобичајен *Android* дијалог, а за *desktop* - *Swing* дијалог. Уколико одлучите писати своје контроле за унос са тастатуре, на *desktop*-у, *iOS*-у и на *Android* уређајима са физичком тастатуром ће то бити лако изводљиво. За *Android*-е који немају физичку тастатуру, може се користити *onScreen* тастатура, али постоје багови који неће хтјети приказати тастатуру уопште, или одређени виртуални тастери неће функционисати. Од тастатура познато је да *stock android* или *Google*-ова тастатура одлично ради. Од баговитих тастатура могу се споменути *HTC* и *Samsung*-ове и многе још друге. Овај проблем је присутан и зна да зада главобољу, али да не буде као потпуно обесхрабљење, рећи ћемо да није фаталан и постоје начини да се заобиђе, као што је на примјер додатан *Activity* у *Android* пројекту који служи за скупљање уобичајених података.

Можда бисте жељели на *desktop*-у користити могућности које постоје на мобилној платформи као што су *multitouch*, акцелерометар и компас, да ли због бржег тестирања или да бисте створили неку врсту хибридне платформе. У томе ће вам помоћи класе *RemoteSender* и *RemoteInput*. *RemoteInput* имплементира интерфејс *Input* тако да све горе што смо до сад навели, јесте подржано. *RemoteInput* је тај који отвара улазну конекцију и чека да се повеже неки *RemoteSender* који имплементира интерфејс *InputProcessor* и у конструктору узима *IP* адресу и порт на који треба да се повеже. На *Play Store*-у постоји *Gdx Remote* апликација која вам може уштедјети вријеме.

Гејмери имају још један вид улаза за рачунар, а то су џојстици или *gamepad*-ови. У *LibGDX*-у они су подржани преко екстензије *gdx-controllers*. Може се користити *pool*-овање, или се могу регистровати *event listener*-и. Пошто не постоји стандард по питању мапирања дугмади на овим уређајима, биће потребно да корисника проведете кроз конфигурацију џојстика. Тренутно једини мапирани контролер је *Ouya* за који не морати провести играча кроз конфигурацију. Ова екстензија може да се користи и на *Android* уређајима који покрећу најмање 3.1 верзију овог система.

На крају да резимирамо укратко: *LibGDX* посједује добру апстракцију и богату подршку за различите улазне уређаје. Осим бага са неким *onScreen* тастатурама, можемо рећи да смо у потпуности задовољни како је улаз одрађен у овом *framework*-у.

Увод у програмски језик *C*

(4. део)

Аутор: Вељко Симић

Низови и матрице

У прошлом броју смо причали о условном гранању и контроли тока програма. Научили смо рад са петљама, па бисмо овај текст, у коме ће бити речи о низовима, почели једним питањем: како ћемо написати програм који рачуна просечну вредност за десет вредности које се уносе? Претпостављамо да би ваше решење имало неку петљу која би се извршавала десет пута и у њој бисте уносили вредности у неку променљиву, назовимо је збир, сабирали бисте те вредности и на крају бисте ту променљиву поделили са 10. Добро, хајде да мало отежамо задатак. После рачунања просека исписати све вредности које су веће од њега! Ту настаје проблем: ми те вредности нисмо запамтили, већ само њихов збир. Када бисмо покушали да задатак решимо са десет различитих променљивих, задатак би био поприлично ограничен и веома тешко бисмо га уопштили за, на пример, шеснаест вредности. За овакве, а и многе друге ситуације, користе се низови.

Низ је одређен број меморијских локација које имају исти назив. Појединачним вредностима се приступа

помоћу њиховог индекса (њиховог редног броја у низу) и све вредности у низу морају бити истог типа. Индекс низа у програмском језику *C* се пише у угластим заградама и, пошто све почиње од 0, то важи и за нумерацију чланова низа.

Општа декларација низа изгледа овако:

```
tip ime_niza[broj_članova];
```

Нпр. ако нам треба низ који ћемо назвати Пера, од десет чланова типа *int*, декларисаћемо га овако:

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

Кад желите да пети члан тог низа има вредност 42:

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

Као што видите, све почиње од 0, па пети члан низа има индекс 4. Један од уобичајених почетничких лапсуса јесте приступање члану који не постоји. У овом случају би био члан са индексом 10 – дакле пера[10] не постоји, а ова грешка се назива *off by one*.

Можда мислите да одређивање броја чланова низа при декларацији ограничава низове, али, као што смо рекли на почетку, низ је скуп меморијских локација и рачунар мора знати колико меморије треба да резервише. Постоји начин динамичког додељивања меморије низу. То ћемо описати у неком од наредних текстова. Не морају сви чланови низа бити искоришћени. Тако да, ако сте резервисали десет места, можете да искористите десет, једно, али и ниједно.

У програмском језику *C* вредности елемената низа нису унапред декларисане – дакле, у тим елементима се налази вредност која се налазила на тој меморијској локацији, осим у случају када је низ дефинисан као глобална промењива. Тада сви чланови низа имају вредност 0.

Сада када можемо рећи да имате неко теоријско знање о низовима, можемо урадити задатак с почетка текста.

```
#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;
}
```

Низови такође могу да буду вишедимензионални. Дводимензионални низови се називају матрице. Матрице имају велику улогу пре свега у чувању и обради табеларних података. Да бисте добро владали матрицама, потребно је да имате искуства са вишеструким *for* петљама. Пролазак кроз матрицу је шаблонски поступак и своди се на употребу две угњеждене петље *for*, од којих је спољна за редове, а унутрашња за колоне. Тако пролазимо кроз матрицу ред по ред. Матрица се дефинише слично као низ, само што има две угласте заграде које означавању индексе рада и колоне. Ако желимо да дефинишемо матрицу 10×10 типа *int*, то би изгледало овако:

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

Следи пример учитавања и исписа матрице:

```
#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;
}
```

Ово је био кратак увод у дискусију о низовима и матрицама. У следећем броју ћемо показати неке нове технике са овим структурама и неке нове ствари у *C* језику.

Утицај математике на настанак и темеље рачунарства (3. део)

Ограничења, проблеми и њихов значај за криптографију

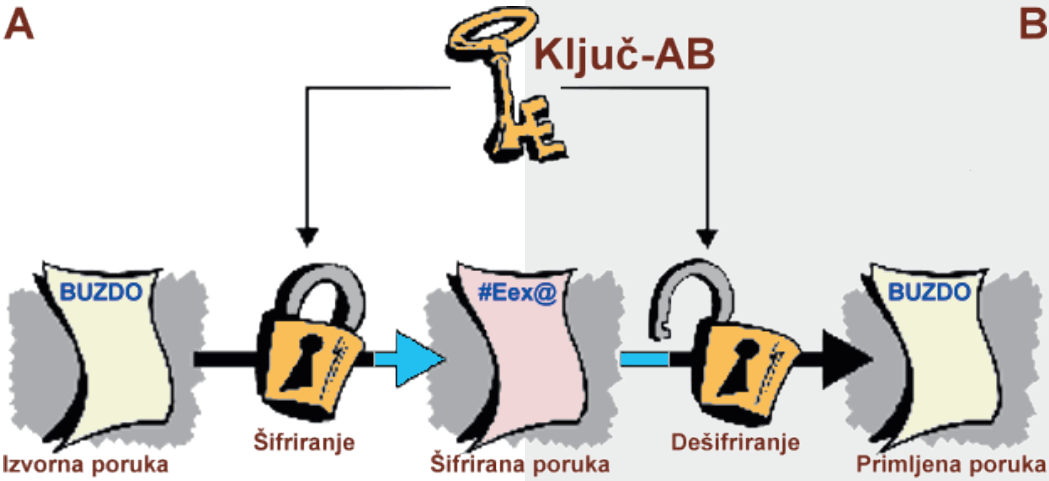
Аутор: Недељко Стефановић

Међу прве резултате спадају и резултати о немогућности решавања неких проблема алгоритмом. Један од таквих резултата је и проблем заустављања који се састоји у томе да за дати програм на улазу, који сам не захтева никакав улаз, одредимо да ли би се тај програм једном пуштен у рад завршио у коначном броју корака.

Други сродан резултат је да није могуће направити програмски језик који би обухватио све алгоритме и чији би се сви програми заустављали у коначном броју корака. Да би неки програмски језик обухватио све алгоритме (заустављиве поступке), он мора да допушта и конструкције као што су бесконачне петље, тј. конструкције које могу да раде, а да се никада не зауставе. Највећи број програмских језика је баш такав, а има и система код којих се жртвује обухватање свих алгоритама зарад универзалне заустављивости. Пример је помоћник у доказивању теорема *Agda*.

Осим доказивања да неки проблеми нису алгоритамски решиви, изучава се и алгоритамска сложеност проблема који се могу алгоритамски решити. Сложеност одређеног алгоритма за решавање неког проблема су ресурси (временски или меморијски или и једни и други) за његово извршавање, док је сложеност проблема заправо сложеност најефикаснијег могућег алгоритма за његово решавање. Понекад можемо знати да за неки задатак имамо оптималан алгоритам, али то најчешће није случај јер је то јако тешко доказати.

Понекад је добро што су неки проблеми алгоритамски јако тешки јер не желимо да буду решени. Такви су проблеми разбијања криптографских примитива чије би решавање довело до злоупотреба. Било би јако добро да имамо криптографске примитиве за које имамо доказе да се не могу разбити без одређених израчунатих ресурса који превазилазе снагу било каквог хардвера који се може произвести. Међутим, то није случај, а искључиви разлог је што још увек није достигнут потребан степен развоја



математике. За сада се криптографска безбедност проверава емпиријски, тако што се алгоритми објављују у научним часописима, па ако се за одређен број година нико није јавио са поступком разбијања, онда се алгоритам сматра безбедним. Свакако би боље било имати доказ безбедности.

Криптографске примитиве треба свакако да буду ефикасне за употребу на предвиђен начин, а што теже за разбијање. Обично се као захтев за ефикасном употребом узима да број корака буде ограничен полиномом по сложености улаза (овде је то величина кључа). За такве проблеме се каже да припадају класи сложености *P*. Као захтев за тешко решавање се обично узима да број корака расте експоненцијално у односу на сложеност улаза.

Све примитиве се могу разбити у полиномијалном времену на машинама са неограниченим паралелизмом (нпр. бесконачним бројем процесора који могу паралелно да раде). Ако тражимо приватни кључ од 100 битова када је дат јавни кључ, ми заправо треба да проверимо све могуће низове од 100 битова, који од њих чини приватни кључ који се слаже са датим јавним. Прво можемо проблем поделити на два случаја – оне код којих је први бит једнак 0 и оне код којих је први бит једнак 1. Те случајеве могу да обрађују два процесора паралелно. Затим, сваки од та два случаја поделимо на два подслучаја – када је други бит једнак 0 и када је други бит једнак 1. Те подслучајеве могу паралелно да обрађују четири процесора. Тако ћемо у сто корака цепања сваког од подслучајева на два подслучаја у сто корака упослити процесоре од којих сваки обрађује један низ од 100 битова и сви раде паралелно. То омогућава да се на таквим машинама тај проблем реши ефикасно. Слична идеја се може применити и на разбијање симетричних кључева и криптографских хеш (енг. *hash*) функција.

За такве проблеме се каже да припадају класи *NP*, која из наведених разлога чини

теоријски максимум криптографске безбедности.

За класе *P* и *NP* се још увек не зна да ли су исте или различите. За решење тог проблема је чак понуђена награда од милион америчких долара и он свакако представља централни нерешени проблем теоријског рачунарства. Ако су те класе једнаке, с обзиром на то да проблеми разбијања увек припадају класи *NP*, они у том случају припадају и класи *P*, што значи да је ефикасно разбијање могуће, па би примена криптографије била знатно ограничена и отежана. У супротном остаје могућност да постоји проблем који је применљив на криптографију и има потребне особине. Стога је у сваком случају неопходно решити тај проблем да би се стигло до примена у криптографији.

Мада је машине са неограниченим паралелизмом немогуће направити, оне нужно учествују у формулацијама ставова релевантних истраживања, која се спроводе јер је природа проблема таква. Другачије није могуће доћи до резултата јер је предуслов за неоспоран доказ неког става да став по својој формулацији буде тачан.

Чак и када се то успе, остаје још један проблем. Физичари су открили другачији приступ израчунавању тзв. квантним рачунарима, који мада могу да решавају потпуно исте проблеме као класични (тј. не доводе у питање Черч-Тјурингову тезу), неке проблеме могу да решавају и ефикасније, где спадају и проблеми разбијања неких (не свих) криптографских алгоритама. Стога треба доказати отпорност и на нападе квантним

рачунарима (тзв. проблем постквантне криптографије), што је још тежи задатак.

Још једна примена

За крај, поменимо један правац истраживања који обједињује формализацију математике и формализацију појма алгоритма.

Програми се обично тестирају на коначном броју примера. Мада се примери пажљиво бирају тако да вероватноћа неиспољавања грешке ако постоји буде што мања, обично нешто промакне. Други пут је формална провера софтвера, где се жељене особине неког програмског кода доказују као теореме. Међутим, пошто су људи подложни грешкама, доказе треба да провери машина.

У том погледу, најпре имамо проверавач доказа којима мора целокупан доказ бити дат на улазу. С обзиром на то да је људима напорно да уносе баш сваки корак доказа, други приступ су доказивачи теорема који аутоматски доказују задату теорему. Међутим, пошто се испоставило да је тај циљ за већину математичких теорија чак недостижан, златна средина су помоћници у доказивању који такође захтевају доказ на улазу, али не сваки корак, јер имају „ограничену памет”, тако да човек не мора да уноси баш сваки корак, већ само оно за шта машина каже да јој је остало „нејасно”.

Водећи такви програми су *Isabelle*, *Coq* и *Agda*, при чему су сви они академски пројекти доступни као слободан софтвер отвореног кода. То је у овом случају чак неопходно, јер је провера исправности програма који проверава доказ, саставни део научне провере доказа које ти програми проверавају. Стога је тај модел уобичајен за академске пројекте, јер у супротном не би било могуће научно позивање на резултате који се њима добијају.

Лоша вест је да такав приступ, мада елиминише грешке у изворном коду у целини (а приступ је применљив и на друге софтверске компоненте, као и на хардвер), захтева много квалификованију радну снагу од класичне и самим тим је далеко скупљи, па се за сада примењује само за намене високог ризика, где може доћи до губитка људских живота, нарушавања људског здравља или велике материјалне штете.

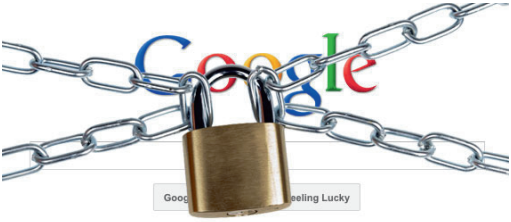
Ипак, верујемо да тај приступ има ширу будућност (мада не тако скору). Сваки програмски језик омогућава израду софтвера до неке сложености, када људи почињу да праве више нових грешака, него што исправљају старе. Са овим приступом нема граница у сложености, тако да постепено могу да буду прављене сложене компоненте које ће да користе и остали који развијају софтвер.

Демократија захтева слободан софтвер

Аутор: Матијас Киршнер
Превео и адаптирао: Дејан Маглов

Технологија је кроз историју утицала на друштво. Читање, писање, аритметика, пољопривреда, штампа и радио су примери изума који су променили наш начин схватања трговине, уметности и науке. Софтвер је са културолошког стајалишта најважнија технологија 21. века. *Free Software Foundation Europe* (*FSF Europe*) обавезала се да обезбеди људима у нашем друштву право да обликују ову технологију по својим потребама.

Данас је немогуће замислити свакодневни живот без софтвера. Већина нас не може да проведе ниједан дан без коришћења софтвера. Људи користе софтвер на радном месту (радна станица), на лаптопу и на мобилним телефонима. Софтвер се такође налази и на мање очигледним местима као што су возови, аутомобили, телевизори, вешмашине, фрижидери, и многи други уређаји. Већина од ових уређаја не може да функционише без софтвера. Без софтвера не бисмо могли писати писма, телефонирати, ићи у куповину или путовати као што смо навикли. Софтвер је централни инструмент нашег друштва. Када други контролишу алат тако важан за нас као што је софтвер, они могу да изврше велики утицај на наше акције. Ко контролише претраживач, који ми користимо, одређује шта ћемо пронаћи. Онај ко контролише нашу електронску пошту, има прилику да нас цензурише. Једноставно речено, контрола комуникационог сервиса подразумева способност одлучивања ко може да размењује, шта и са ким. Слично, онај који одлучује како софтвер функционише, има велики утицај на то како живимо и шта радимо.



У модерним демократијама моћ је одвојена. Ми делимо власт на законодавну, извршну и судску власт и свака има своју посебну институцију. Осим тога ми делимо одговорност на неколико нивоа надлежности, односно на централну владу, регионалне владе и локалне самоуправе. Кључна функција слободе штампе је да нас штити од формирања информативног монопола, где би превише моћи било концентрисано у рукама мањине. Кључна корист ефика-

сне демократије је да можете дати било какву функцију унутар демократског система и вашем највећем политичком противнику. (Последња реченица је кључна за схватање савремене демократије. Ово је идеал који су достигле све највеће капиталистичке демократије. Идеал је створити привид демократије код којег изгледа да народ бира своју власт, а у ствари, ко год је на власти, ништа се не мења, барем ништа кључно. То није проблем ако постоји консензус око националних интереса које нико не сме да угрози, али у свим осталим случајевима оваква демократија може да створи само проблем. - прим. прев.)

Веома је опасно за демократију да софтвер, критични друштвени инструмент, буде под контролом мале групе моћника. (Овде је кључ софтвер, али то исто важи и за енергију, кључне сировине, храну и лекове. То су кључни центри моћи у данашњој демократији а не политичари. - прим.прев.) Не само да наша комуникација зависи од софтвера, већ зависи и велики део инфраструктуре друштва. *FSF Europe* жели да заступа интересе корисника рачунара, а да се избори да у будућности контролу над софтвером имају сви. Друштво не сме себи да приушти да буде зависно од приватних интереса када је у питању алат тако важан као што је софтвер.

Наше друштво мора да обезбеди да свако има прилику да обликује софтвер по својој мери. То претпоставља да имамо слободу да користимо софтвер за било коју сврху, да проучавамо како софтвер ради, да га делимо са другима, и сами побољшавамо.

- **Право на коришћење:** Представља слободу употребе софтвера за било коју сврху без ограничења (на пример забране коришћења у комерцијалне или пословне сврхе). То обезбеђује могућност појединцу да доприноси заједници.
- **Право на проучавање:** То је право на слободу проучавања како софтвер функционише, односно изворни код, што представља срж за разумевање рада рачунара.
- **Право на дељење:** Слобода дељења софтвера омогућује да можемо помоћи другима тако што бисмо најбољи софтвер делили са њима.
- **Право на унапређење:** На крају, друштво мора имати слободу да модификује софтвер, мења га у сврху унапређења и прилагођавања личним потребама.

Софтвер који поштује ове четири слободе, јесте слободан софтвер.

Демократском друштву су потребни чврсти темељи. Једна од тих фундамената је слободан софтвер.

Литература:
https://fsfe.org/freesoftware/society/democracy.en.html

Pure

Аутор: Златан Васовић

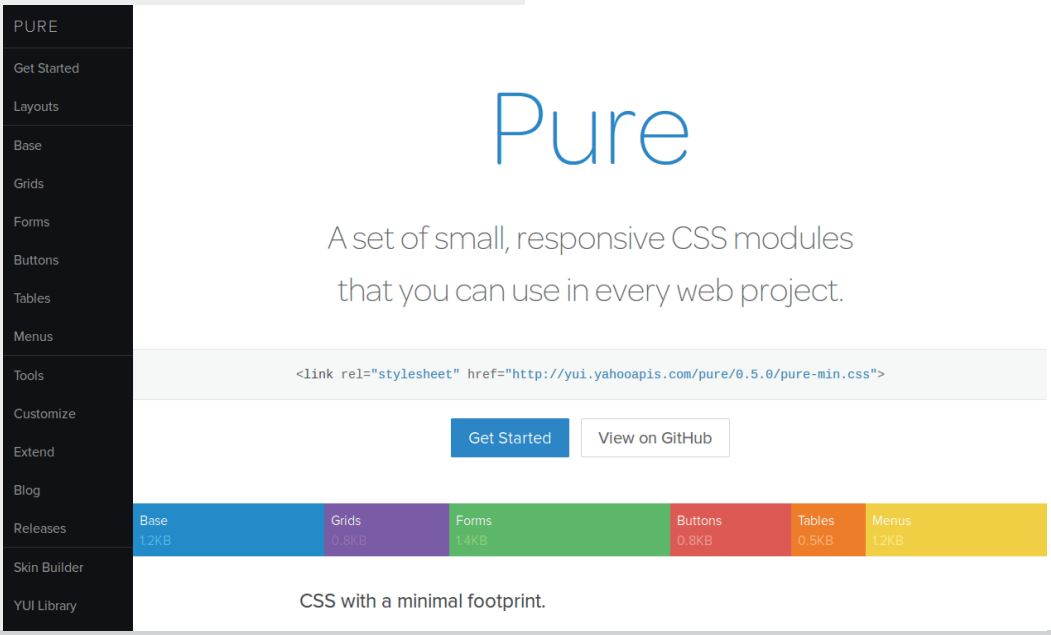
CSS је увек био интересантан језик за *framework*, јер *web* дизајнерима треба некакав сет стилова који ће им олакшати посао при изради *wеб* сајтова. У мору *CSS framework*-а, на врх су се истакли *Bootstrap* [1] и *Foundation* [2]. Ипак, *frame.work*-ови су углавном велики, са превише елемената. Из тог разлога се појавила нова идеја — минималистички *framework*.

Yahoo web development тим је решио да направи *framework* и за своје, и за потребе других, који садржи само основне елементе. Резултат тога је *Pure* [3], сада већ популарни минималистички *framework*.

Осврт

Pure садржи само основне елементе — типографију, *grid*, форме, дугмиће (енгл. *buttons*), табеле и менije.

Компресован и „гзипован”, *Pure* „тежи” само *4.4kB*.



Употреба

Pure се може директно учитати са *web*-а преко брзог *YUI API*-ја. Потребно је додати следећи код у *<head> HTML* странице:

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

Због мале величине датотеке, не би требало да утиче на учитавање странице.

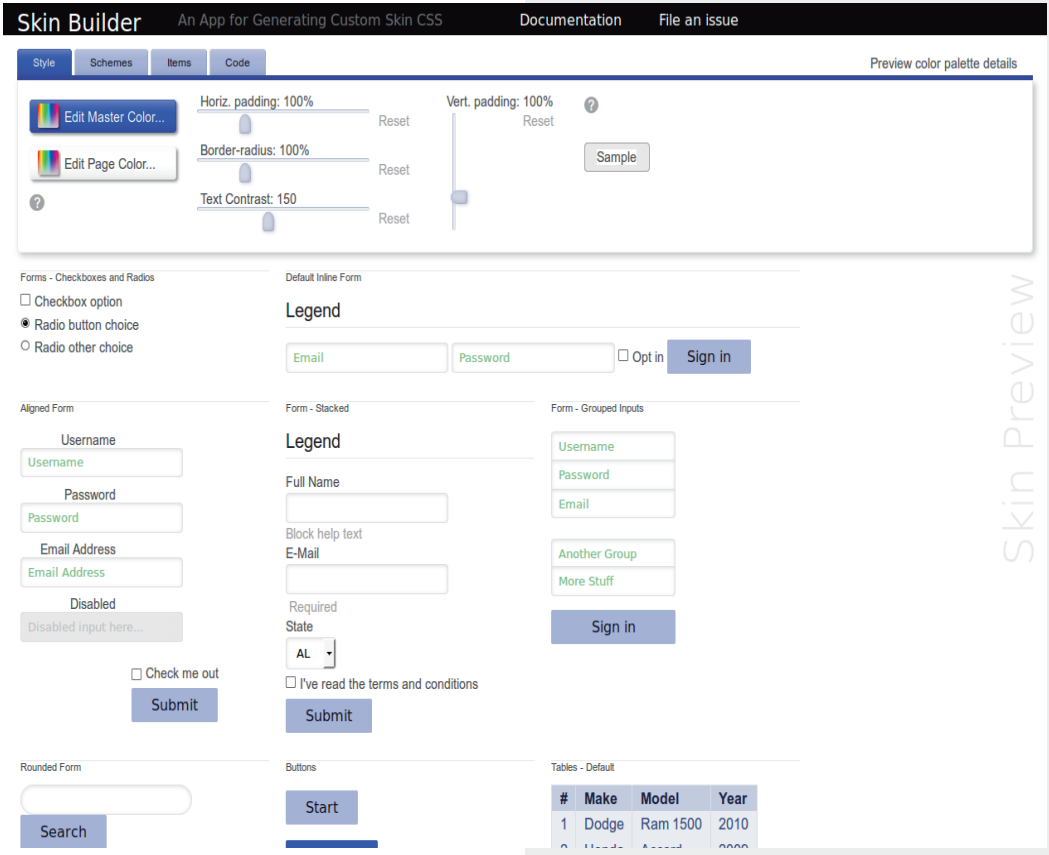
Може се и директно преузети са линка [4].

Уређивање

Framework је осмишљен тако да се лако може уредити, како од стране дизајнера, тако и од стране програмера. За дизајнере ту је „*Skin Builder*" [5], а за програмере изворни код у *GitHub* репозиторијуму [6].

Skin Builder-ом можете мењати боју позадине, текста, радијус и слично, како бисте прилагодили *Pure* својим потребама.

Ако вам је потребна било каква додатна помоћ, прочитајте http://purecss.io/start/ .

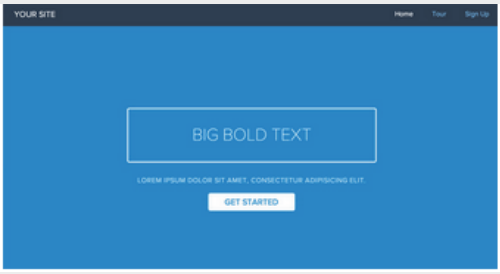


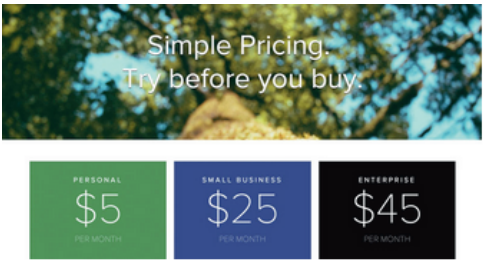
Закључак

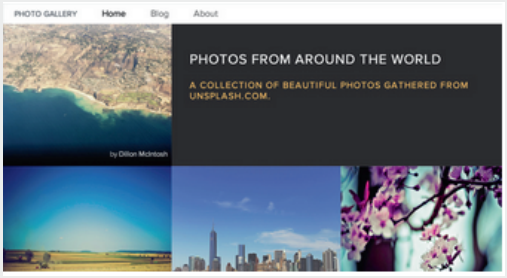
Pure је веома користан *framework* за оне који почињу да раде са *CSS*-ом, али и за оне који не желе да троше време на прављење целог *framework*-а од нуле. Заслужује нашу препоруку (прим.аут.).

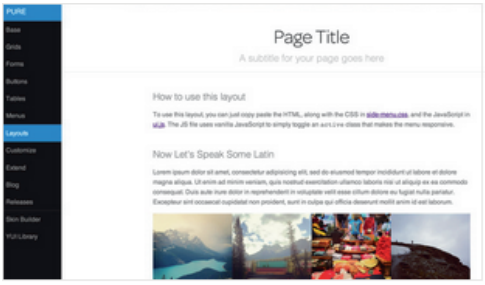
Линкови

[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/









Енкриптована електронска пошта

(2. део)

Аутор: Петар Симовић

Пошто смо се у прошлом делу укратко упознали са оваквим видом енкрипције, сада ћемо мало детаљније проћи кроз процес инсталације и коришћења енкрипције за шифровање и сигурносну размену електронске поште. Пре него што наставимо, напоменућемо неколико ствари. Прва ствар је вероватно банална читаоцима претходног дела, а односи се на генерисање кључева. Наиме, пре неколико недеља објављен је текст (http://goo.gl/7yxTfa) у коме *Snowden* говори како енкрипција функционише и како доскочити Америчкој безбедносној агенцији шифрујући своју електронску пошту користећи *PGP*, што је у реду, али се такође сугерише да се користи бесплатни *on-line* програм (*iGolder*: http://goo.gl/SvQivp) за генерисање кључева (и приватног и јавног), што господин *Snowden* никада није навео. Наравно, ово није први пут да се ситуација глобалног надзора, неупућеност корисника и изјаве *Snowden*-а користе за навођење корисника на погрешан пут, па овом приликом скрећемо пажњу да се кључеви морају генерисати на вашој машини и да се мора чувати приватни кључ. Друга ствар је да се не ослањате превише на *on-line* услуге када су у питању приватност и сигурност података. Тако се, на пример, сајт једне од новијих *on-line* апликација (*Intactmail*: http://goo.gl/Z4n8pW) за шифровање електронске поште већ гаси, иако није прошло ни пола године откако се о њој почело писати (http://goo.gl/YKXo7l), тако да је најсигурнији штреберски начин „све преко терминала", или за почетнике преко неких додатака за *desktop* апликације попут *Thunderbird*-а.

Сада можемо да пређемо на инсталацију. Биће вам потребни следећи програми:

- *GnuPG*, који је на већини данашњих *Linux* дистрибуција већ укључен у саму инсталацију оперативног система тако да је велика вероватноћа да га већ имате инсталираног, што можете проверити у терминалу следећом командом:

```
gpg --version
```

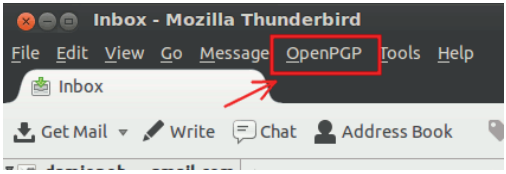
- *Thunderbird* (http://goo.gl/RLdzIR) –

није обавезно да то буде овај програм, па тако можете користи и *Claws Mail* који редовно иде уз *Tails* или *Icedove*, или неки други *open-source* програм. Претходно проверите које сигурносне додатке за енкрипцију подржава.

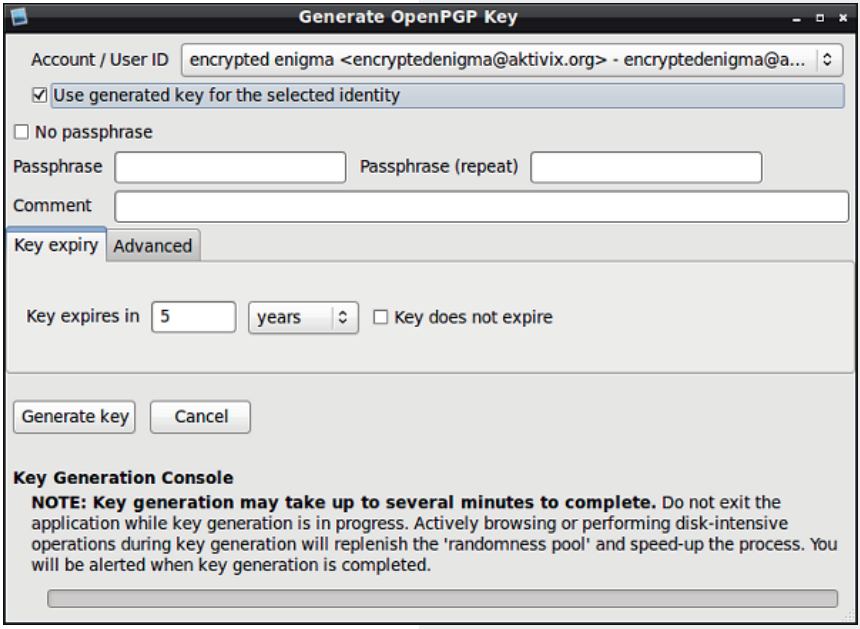
- *Enigmail* (http://goo.gl/J3sztY) екстензија за *Thunderbird* али и за друге програме попут *Icedove*-а, коју можете инсталирати из *Thunderbird*-а (*Tools » Add-ons»*, па тражити *„Enigmail”*).

Након што сте инсталирали потребне апликације, направите налог електронске поште, или унесите већ постојећи (*Create new account » Email)*, и након што попуните тражена поља о адреси електронске поште и шифру која јој одговара, можете притиснути *Read messages*. Биће учитана сва ваша пошта са сервера тог налога електронске поште. Потом је потребно да направите пар кључева који ћете користити за шифровање уз тај налог. Уколико користите више налога, за сваки ће вам бити потребни посебни кључеви, али полако: када направите први и почнете да га користите, додавање нових налога и генерисање кључева за исти неће бити проблем.

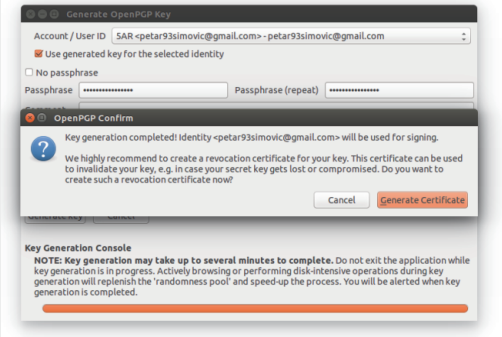
Сада је потребно да генеришете први пар кључева што ћете урадити из *Thunderbird*-а, где би требало да имате опцију *OpenPGP*. У њеном падајућем менију одаберите *Key Management*. Отвориће вам се нови прозор и у његовим опцијама у врху прозора потражите опцију *Generate*, па онда *New Key Pair*.



Пре него што притиснете *Generate*, морате попунити поља за сигурносну фразу (*Passphrase*), која представља лозинку за приступ вашем приватном кључу за одређени налог електронске поште, и проверити да ли је приказани налог електронске поште онај за који генеришете кључеве (поље *Account » User ID*). Сигурносну фразу треба да негде сачувате или запишете јер ће вам често бити потребна. Такође, сваки налог ће имати своју независну фразу као и енкрипционе кључеве. Уколико сада притиснете *Generate*, рачунар ће почети да генерише 2048-битне *RSA* кључеве, што је задовољавајућа дужина кључева који ће истећи за пет година. Најбоље је да ове опције све оставите какве су подразумеване, уколико сте почетник, док напредније кориснике охрабрујемо да повећају дужину кључева на 4096-бита и да време истека смање на две године. Још само једна напомена пре него што притиснете *Generate* дугме и рачунар све уради за вас: прочитајте белешку масним словима испод *Generate* дугмета и припремите се да активно сурфујете нетом, отварајте све апликације које вам падну на памет, пустите неки видео и музику, како би рачунар имао висок степен ентропије о којој смо причали у прошлом делу и припремите неку екстерну меморију за складиштење поверљивих података након генерисања кључева, у виду *USB* меморије или *CD*-а.

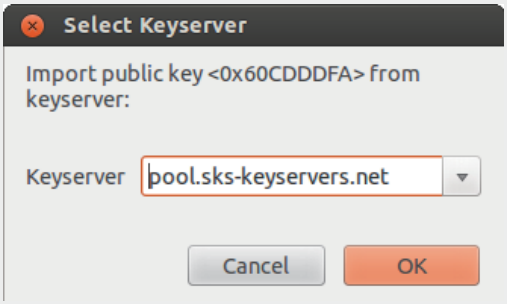


По завршетку креирања кључева показаће вам се порука која препоручује да креирате и сертификат у случају да изгубите кључеве, или их неко сазна. Обавезно прихватите и сачувајте сертификат! Пошто већ има доста фајлова које треба да чувате у вези са енкрипцијом ваше поште, предлажемо вам да их уредно сачувате у неки празан директоријум посебно за ове намене који ћете после преснимити на *USB* или *CD* (за додатне мере опреза можете директоријум шифровати, па га тек онда преснимити).

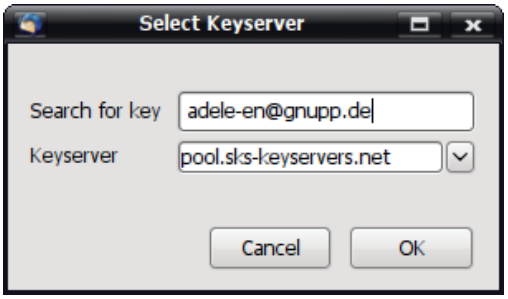


Сада би у отвореном прозору *OpenPGP Key Management*-а требало да вам се појави нови податак са вашим мејлом, што је уствари ваш пар кључева. Можете приметити да он има и свој *Key ID* кога би требало, такође, да запишете или сачувате негде. Немојте затварати овај прозор јер вам треба за следећи корак. Следећа ствар је такође важна и односи се на објављивање вашег јавног кључа на

један од сервера јавних кључева. Ово је веома корисно јер не морате порукама размењивати кључеве ако сте их обоје објавили на сервер јавних кључева, него је потребно да само претражите сервер о подацима за имејл чији јавни кључ желите. Ово можете урадити тако што ћете у отвореном прозору *OpenPGP KEY MANAGEMENT* притиснути десни клик миша на кључеве које сте управо креирали и одабрати опцију *UPLOAD PUBLIC KEYS TO KEYSERVER*. Оставите *keyserver* да буде подразумевани *„pool.sks-keyservers.net"* и притисните *OK*!



Пред крај, да бисте се уверили да ово заиста ради, можете послати енкриптовану или дигитално потписану поруку аутоматском *OpenPGP* роботу *Adele*, који ће одмах на њу одговорити. Прво изаберите из *Thunderbird*-а опцију *OpenPGP*, па *Key Management*, па онда из његових опција *Keyserver*, затим *Search for Keys* и ту унесите имејл адресу *Adele* робота: adele-en@gnupp.de на серверу јавних кључева. Ваш јавни кључ можете послати примаоцу и као *Attachment* (OPENPGP » KEY MANAGEMENT » десни клик на ваш мејл са кога шаљете » SEND PUBLIC KEYS BY EMAIL) што ће отворити нову поруку и укључити у *Attachment* ваш јавни кључ. Уколико сте већ свој кључ објавили на сервер јавних кључева, није потребно да га шаљете поруком, већ само реците примаоцу да га потражи на серверу.



Након тога ће њена адреса бити у менију *Key Management*-а из кога треба да десним дугметом миша кликнете на њену адресу и да изаберете опцију *Sign key*, подесите ниво поверења и унесете вашу сигурносну фразу коју сте, надамо се, сачували. Уколико нисте сачували сигурносну фразу, мораћете да правите нове кључеве и старе да обришете, па све из почетка.

Ово је основа која вам је потребна да бисте своју електронску пошту осигурали шифровањем. Наравно, пошто је ово електронска пошта и потребно је двоје да би функционисала, морате поштовати слободу онога са друге стране ако не жели да шифрује своју пошту, и зато је потребно да се најпре пробуди свест међу људима о криптографији, па ће је почети чешће користити.

Корак до *Google*-а (6. део)

Аутор: Дејан Чугаљ

Толико тога је речено, урађено, написано, и на крају објашњено у *Lucene* серијалу. За крај остаје фамозни **Индекс** који је срж *Lucene*.

Тај **Индекс**, који није обичан *Index*, све више сагледавајући *Lucene*, видимо да је то оно што чини *FLOSS* заједницу (прим.аут.). **Индекс** нам даје општу представу да *Google* није једини и универзални шаблон по ком би требало да се водимо. Као пример морамо навести инцидент који се десио у Кини и који би требало да представи класично избегавање монополизма, како у економским наукама, тако и у *IT* сфери.

Једноставном одлуком тако моћне компаније као што је *Google*, скоро трећина човечанства је остала без круцијалног дела интернет коришћења, а то је претрага (прим.аут.). Резултат овог монополистичког понашања *Google*-а је изродио *Baidu*, јединствени претраживач коришћен само у Кини, а нама даје за пример употребу *Lucene* фамилије јединственог принципа, алгоритама, који смо до сада укратко, колико је то могуће, „претрчали" у *Java* програмском језику.

Иако би овде требало да широко разматрамо **Индекс**, тај појам о ком говоримо скоро седам месеци, покушаћемо да га сведемо на неко теоријско разматрање опште-затеченог стања глобалног *IT*-а. Зашто спомињемо ово, зашто је то толико битно у овако „разрађеном" и „усклађеном", скоро па бисмо рекли и стандардизованом свету интернет технологија? Оно што чини интернет, управо је та **слобода**, *FLOSS* заједница, дељење опште стеченог знања и тежња ка побољшању, окосница младих научника који стреме остваривању циља науком, а у сврху побољшања свеопштег. Тако је и рођен *GNU/ Linux*(прим.аут.).

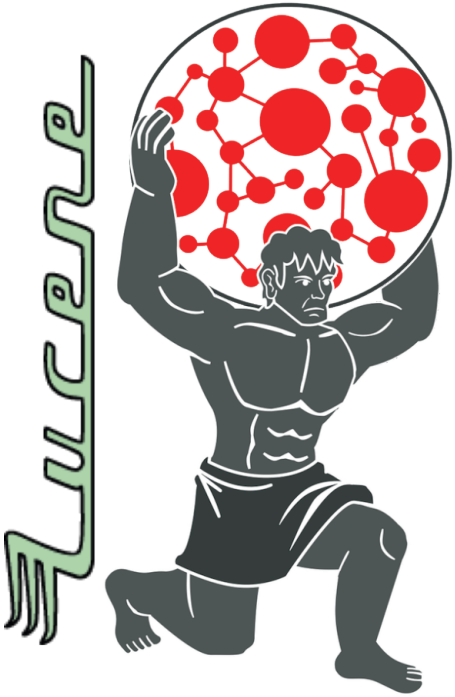
Невероватно залагање, самопожртвовање *Richard*-а *Matthew*-а *Stallman*-а, оставило је *open-source* лиценцу - *GNU General*

Public License као завештање пионирског корака којим смо се приближили управо тим *Lucene* **Индексом**. Како бисмо објаснили тај исти **Индекс**, морамо да се вратимо на почетак серијала и да опет споменемо да је *Lucene* управо произишао из *Google*-а, тј. једног од „радника" који је радио у *Google*-овом развојном тиму.

Некако остајемо затечени чињеницом да се све своди на појединце, индивидуе, да су највећа открића везана уско, широко, за те бриљантне умове, који склапајући

све коцкице у целину, дају нама, обичним људима, могућност да се некако одвојимо од глобалистичко-монополистичке основе и да почнемо да размишљамо својом главом (прим.аут.).

Оно што чини тај фамозни *Lucene* **Индекс** специјалним, није више у сфери програмирања, алгоритма, већ представља окосницу, прву линију фронта борбе којом би требало сви да се водимо, али како наши читаоци прате ЛиБРЕ! часопис, и самим тим што читају крај серијала о *Lucene*, мислимо да смо корак ближе победи (прим.аут.).



BalCCon (https://balccon.org) организује заједница и свака помоћ нам је добродошла.

Конгрес не би било могуће организовати без људи који ће волонтирати на њему и помоћи нам да се *BalCCon* одржи.

BalCCon се ослања на вашу помоћ. Молимо вас да размислите о волонтирању на *BalCCon2k14* - Second Base! Можете се пријавити слањем *e-maila*, на jelena [at] balccon [dot] org.

E-mail наслов: Волонтер *BalCCon2k14*
Пошаљите:

Име и презиме (надимак):

Земља:

E-mail:

Број мобилног:

Величина мајице:

Нешто о себи: (до 1000 речи)

Битно је само да волонтери желе да нешто ново науче и да помогну. Све потребне информације волонтери ће добити на лицу места, а у току конгреса ће имати подршку координатора волонтера.

Рок за пријаву је 25.08.2014.

Хвала вам што сте одлучили да се пријавите за волонтирање на *BalCCon2k14*.